UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS INC. and FORTINET INC.,
Petitioner

IPR2024-00539
U.S. Patent No. 8,051,460

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

I. INTRODUCTION 9
II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE 10
III. LEVEL OF ORDINARY SKILL IN THE ART 15
IV. RELEVANT LEGAL STANDARDS 16
V. OVERVIEW OF THE 460 PATENT 18
VI. CLAIM CONSTRUCTION 21
VII. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE 22
VIII. THE PRINCIPAL PRIOR ART 22
A. Summary of Krantz 22
B. Summary of Herrmann 25
C. The Combination of Krantz and Herrmann 29
IX. Krantz, OR KRANTZ and HERRMANN render obvious CLAIMS 1-6, 10-14, 16-22, 27, and 29-30 36
A. Detailed Analysis of the Challenged Claims 36
1. Claim 1 36
a. [1.0] A method of granting access to a protected network, the method comprising: 36
b. [1.1] receiving a request for access to a less-restricted subset of the protected network from an access device, ... 43
c. [1.2] the request received through a communication port of an access point, ... 48
d. [1.3] the communication port configured for communicating between the access device and a restricted subset of the protected network, ... 52
e. [1.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and 62
f. [1.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without

passing the data through the gatekeeper, when the requirements of the security policy are satisfied. 68
2. Claim 2 77
a. [2.0] The method of claim 1, further comprising authenticating a user of the access device. 77
3. Claim 3 78
a. [3.0] The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy. 78
4. Claim 4 81
a. [4.0] The method of claim 3, wherein the system data includes antivirus software status. 81
5. Claim 5 83
a. [5.0] The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and 83
b. [5.1] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy. 88
6. Claim 6 88
a. [6.0] The method of claim 5, wherein the system data includes information regarding devices connected to the access device. 88
7. Claim 10 91
a. [10.0] The method of claim 1, wherein the access point is a network switch. 91
8. Claim 11 92
a. [11.0] The method of claim 1, wherein the access point is a wireless access point. 92
9. Claim 12 92
a. [12.0] The method of claim 1, wherein the access point is a remote access virtual private network. 92

10. Claim 13 94
    a. [13.0] The method of claim 1, wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network. 94
11. Claim 14 95
    a. [14.0] The method of claim 1, wherein the restricted subset of the protected network is characterized by an access control list. 95
12. Claim 16 97
    a. [16.0] A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising: 97
    b. [16.1] receiving a request for access to a less-restricted subset of the protected network from an access device,. 99
    c. [16.2] the request being received through a communication port of an access point, ... 99
    d. [16.3] the communication port configured for communicating between the access device and a restricted subset of the protected network, ... 99
    e. [16.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; and 99
    f. [16.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when requirements of the security policy are satisfied. 99
13. Claim 17 100
    a. [17.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device. 100
14. Claim 18 100
    a. [18.0] The non-transitory computer readable storage medium of claim 16, ... 100

b. [18.1] wherein the program is further executable by a processor to obtain system data from the access device, and.....100
c. [18.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....100
15. Claim 19.....100
a. [19.0] *The* non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data.....100
16. Claim 20.....100
a. [20.0] The non-transitory computer readable storage medium of claim 16,.....100
b. [20.1] wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and.....101
c. [20.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.....101
17. Claim 21.....101
a. [21.0] The non-transitory computer storage readable medium of claim 20, wherein the system data includes information regarding devices connected to the access device.....101
18. Claim 22.....101
a. [22.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after recofiguring the communication port for communicating between the access device and the less-restricted subset.....101
19. Claim 27.....105
a. [27.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further

executable to update the access device when requirements of the security policy are not satisfied. ...105

20. Claim 29 ...106

a. [29.0] The non-transitory computer readable storage medium of claim 16, wherein the restricted subset of the protected network is characterized by an access control list ...106

21. Claim 30 ...106

a. [30.0] The non-transitory computer readable storage medium of claim 29, wherein access to the restricted subset of the protected network is responsive to a VLAN configured to communicate with the protected network subject to the access control list. ...106

B. Additional Obviousness Analysis of Claims 1-2, 10-14, 16-17, 27 and 29-30 based on Krantz and Herrmann ...107

X. CONCLUSION ...107

TABLE OF AUTHORITIES

Page(s)

Statutes

18 U.S.C. § 1001 108

35 U.S.C. § 102 (e) 22, 25

35 U.S.C. § 103 .....3, 17

EXHIBIT LIST

No.	Exhibit Description
1001	U.S. Patent No. 8,051,460
1002	U.S. Patent No. 8,051,460File History
1003	Declaration of Henry Houh, Ph.D
1004	CV of Henry Houh, Ph.D
1005	U.S. Patent Pub. No. 2004/0111520 to Krantz et al
1006	U.S. Patent Pub. No. 2004/0107360 to Herrmann et al
1007	IEEE Std 802.1Q-1998 – IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks
1008	U.S. Patent No. 6,430,621 to Srikanth et al.
1009	U.S. Patent No. 6,032,194 to Gai et al.
1010	Cisco IOS 12.0 Switching Services (1999)
1011	Microsoft Computer Dictionary 5th Edition (2002)
1012	Webster's New World Computer Dictionary (2001)
1013	Dictionary of Computer and Internet Terms 8th Edition (2003)
1014	U.S. Patent No. 5,987,611 to Freund
1015	U.S. Patent No. 7,260,726 to Doe et al
1016	RFC 2716 – PPP EAP TLS Authentication Protocol
1017	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. 8,051,460 ("the 460 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 1-6, 10-14, 16-22, 27, and 29-30 ("the Challenged Claims") of the 460 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 460 Patent, Ex.1001.

b. the prosecution history of the 460 Patent ("460 File History"), Ex.1002.

c. U.S. Patent Pub. No. 2004/0111520 to Krantz et al., ("Krantz"), Ex.1005.

d. U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. ("Herrmann"), (Ex.1006).

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.1004. 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 460 Patent. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields. Lack of professional experience can be remedied by additional education, and vice versa.

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 460 Patent.

IV. RELEVANT LEGAL STANDARDS

23. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the 460 Patent, I am relying on certain basic legal principles that counsel has explained to me.

24. I understand that prior art to the 460 Patent includes patents and printed publications in the relevant art that predate the priority date of the 460 Patent. For purposes of this Declaration, I am applying September 24, 2003, as the priority date of the 460 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 460 PATENT

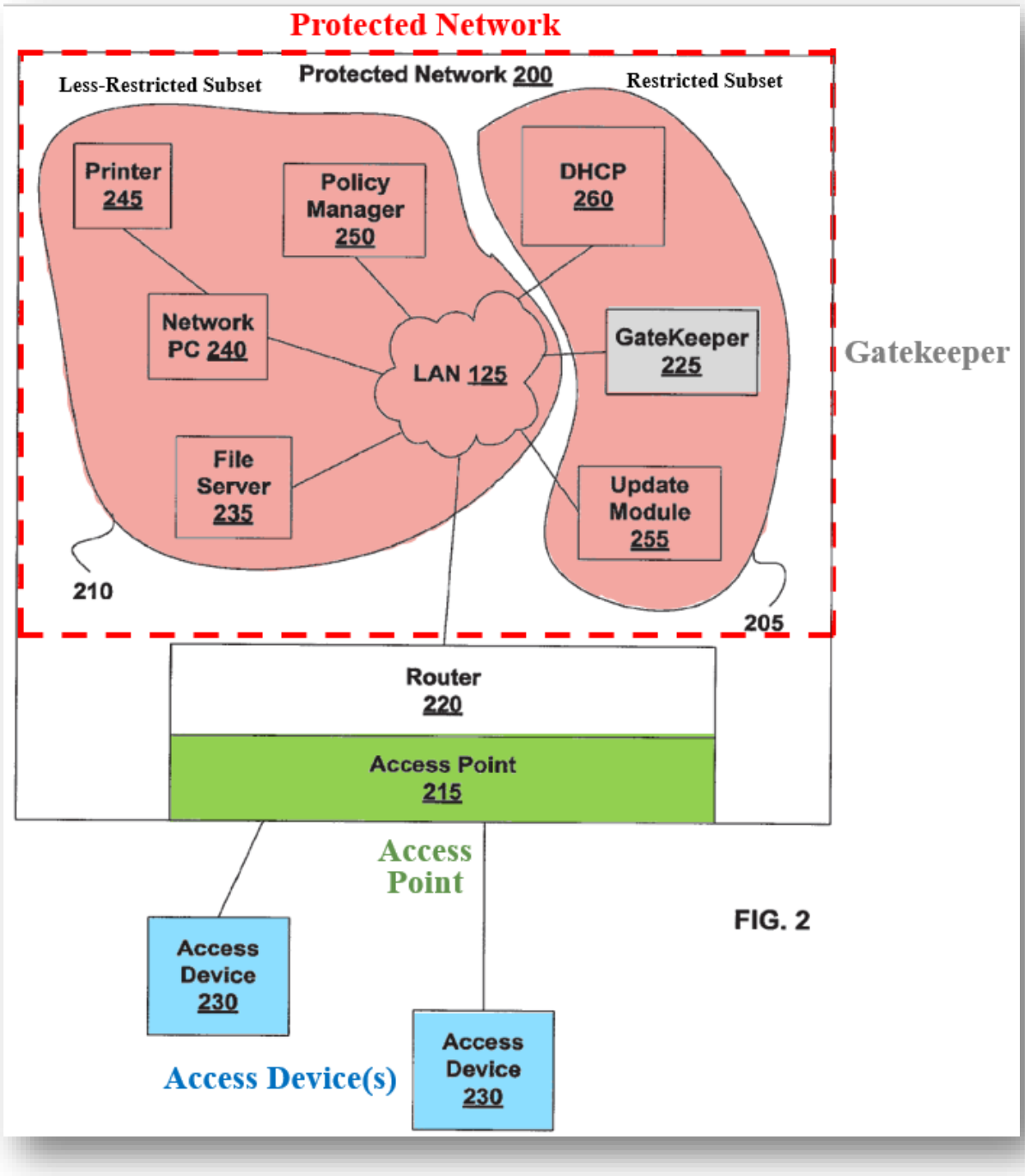
30. The 460 Patent states that it is "a continuation and claims the priority benefit of U.S. patent application Ser. No. 10/949,179 filed Sep. 24, 2004 now U.S. Pat. No. 7,523,484, and entitled "Systems and Methods of Controlling Network Access," which claims the priority benefit of U.S. Provisional Patent Application No. 60/505,582 filed Sep. 24, 2003 and entitled "Gatekeeper Inventions for Controlling Access to a Corporate Network" and U.S. Provisional Patent Application No. 60/513,080 filed Oct. 21, 2003 and entitled "Gatekeeper

Invention for Controlling Access to a Corporate Network Using 802.1x." 460 Patent, 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 460 Patent, including that of U.S. Patent No. 7,523,484, to which the 460 Patent claims priority, and note that none of the activity there is pertinent to my analysis.

32. U.S. Patent No. 8,051,460 ("the 460 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." 460 Patent, 2:53-54. Access to less-restricted networks from a device "are first passed to the restricted subset." 460 Patent, 2:54-56. Elements of the "restricted subset"—such as a "gatekeeper"—"are then used to apply security policies" to the device requesting access. 460 Patent, 2:56-58. If the requesting device satisfies the "security policies," access is then granted "to a less-restricted subset of the protected network." 460 Patent, 2:58-60. The 460 Patent further explains that both "the passing of access requests to the restricted subset" and the subsequent granting of such requests is "accomplished by configuring and reconfiguring a communication port of an access point." 460 Patent, 2:61-63.

33. Figure 2 depicts various embodiments of the invention described in the 460 Patent, and is annotated below:



Ex.1001 (460 Patent), Fig. 2 (annotated)

34. For example, Figure 2 includes "Protected Network 200," which is described in the 460 Patent as "either physically or logically divided into a

Restricted Subset 205 and a Less-Restricted Subset 210." 460 Patent, 5:55-58. The 460 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." 460 Patent, 5:59-64. The 460 Patent describes that the security policy may proscribe up-to-date virus software and encryption protocols, (Ex.1001 2:18-26), include requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1001, 6:38-52), or authenticate an access device (or user) of the access device. Ex.1001, 11:35-43, 12:4-6.

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 460 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.

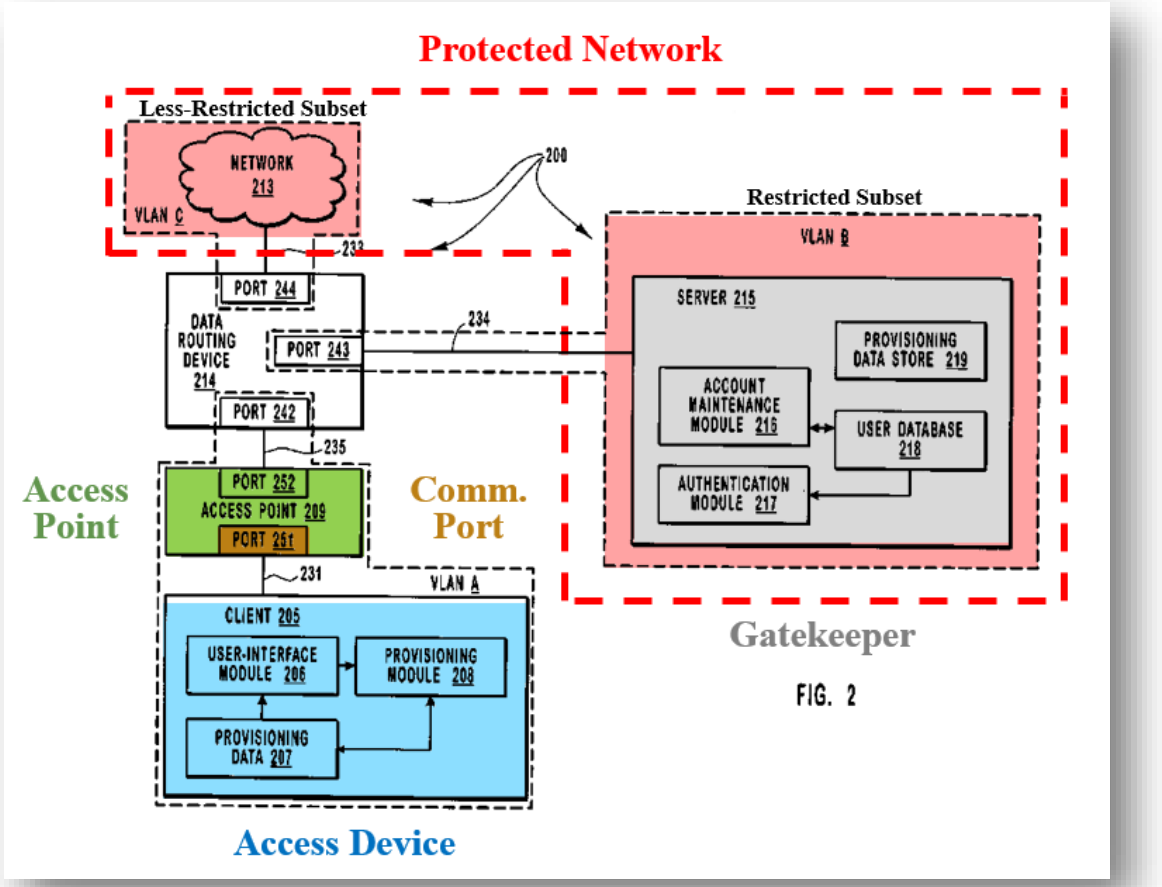
VIII. THE PRINCIPAL PRIOR ART

A. Summary of Krantz

40. U.S. Patent Pub. No. 2004/0111520 to Krantz et al. (Ex.1005) was filed on December 6, 2002, and published on June 10, 2004. I understand that it is therefore prior art to the 460 Patent at least under 35 U.S.C. § 102 (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. 1005, [0015].

42. More specifically, Krantz discloses a system in which a device attempts to access a protected network. *See, e.g.*, Ex.1005, [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.1005) (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 in server 215. Ex.1005, [0073], [0076]. The server is

also responsible for ensuring that the client device adheres to certain configuration settings—including the established encryption protocol—for gaining access to the network authorized to be accessed. Ex.1005 [0110]-[0111].

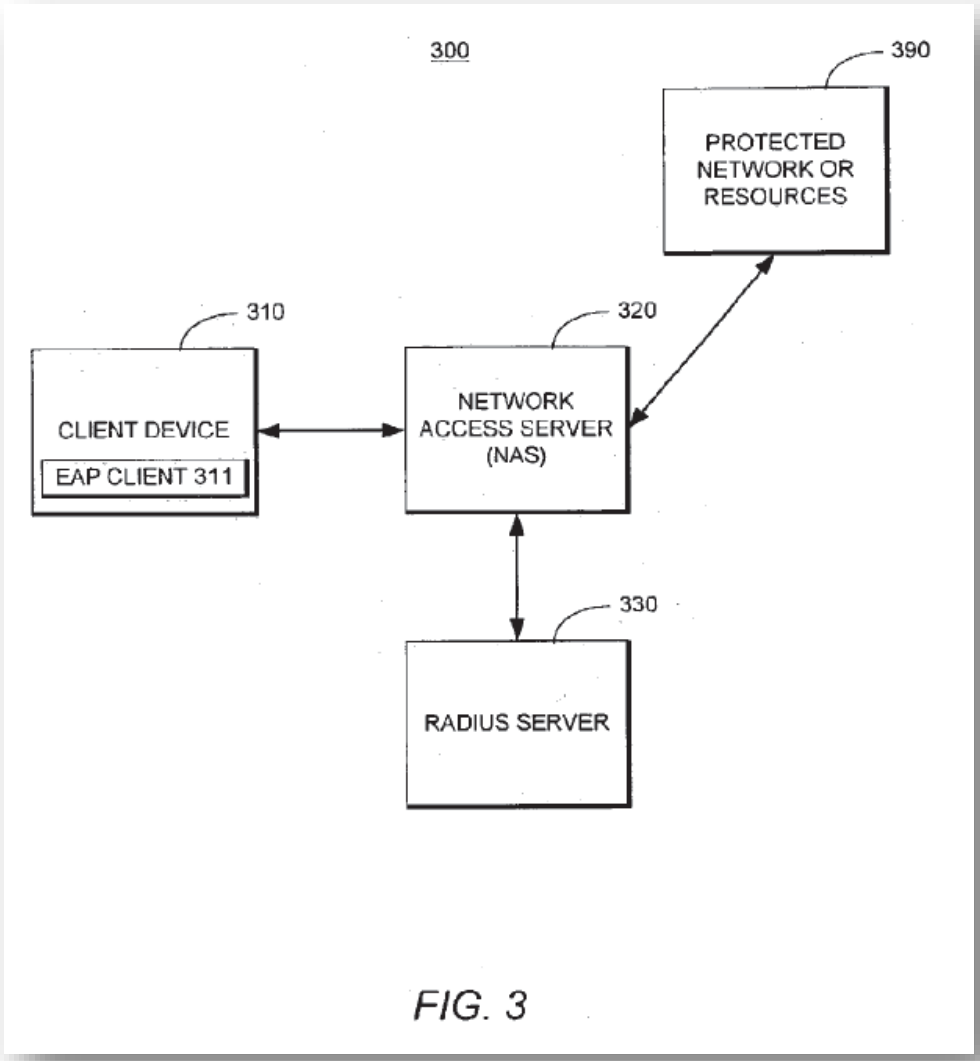
B. Summary of Herrmann

45. U.S. Patent Pub. No. 2004/0107360 to Herrmann et al. (Ex.1006) 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 460 Patent at least under 35 U.S.C. § 102 (e).

46. Hermann is directed to enforcing security policies when providing access to a network. Hermann describes that if a client device connected to a network . . . [and] is infected with a virus or worm, it may infect other machines on the same network. Ensuring that devices connected to the network are running current anti-Virus programs is particularly important, as virus suppression methods are very time sensitive. Ex.1006 [0012].

47. As a solution, Hermann proposes the collection of information from a client device which is used during the authentication process to enforce network security policies. For example, Herrmann teaches a system in which a client device attempts to access a network and information is collected to determine whether the client can gain access to protected network resources. Ex.1006,

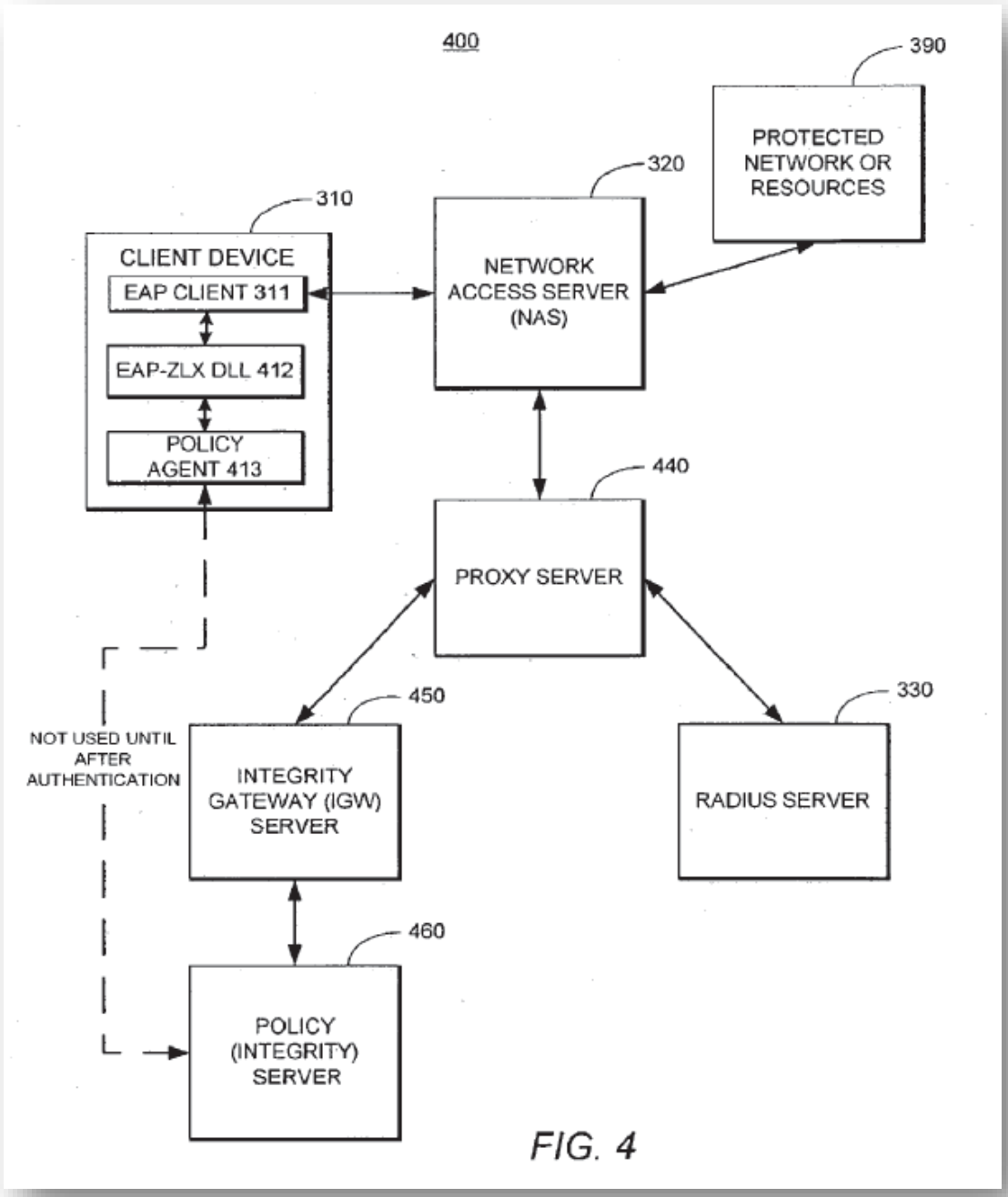
[Abstract], [0063]. The network access system is described with respect to Figures 3 and 4. The basic architecture of the system includes at least a client access device, network access server, and protected network and/or resources are shown below in Figure 3 of Herrmann. Ex.1005, [0018], [0053], [0063]



Herrmann, Fig. 3 (Ex.1006)

48. 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.*

49. 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 460" … which "ensures that all users accessing a particular system or network comply with specified security policies, including access rights and cooperative anti-virus enforcement" and can deny network access for access devices that are not in compliance. *Id.*, [0067].



Herrmann, Fig. 4 (Ex.1006)

50. 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

51. It would have been obvious to include Herrmann's techniques related to enforcing security policies (including checking for anti-virus protection at the client) and obtaining system data from an access device in the system of Krantz for the reasons explained below. In particular, the Krantz system already discloses that "access point 209 may block [] protocols … from being transferred **until client 205 is authenticated (and authorized)**. Ex.1005, [0072]. Specifically, Krantz explains that as part of its security policies, client devices are authenticated, (Ex.1005, [0067]-[0074], [099]) and users of client devices are authenticated, Ex.1005, [0074], [0076]. Ex.1005, [0076].

52. A POSITA would recognize that checking for anti-virus software as part of a security policy would merely be an additional item for server 215 to check in the process already disclosed by Krantz. Ex.1005, [Fig. 3], [0068]-[0076] (describing the steps of authenticating client devices and users). Like Krantz, Herrmann discloses a "policy server 460 [which] may enforce a variety of different types of security policies or rules." Ex.1006, [0068]. One such rule, to be authorized for network access, would be "a policy requiring that a **specific virus protection program** is operational on each client device that is connected to a

network." Ex.1006, [0012]. Herrmann expressly recites that the policy server determines whether the client device 310 is in compliance with applicable security policies. Ex.1006 [0066].

53. A POSITA would also be motivated to modify the teachings of Krantz to include determining whether the requirements of a security policy that include checking for virus protection are satisfied as taught by Herrmann for several reasons. As explained in detail below, Krantz already describes a security policy that includes requiring authentication of a client device and users. Krantz also teaches providing a configuration file with the proper encryption protocol (and other necessary configuration information), the client device is configured to for compatible operation with the network. Herrmann discloses that it is "particularly important" that devices connected to the network are running current anti-virus programs, and that one way of ensuring this is implementing a "policy requiring that a **specific virus protection program.**" Ex.1006, [0068]; *see also*, Ex.1006, [0012] (noting it is critical that all machines in a network maintain updated antivirus software so the network is not infiltrated by newly released viruses). Herrmann expressly recites that the policy server determines whether the client device 310 is in compliance with applicable security policies, which would include specific virus detection. Ex.1006, [0066]. Thus, a POSITA would be motivated to modify the teachings of Krantz to include in a security policy requirements that a

specific virus protection program be utilized, and to make a determination if the client device satisfies the applicable security policies before allowing the client device to access protected networks in order to prevent viruses from infecting the protected network and to ensure network compatibility

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

55. The 460 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 460 Patent it discusses GateKeeper 110 (Ex.1001, 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.1001, 2:23-26.

56. Both Krantz and Herrmann are analogous art to the 460 Patent for at least two reasons. *First*, Krantz and Herrmann are both directed toward the same field of endeavor of the 460 Patent—network security. Ex.1001, 1:23-24 ("The invention is in the field of computing systems and more specifically in the field of

network security."); Ex.1005, Abstract ("A computer system attempts to authenticate with a server to gain authorization to access a first network."); Ex.1006, Abstract ("A system and methodology for policy enforcement during authentication of a client device for access to a network is described.").

57. *Second*, both Krantz and Herrmann are reasonably pertinent to a problem described by the 460 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.1001, 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.").

58. Krantz discloses a security policy beyond user authentication and encryption protocols. For instance, "[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C**." Ex.1005, [0068]. The use of EAP-TLS (*e.g.*, Ex.1005, [0067]-[0074], [0100]) was a known

authentication protocol that would be used to authenticate client devices. Ex.1016 [RFC2716] at 1, 2. Krantz further discloses that the security policy can include "a configuration sub-file to indicate whether or not **operating system credentials** should be used for authentication." *Id.*, [0099].

59. 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].

60. 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.1006, [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].

61. 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].

62. 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.

63. It would have been obvious to combine Herrmann with Krantz because a POSITA would have been motivated to do so based on the teachings of Krantz. For example, Krantz explains that its system relates to a server that "includes the functionality to authorize clients to access a second network"

EX.1005, [0016]. EX.1005, [0002]. Similarly, Herrmann explains that "[t]he present invention relates to … policy enforcement on **computer systems** connected on one or more networks…" EX.1006, [0003].

64. 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.1005, [0014] ("Therefore what would be advantageous are systems, methods, computer program products, and data structures for increasing the level of automation when provisioning and configuring a computer system to access a network."); *id.*, [0019] ("If credentials do not authorize full access … the server can respond by sending a notification … [including] conditions (e.g., signup, renewal etc.) a user must satisfy to become authorized for full access to resources …" Thus, A POSITA would have recognized that Herrmann's disclosure of a policy server checking that a computer device complies with, e.g., an antivirus security policy, would be complimentary to the system of Krantz,

which seeks an automated process for providing network security. In addition, a POSITA would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as doing would involve minimal changes to the existing Krantz system.

IX. KRANTZ, OR KRANTZ AND HERRMANN RENDER OBVIOUS CLAIMS 1-6, 10-14, 16-22, 27, AND 29-30

A. Detailed Analysis of the Challenged Claims

1. Claim 1

a. [1.0] A method of granting access to a protected network, the method comprising:

65. Krantz discloses "*[a] method of granting access to a protected network*."

66. The "*protected network*" of the 460 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.1001, 6:5-9.

67. The network disclosed in Krantz is such a "*protected network*" as described in the 460 Patent. As will be explained in the following paragraphs, VLAN B and VLAN C of Krantz (e.g., as depicted in Fig. 4) constitute a protected network consistent with the "*protected network*" of the 460 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.1005, [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.1005, [0017] (explaining that the above techniques can be used such 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.").

68. Krantz discloses network access protocols whereby "[a] server includes the **functionality to authorize clients to access a second network** …" Ex.1005, [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.1005, [0016].

69. 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").

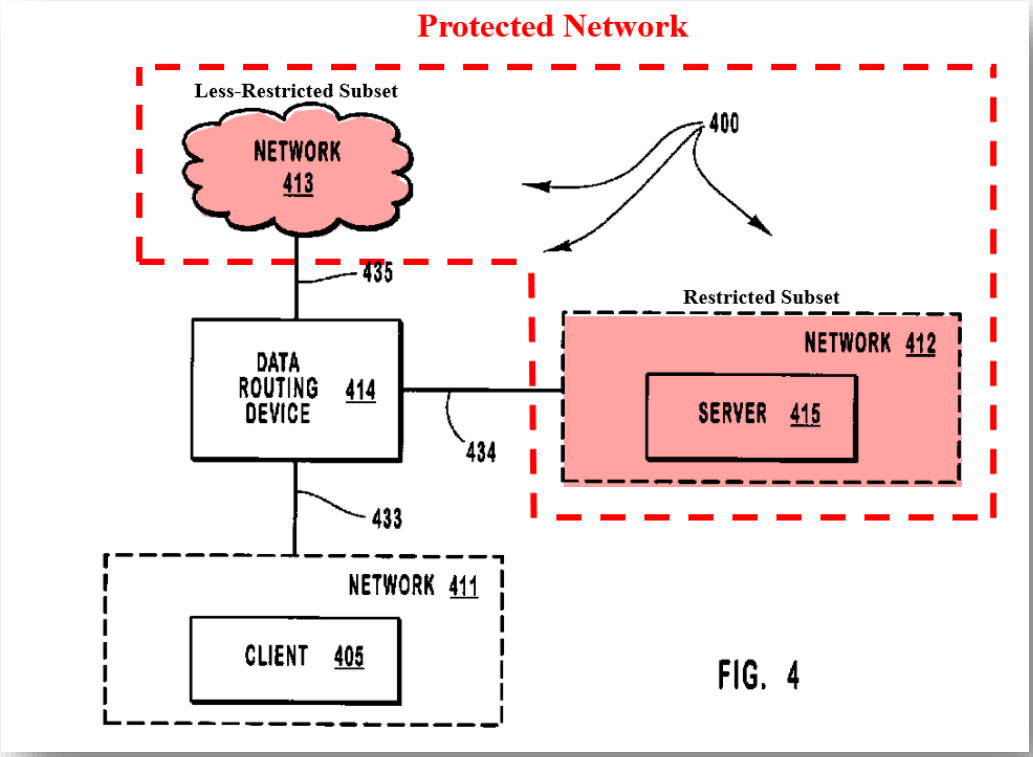
Ex.1005, [0038].

70. 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.1011, 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.1012, 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."). Similarly, Krantz explains that

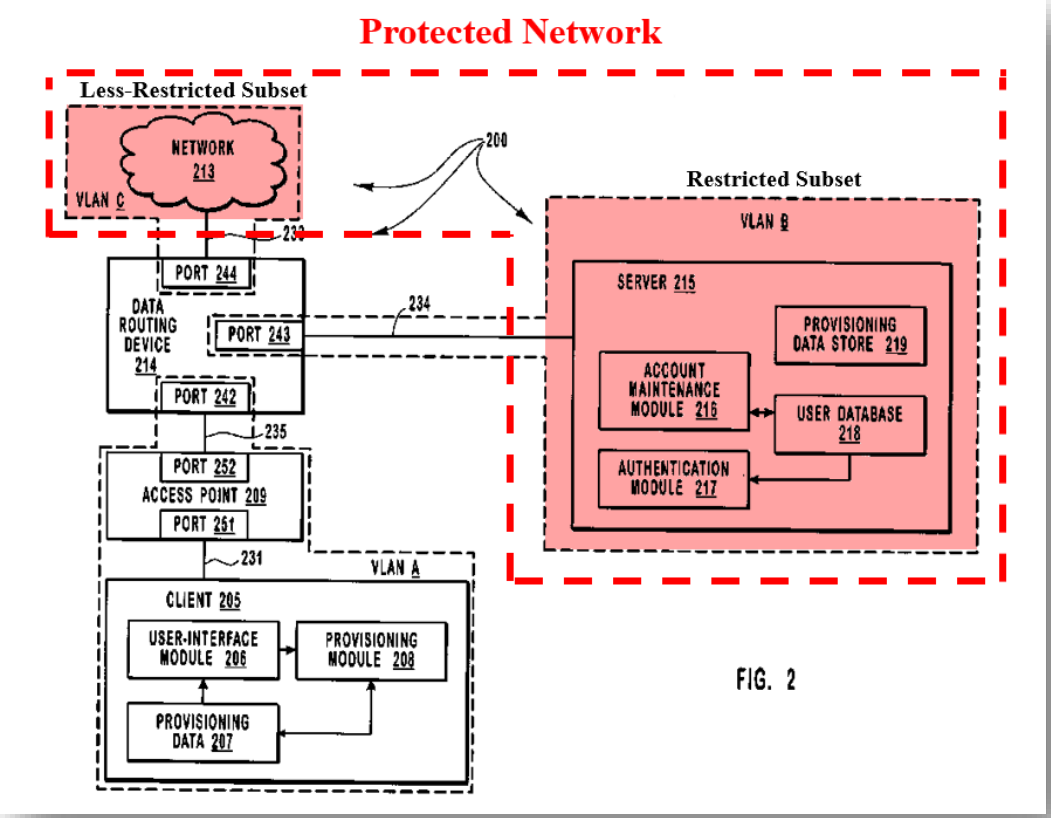
"[l]ogical communication links **can include hardwired links, wireless links, or a combination**" thereof. Ex.1005, [0038]

71. The 460 Patent describes some of the "*protected network's*" characteristics. For example, the 460 Patent explains that a "*protected network*" may be "**physically or logically divided** into a restricted subset and one or more less-restricted subsets." Ex.1001, 2:52-54. The 460 Patent also explains that such restricted and less-restricted subsets "are typically characterized by Virtual Local Area Networks (e.g., VLANs)," (Ex.1001, 2:66-3:4), and further explains that the "*protected network*" may include "access restrictions." Ex.1001, 6:21-33.

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



Ex.1005 (Krantz), Figure 4 (annotated)



Ex.1005 (Krantz), Figure 2 (annotated).

73. 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.1005, 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.1005, [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.1005, [0057]. Figure 2 and its description thus provide certain specific techniques to be implemented in Krantz's networking architecture. *See generally* Ex.1005, Figures 2 and 4 and related descriptions. Accordingly, and as depicted above, the combination of Network 413 and Network 412 (also annotated as VLAN C and VLAN B) constitute a single logical "*protected network*." Given the near similarity in disclosure between the embodiment described in Figure 2 and the 460 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.

74. To the extent the "*protected network*" is required to be a single network, Krantz explains that its "*access*" control techniques can also be used "**within a single network**." Ex.1005, [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.1005, [0055].

75. As Krantz explains, the disclosed system "**may authorize the client for at least partial access to the single network**" ("*a method of granting*

access"), and as explained in more detail below, one example of "*granting*" such "*access*" in Krantz is "by authorizing client access to selected computer systems or modules on the single network." Ex.1005, [0017]; *see also* Ex.1005, [0016], [0071] [0074]-[0076], e.g., [0068] ("[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C**.") *see also* Ex.1005, [0104], [0107]-[0109].

76. Accordingly, Krantz discloses "[*a] method of granting access to a protected network*."

b. [1.1] receiving a request for access to a less-restricted subset of the protected network from an access device,

77. Krantz discloses a client 205 (i.e., "*access device*") that "*requests [] access to a less-restricted subset of a protected network*."

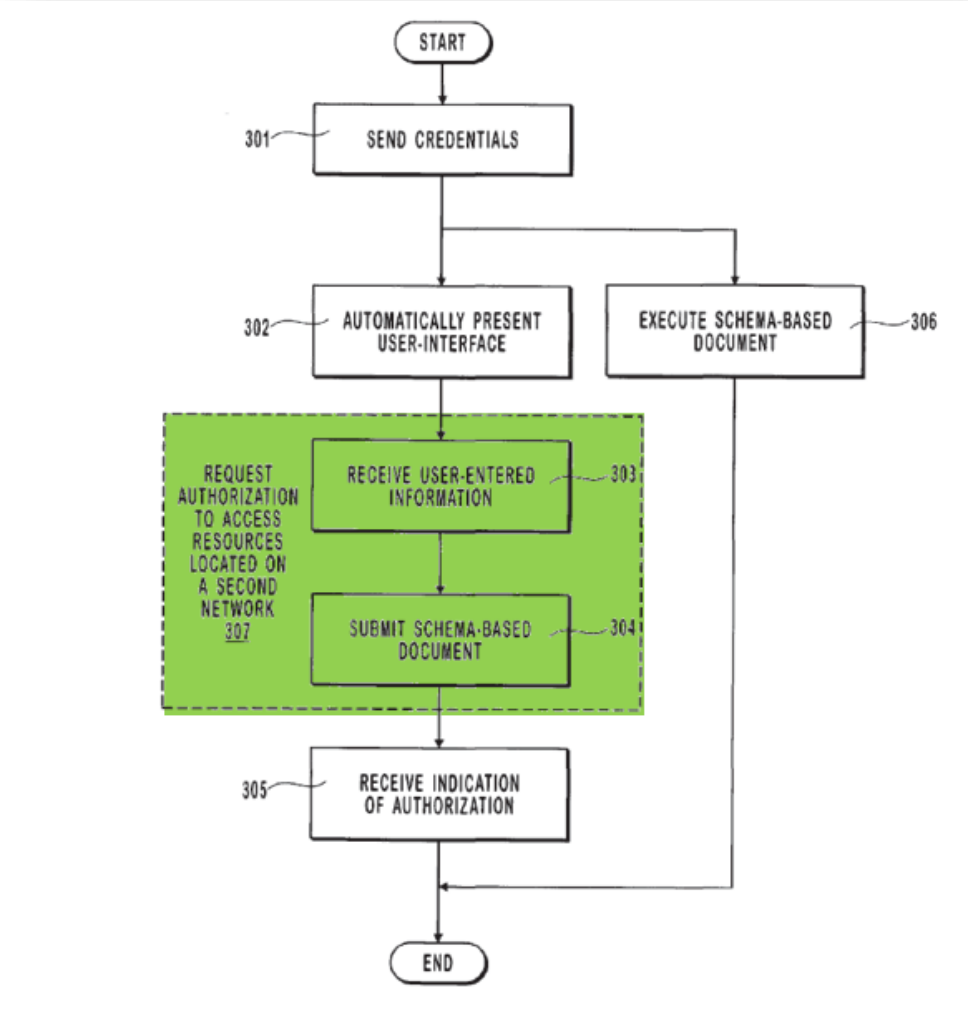
78. For example, Krantz discloses that "a server has the functionality to authorize access" to a network and/or selected elements within a network after the client 205 ("*access device*") sends credentials to the server ("*receiving a request.*") *See, e.g.*, Ex.1005, [0016], [0071]. Krantz discloses that the "server (**based at least in part on received credentials**) may authorize the client for at least partial

access to the single network." Ex.1005, [0017]; *See also* [0068]-[0076], [0099], [0104], [0107]-[0109] (collectively describing techniques for requesting access in a VLAN environment).

79. 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.1005, [0018]. Other credentials provided by Krantz's "*access device*" may include, for example, "user-identifier[s] and password[s]." Ex.1005, [0076].

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.1005, [0070]. Krantz discloses that "the method 300 includes a functional, result-oriented step for **requesting authorization** (*i.e., "receiving a request"*) **to access resources located on a second network (step 307)"** (*i.e., "to a less-restricted subset of the protected network")*. Ex.1005, [0104]; *see also* Ex.1005, [0071] (describing the client sending credentials to server to authenticate). Krantz further explains that "**[s]tep 307** may include any

corresponding acts for accomplishing the result of requesting authorization to access resources located on the second network." Ex.1005, [0104].

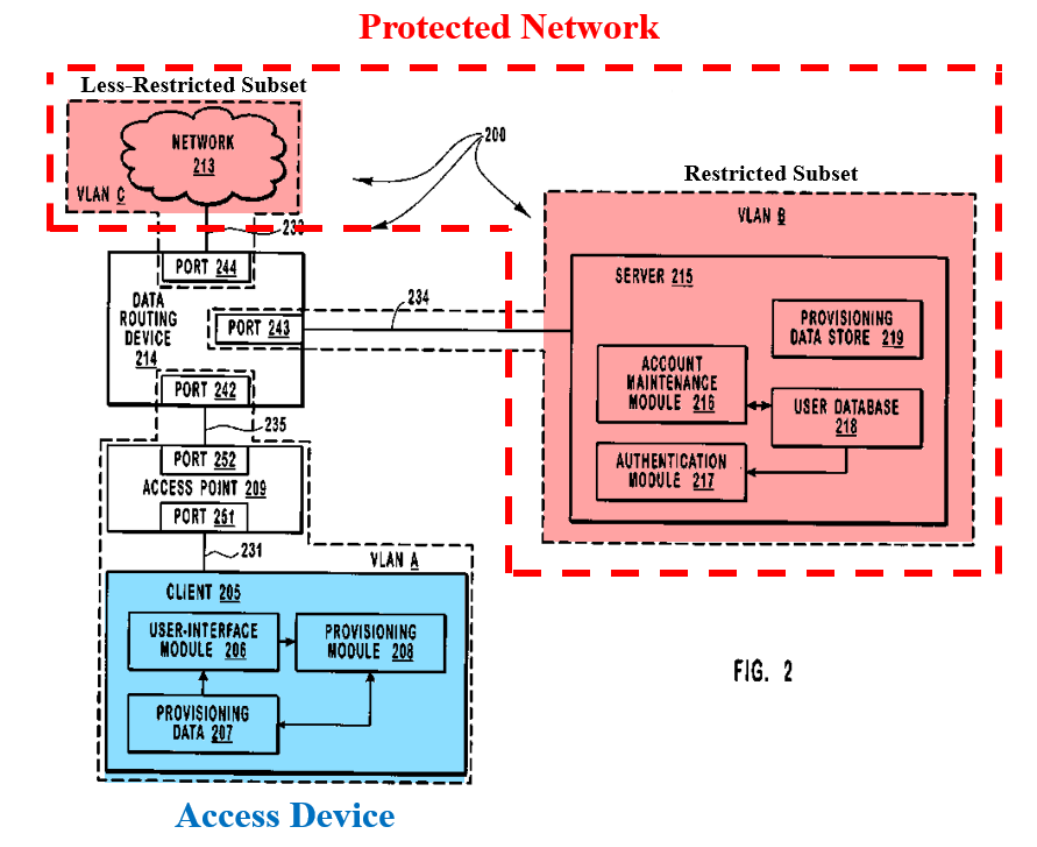


Ex.1005 (Krantz), Figure 3 (annotated)

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." Ex.1005, [0104].

82. The "*access device*"—*i.e.,* "Client 205"—making the "*request*" in Krantz is depicted in Figure 2 in blue and annotated below:



Ex.1005 (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 "*protected network*." Krantz discloses that "[b]ased on [client] credentials, "the server **may**

authorize the client for at least partial access to the second network [*i.e.,* VLAN C] **and/or may deny access to the second network** and authorize the client for at least partial to access to the first network" (*i.e.,* "*a request for access to a less-restricted subset of a protected network.*") Ex.1005, [0016]; *see also* Ex.1005, [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.1005, [0104].

84. In Krantz, the "second network"—*i.e.,* VLAN C—is a "*less-restricted subset of a protected network*" because it provides "full access to [its] resources" to authorized users, *see* Ex.1005, [0019]—precisely as the "*less-restricted subset of a protected network*" is described in the 460 Patent. For example, the 460 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.1001, 5:43-45. Put another way, the "*less-restricted subset of a protected*

network" as described in the 460 Patent provides greater access to elements and/or resources than the "*restricted subset*[7]."

85. Accordingly, Krantz discloses "*receiving a request for access to a less-restricted subset of the protected network from an access device*."

c. [1.2] the request received through a communication port of an access point,

86. Krantz discloses that "*the request is received through a communication port of an access point*."

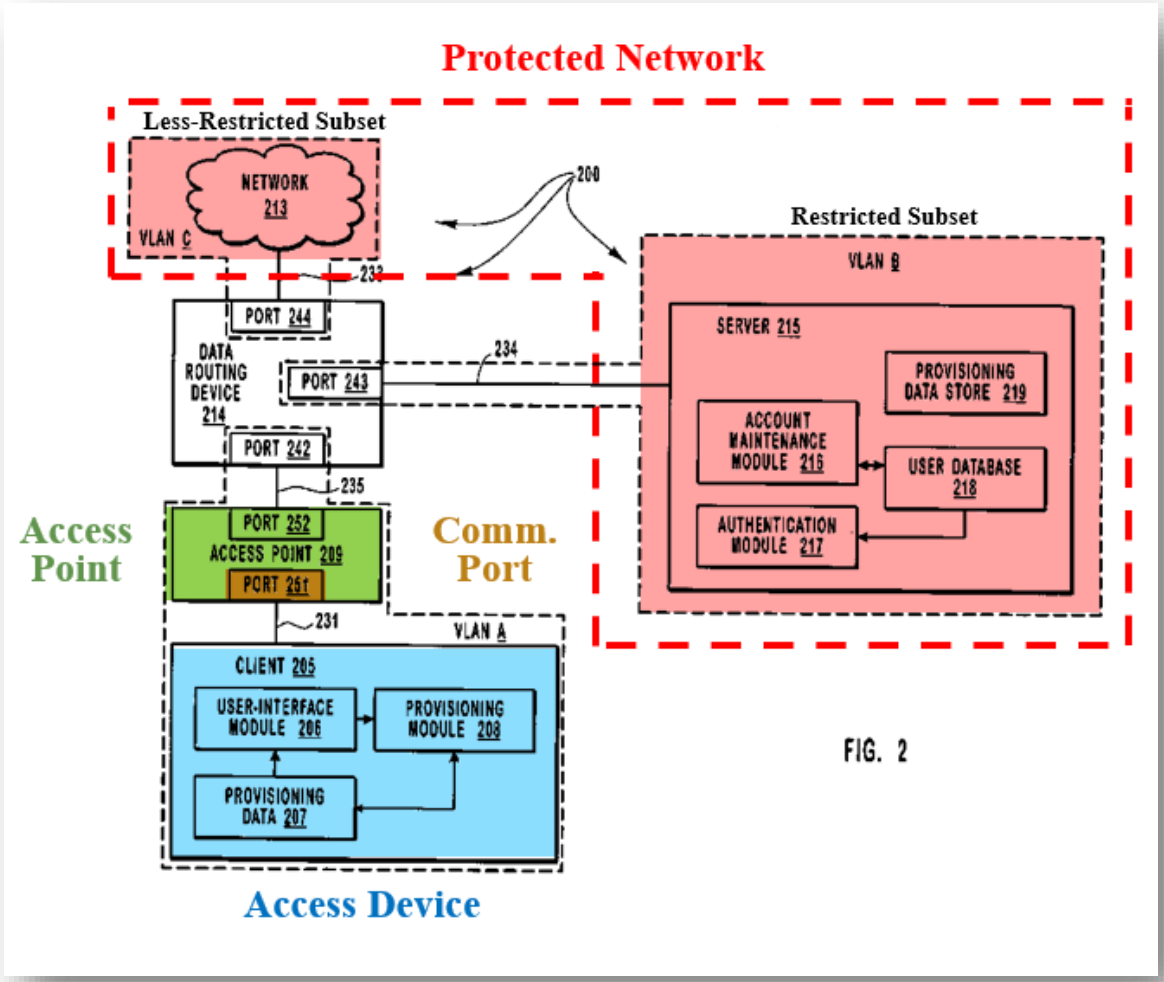
87. As explained above, *see* §X.A.1.b, Krantz discloses "*a request for access to a less-restricted subset of a protected network*" because client 205 requests authorization to access resources on the second network and "*less-restricted subset", i.*e., VLAN C.

88. The 460 Patent explains that "Access Point 215 is, for example, a network switch, a wireless access point, a remote access virtual private network (VPN), secure socket layer VPN, firewall, or the like. When embodied in a network switch, Access Point 215 includes a series of communication ports . . . configured for communication with devices such as Access Device 230, Router

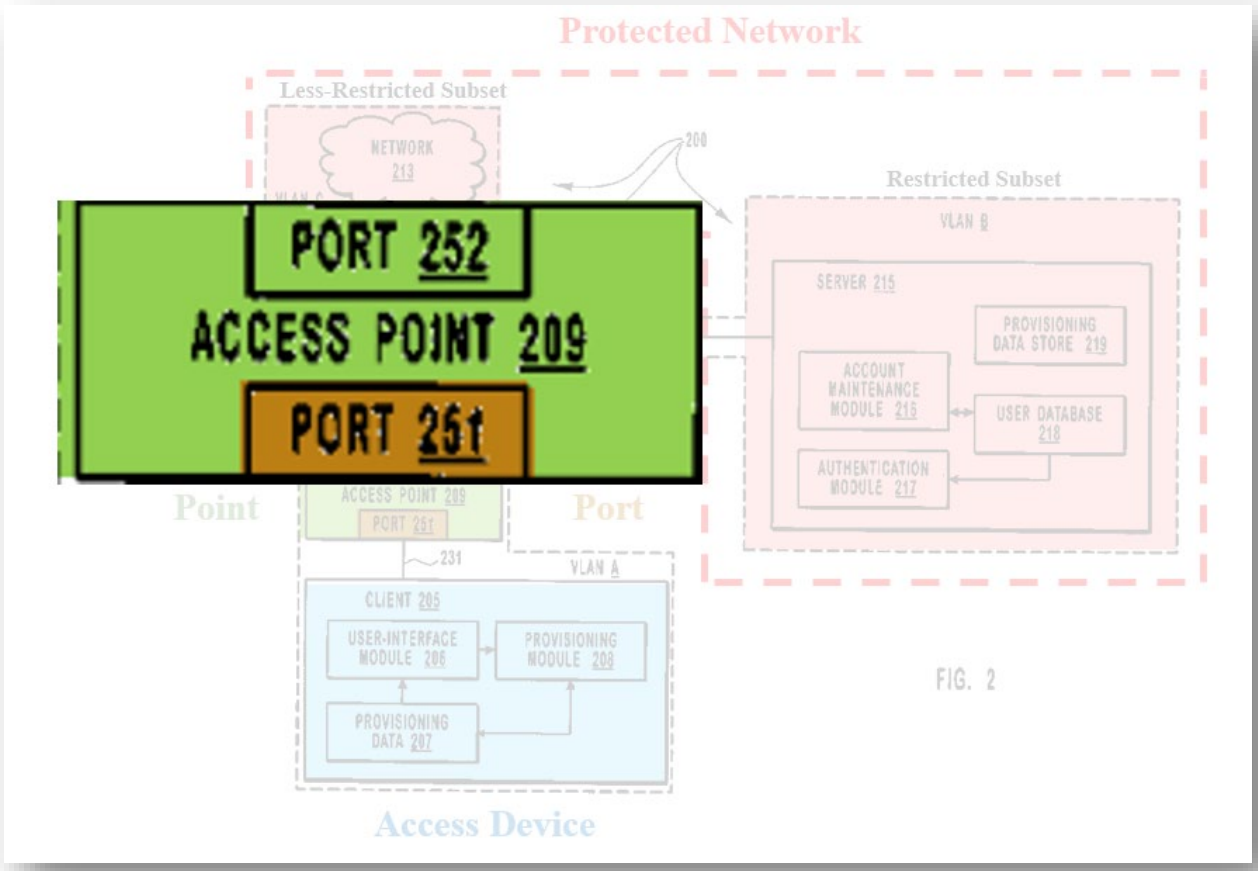
[7] As described in greater detail below, the "*restricted subset*" of Krantz's "*protected network*" is the first network, *i.e.*, VLAN B.

220, Less-Restricted Subset 210 and/or Restricted Subset 205." 460 Patent, 7:57-65.

89. As in the 460 Patent, Krantz's request is received through a "*communication port*"—annotated in brown as "Port 251"—of an "*access point*"—annotated in green as "Access Point 209," as depicted below in Figure 2:

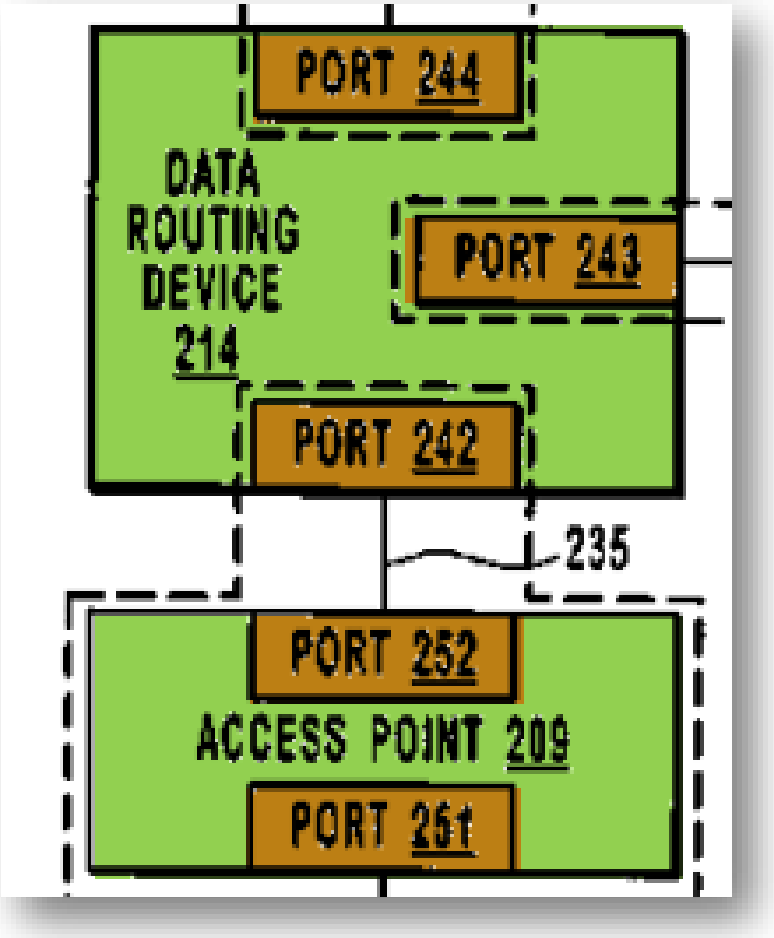


Ex.1005 (Krantz), Figure 2 (annotated)



Ex.1005 (Krantz), Figure 2 (annotated and focused).

90. Alternately, the claimed "*access point*" can be Routing Device 214 in combination with Access Point 209, as I discuss in detail below detail below with respect to limitation [1.3] (Mapping #3), in which the claimed "*communication port*" is port 251 in combination with ports 252 and port(s) 242, 243, and/or 244.



Ex.1005, Figure 2 (annotated).

91. Accordingly, Krantz discloses that "*the request is received through a communication port of an access point*."

d. [1.3] the communication port configured for communicating between the access device and a restricted subset of the protected network,

92. Krantz discloses "*the communication port configured for communicating between the access device and a restricted subset of the protected network*."

93. Initially, the 460 Patent explains that "[a] communication port of the access point is configured such that network traffic directed at the protected network is initially passed through a restricted VLAN rather than through a less-restricted VLAN." Ex.1001, 3:8-11. The 460 further explains that "[if] the device requesting access satisfies requirements of the security policy, then the gatekeeper sends commands to the access point in order to reconfigure the communication port through which the access request was received." Ex.1001, 5:45-49.

94. Krantz discloses claimed functionality in several ways.

95. *First*, Krantz explains that "[a]ccess point 209 can be a wired or wireless access point **that facilitates communication between client 205 and data routing device 214.** As depicted in network architecture 200, access point 209 is connected to client 205 by corresponding logical communication link 231. … Access point 209 includes ports 251 and 252. **Data can be transferred between access port [sic][8] 209 and client 205 through port 251**. **Likewise, data**

[8] Typo in original. "Access port 209" should refer to "Access **Point** 209."

can be transferred between access point 209 and data routing device 214 through port 252." Ex.1005, [0063].

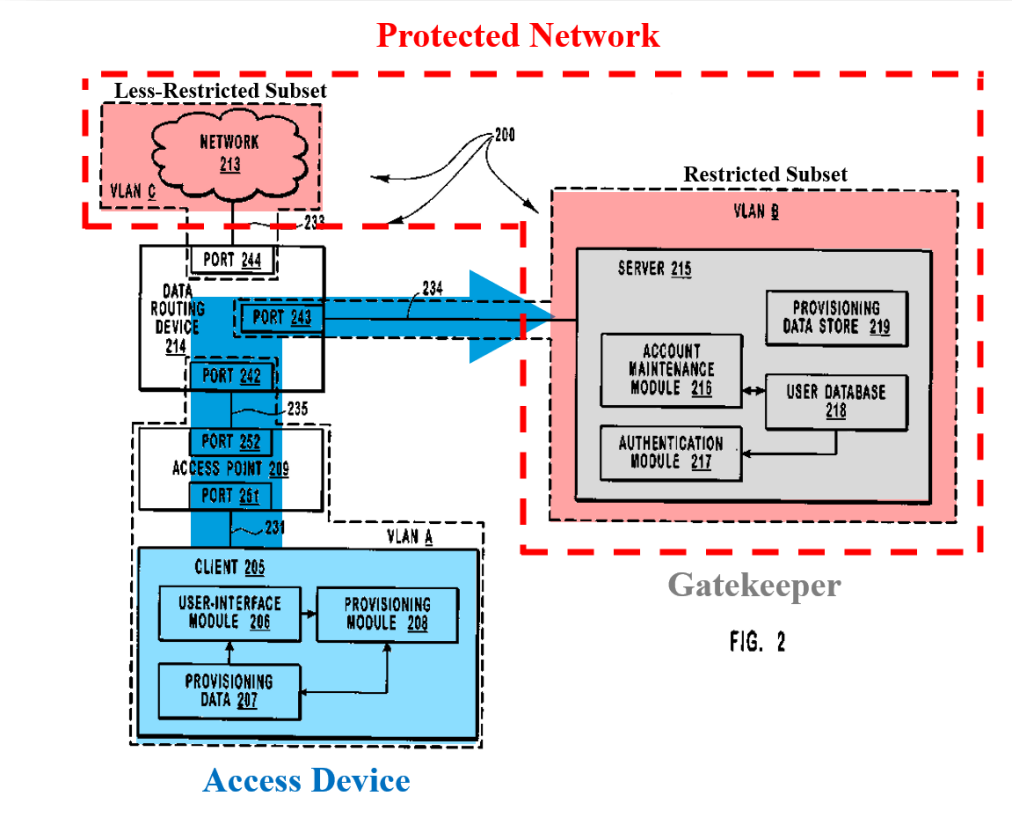
96. Krantz further discloses that "access point 209" (*i.e,* "*access point*") is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213)." Ex.1005, [0064]. Thus, "port 251" (*i.e.,* "*the communication port*") is "*configured for communicating between the access device and restricted subset of the protected network"* because it facilitates the transfer of data between client 205 ("*the access device*") and, ultimately VLAN B (the "*restricted subset of the protected network*.") Ex.1005, [0063]-[0064].

97. *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.1005, [0064]. Krantz is therefore explaining that when configured as a "VLAN aware device," Krantz's Port 251 (*i.e,* the "*communication port*") "*is configured for communicating between the access device and a restricted subset of the protected network*" because Access Point 209 configures Port 251 to insert VLAN Tag Headers into incoming data frames from a client that may only access VLAN B, *i.e*., the "*restricted subset*." Ex.1005, [0064]; Ex.1003, ¶124; *see also* Ex.1005, [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). Configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1007 (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.1008 (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.1009 (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.1010 (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.").

98. The communication path "*between the access device and a restricted subset of the protected network*" is depicted in Figure 2, which I have annotated in blue below:

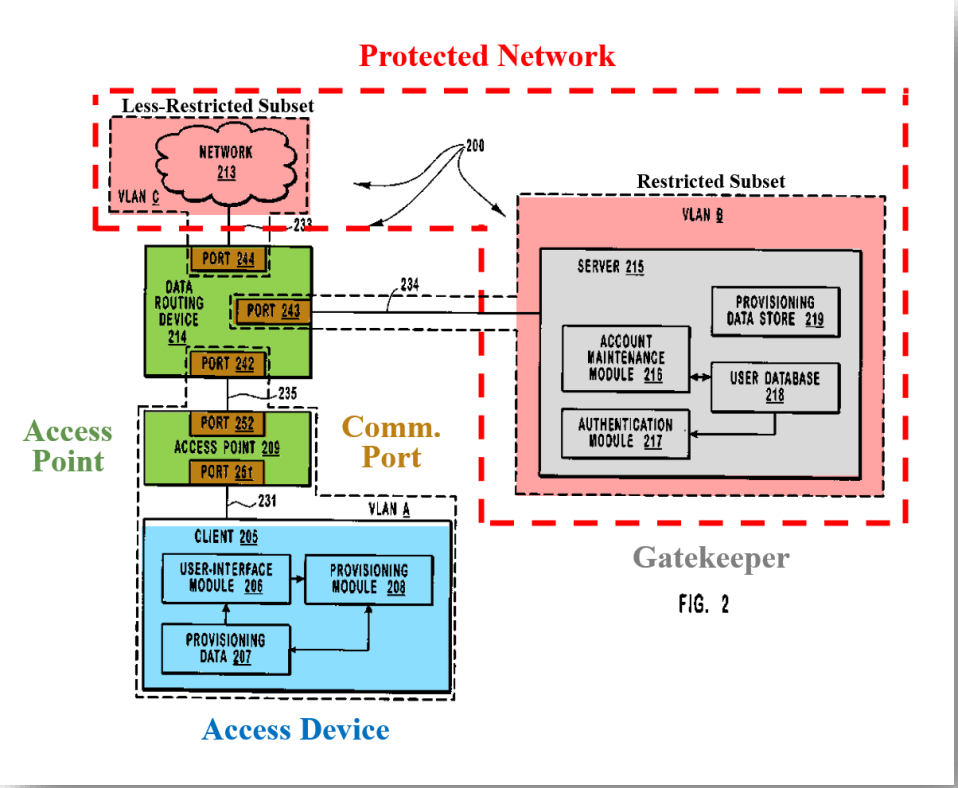


Ex.1005 (Krantz), Figure 2 (annotated)

99. Accordingly, Krantz discloses "*the communication port configured for communicating between the access device and a restricted subset of the protected network.*"

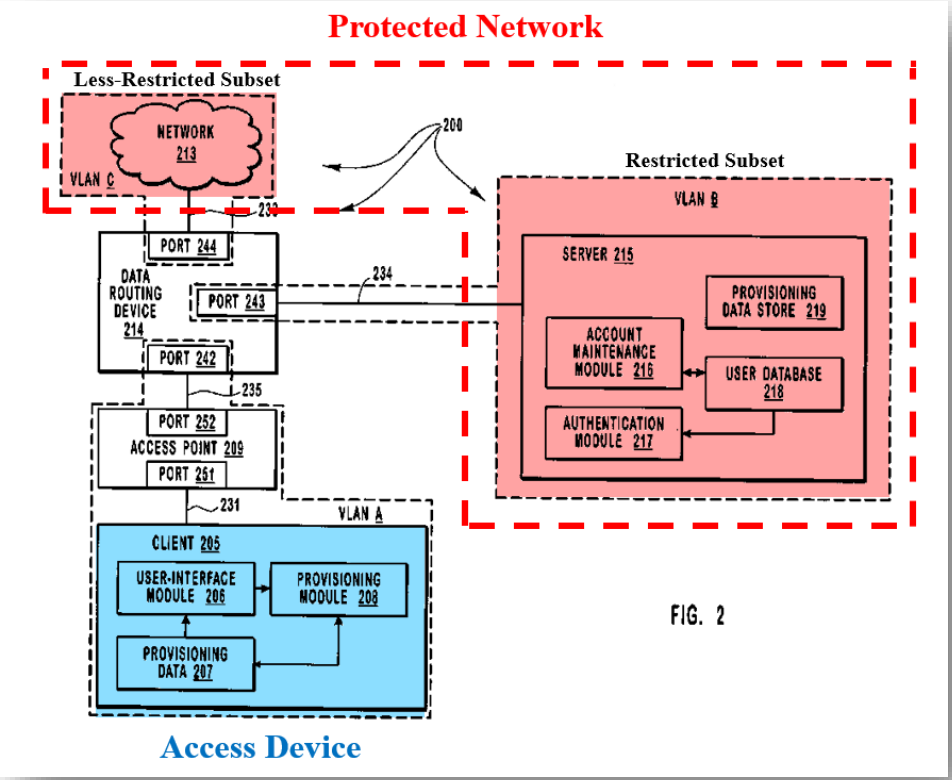
100. To the extent one may assert that Krantz does not expressly disclose the claimed "*the communication port configured for communicating between the access device and a restricted subset of the protected network*," it would have been obvious to implement other "*configur[ation]*" techniques in view of Krantz itself.

101. 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.1005, [0060]. As seen below, the claimed "*communication port configured for communicating between the access device and a restricted subset of the protected network*" can be considered to be port 251 in combination with ports 252, 242, and 243 (port 244 connects to the less-restricted subset in Fig. 2).



Ex.1005 (Krantz), Figure 2 (annotated).

102. 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.1005, [0061]. VLAN's B and C are depicted below for reference.



Ex.1005 (Krantz), Figure 2 (annotated)

103. 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].

104. 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.1005, [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").

105. 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:

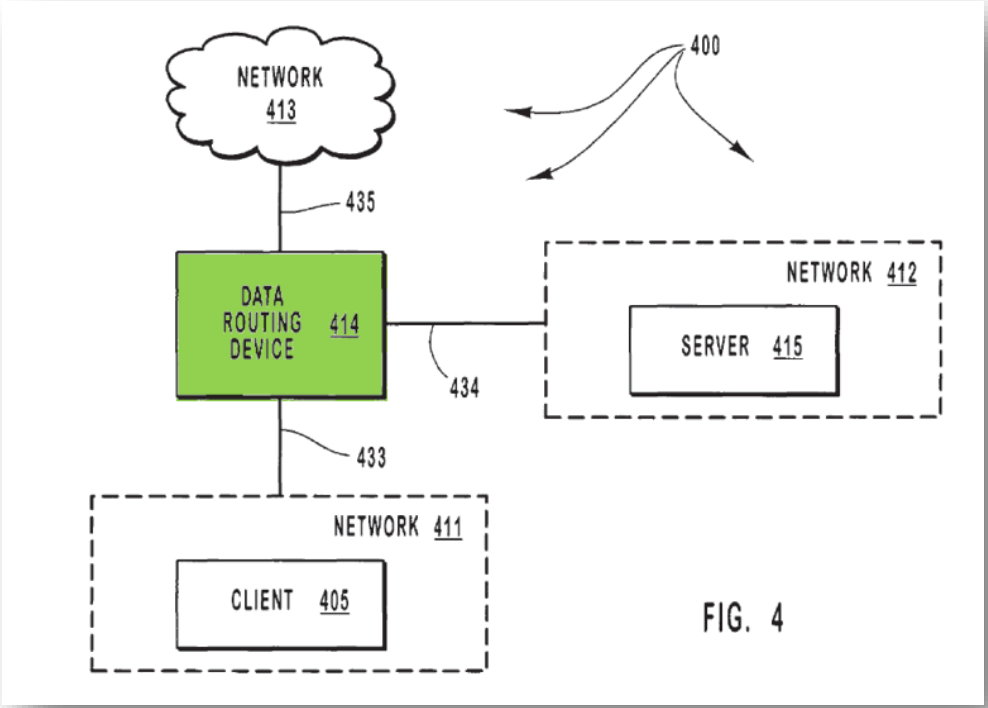


FIG. 4

106. 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.1005, [0051] (emphasis added).

107. 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.1005, [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.1005, [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.1005, [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 and any POSITA would have had a reasonable expectation of success in implementing this technique.

108. 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 immediately above.

109. Accordingly, Krantz renders obvious "*the communication port configured for communicating between the access device and a restricted subset of the protected network*" for this additional reason as well.

e. [1.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and

110. Krantz discloses "*the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and*."

111. As discussed with respect to limitations [1.1] and [1.2], the client makes a "*request*." Moreover, the Abstract of the 460 Patent notes that "[t]he

gatekeeper[9] is configured to enforce a security policy … before granting access to a less-restricted subset of the computing network." Ex.1001, Abstract.

112. Krantz similarly discloses that "[a] client attempts to become authorized to access resources located on a second network … [and] sends credentials to an access point that is communicatively coupled to a server (located on a first network or located on the second network) that can authorize access to the second network." Ex.1005, [0031]. This can generally be observed with respect to Fig. 2, which I will discuss below.

[9] Notably, Applicant admits that this Gatekeeper is prior art. *See*, Ex.1001, 2:30-32 ("GateKeeper … [is] practiced in the prior art.").

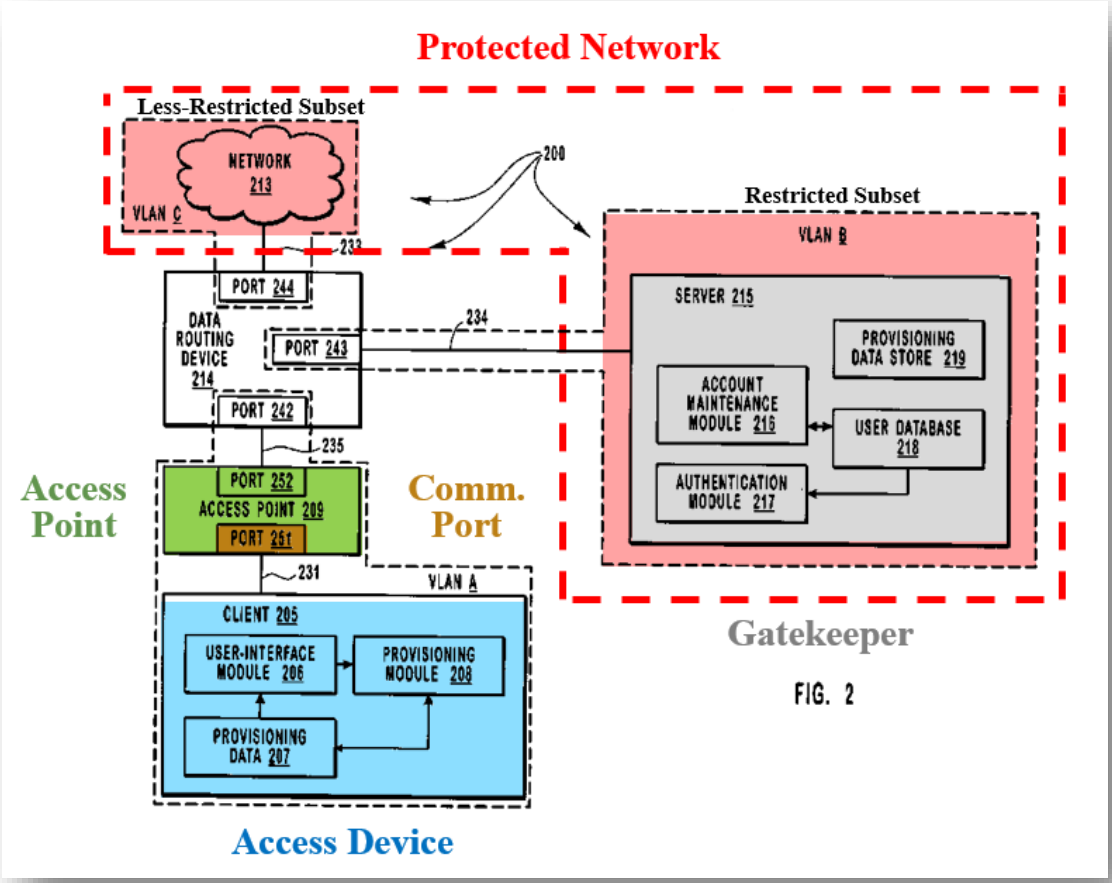


FIG. 2

Ex.1005 (Krantz), Figure 2 (annotated)

113. Furthermore, with respect to the Gatekeeper (depicted above as Server 215), Krantz discloses "*applying a security policy*." As an initial matter, the 460 Patent explains that "the security policies may include requirements for user identification[10] such as usernames and passwords, configuration requirements

[10] Krantz's disclosure of "User Identification" as part of "*applying a security policy* . . . " is described in detail in claim 2 below.

relating to the configuration of Access Device 230 application requirements relating to applications running on Access Device 230, or the like." Ex.1001, 6:40-45

114. Krantz discloses several specific examples of "*applying a security policy to the access device in response to the request.*" 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.1005, [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 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.1005, [0068]. The use of EAP-TLS (*e.g.*, Ex.1005, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1016 [RFC2716] at 1; *see also*, Ex.1016 [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**.")

115. 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.1005, [0099].

116. Krantz also explains that both EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization. Ex.1005, [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.1017, 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.")

117. Furthermore, Krantz discloses "*using the gatekeeper to determine if requirements of the security policy are satisfied by the access device*." In particular each of the techniques described above would involve server 215 ("*gatekeeper*") authenticating the client device in order to authorize it to access the protected network. Ex.1005, [0068]-[0074] (describing transferring client authentication information to authentication module 217); *see also* Ex.1005, [0067]-[0074], [0099]-[0100] (describing the use of EAP). Based on the information exchanged a "*determin[ation]*" is made if the client 205 ("*access device*") has satisfied the requirements of a security policy—*i.e.,* whether the "*access device*" is authenticated and therefore authorized "*for access to a less-restricted subset of the protected network.*" Ex.1005, [0068], [0071], [099].

118. Accordingly, Krantz discloses "*the restricted subset including a gatekeeper; applying a security policy to the access device in response to the*

request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and."

f. [1.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied.

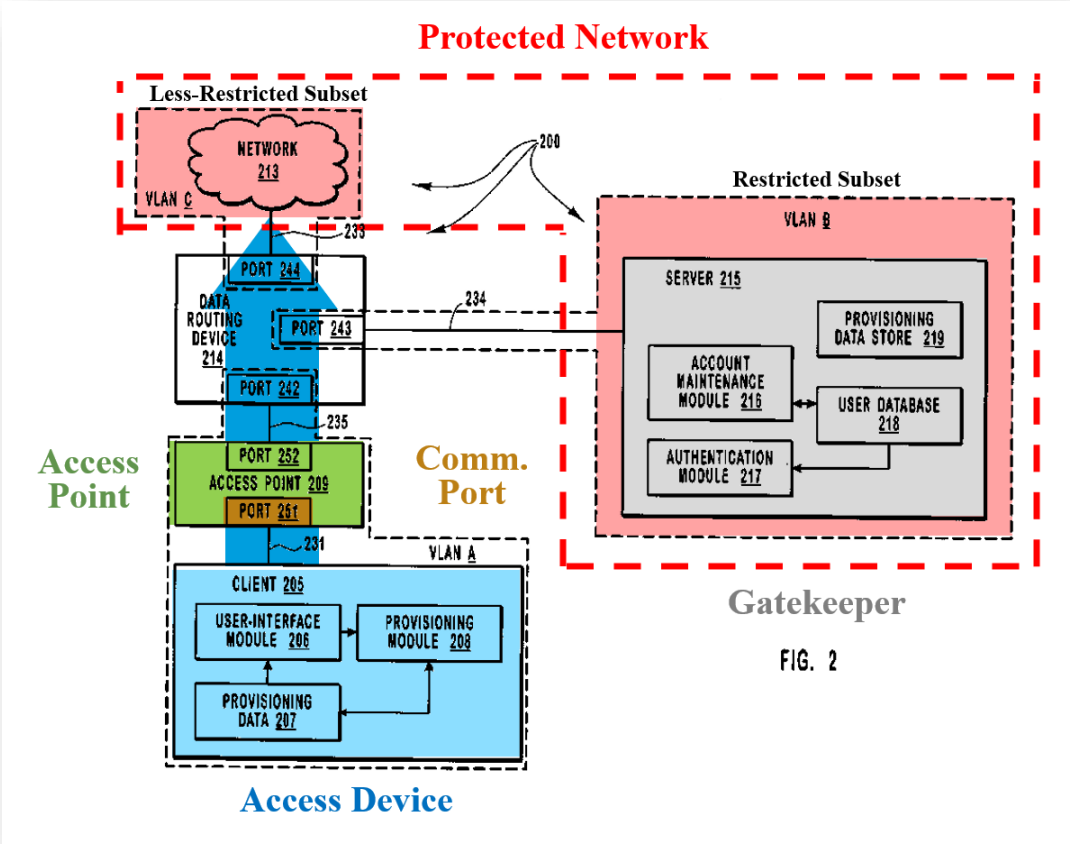
119. Krantz discloses "*reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied*."

120. Krantz discloses that "access point 209" (i.e, "access point") is a wireless access point that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213)." Ex.1005, [0064].

121. As explained in Krantz, "if an authenticated user of client 205 is authorized to access resources located **on VLAN C** (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C." Ex.1005, [0076]. As explained above, Krantz discloses utilizing other security policies including the use of user-identifiers and passwords. Ex.1005, [0076] ("[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare

the credentials to entries in user database 218."). Krantz explains that after the client is authenticated ("*the requirements of the security policy are satisfied,"*) *see* claim [1.4] , "client 205 can then be authorized to access resources located on VLAN C." Ex.1005, [0076]; *see also* Ex.1005, [0031]. Krantz discloses the functionality in several ways.

122. *First*, "port 251" (i.e., "*the communication port*")—after the "requirements of the security policy are satisfied"—facilitates the transfer of data between client 205 ("*the access device*") and, ultimately VLAN C ("the less-restricted subset of the protected network without passing the data through the gatekeeper." Ex.1005, [0063]-[0064]. Port 251 is "*reconfigured*" because it was previously configured to only transfer data to VLAN B for the reasons described above. *See* § IX.A.1.d. That path is depicted below—which would include transferring data "without passing the data through the gatekeeper," i.e., "authentication module 217."



Ex.1005 (Krantz), Figure 2 (annotated).

123. *Second*, Krantz explains that "[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C." Ex.1005, [0064]; *see also* Ex.1005, [0061]. 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.1005, [0023] (emphasis added).

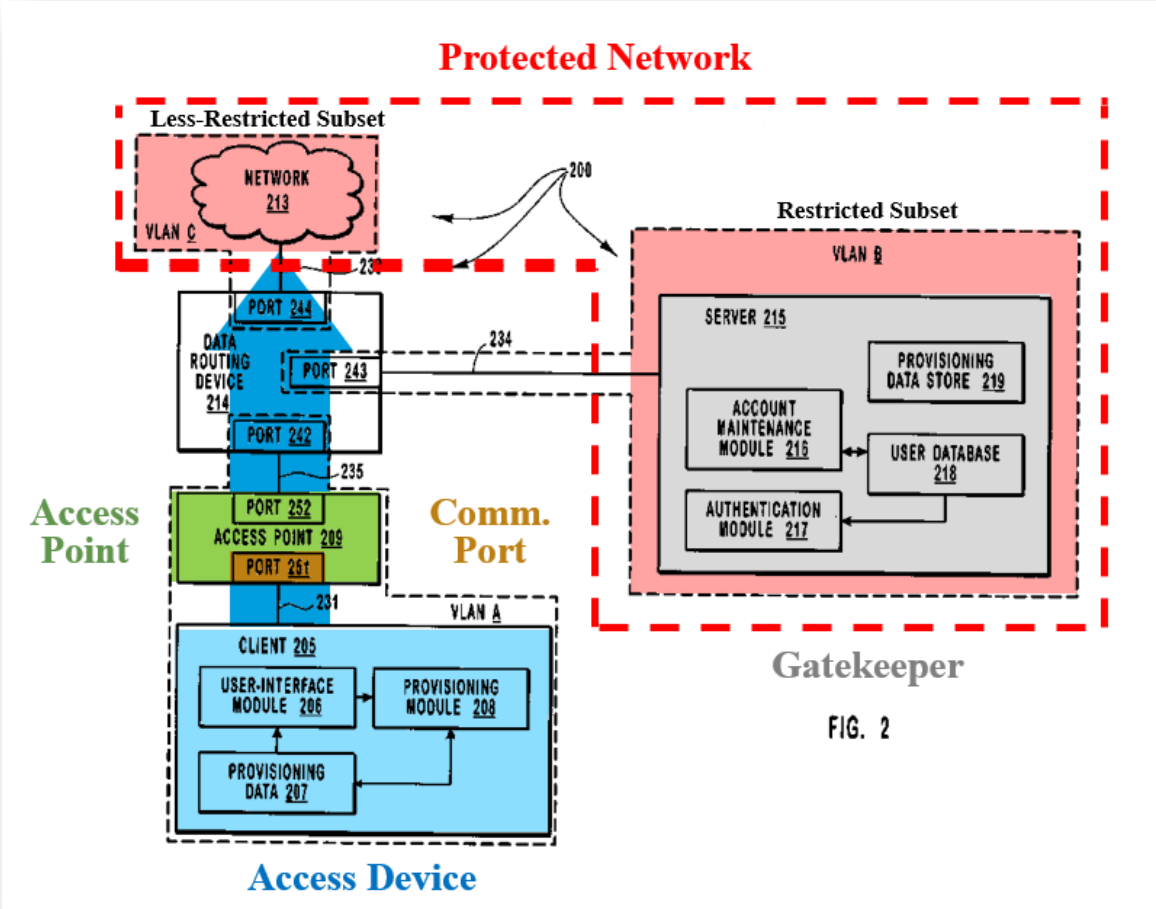
124. Krantz is therefore explaining that when configured as a "VLAN aware device," Krantz's "access point" is "reconfiguring the communication port [i.e., Port 251 of Krantz] for communicating data between the access device and the less-restricted subset of the protected network " because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client **that may now access VLAN C**, i.e., the "less-restricted subset." Ex.1005, [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 has "reconfigured" Port 251 to tag incoming data for transfer to VLAN C rather than VLAN B.

125. 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." As already explained above, configuring input ports in VLAN aware devices to tag

incoming data was a well-known technique to POSITAs by 2003. Ex.1007 (IEEE 802.1Q), 11 (Table 5-1) (explaining 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.1008 (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.1009 (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.1010 (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.").

126. Krantz also discloses that data is communicated in its system from authorized clients "*without passing the data through the gatekeeper, when the requirements of the security policy are satisfied*."

127. Again, with reference to Figure 2 (below), the "*gatekeeper*" (server 215) in Krantz is shown in gray, while the "*access point"*—including Access Point 209—is shown in green with "communication port[s]" shown in brown. Upon a client's authorization, data flows directly from "client 205" to VLAN C—i.e., it does not flow through the "*restricted subset*" (VLAN B) or the "*gatekeeper*." Ex.1005, [0059], [0064], [0107] (describing the way data is transferred in the Krantz system).



Ex.1005 (Krantz), Figure 2 (annotated)

128. Krantz explains 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, and C.** Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2." *Id.* at [0060]; *see also*, e.g., *id.* at [0064] ("Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames

received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C."). Accordingly, by configuring the flow of data in this manner, the "*gatekeeper*" (server 215) need only apply security policies to authorize the access device access to data—such as the resources on VLAN C—but not actually have data pass through it. Ex.1005, [0062] (Any of the ports included in data routing device 214 (e.g., ports 242, 243, and 244) can be configured to transfer tagged data frames but drop untagged data frames.").

129. *Lastly*, and as demonstrated above, an access device can be authenticated in a variety of ways, including exchanging a user-identifier and password, EAP-messages to pass certificate keys, as well as cipher suites. *See,* Ex.1005, [0074]. "When [the] credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). **If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.**" *Id.*, [0076]. Thus, a POSITA would understand that the reconfiguration of a communication port (*id.*, [0053]) occurs when the

requirements of the security policy are satisfied, and the data need not pass through the gatekeeper (*id.*, [0060], [0064]). In particular, based on Krantz's disclosure, the communication path for an authorized "*access device*" would flow through "*communication port*" 244, as depicted in the annotated figure above in blue.

130. Accordingly, Krantz discloses "*reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied*."

131. In addition, to the extent one may assert that Krantz does not disclose "*reconfiguring the communication port*"—*i.e.,* Port 251 on Access Point 209—it would have been obvious to do so based on Krantz itself for the reasons already explained above. *See* §IX.A.1.d. For example, as already explained, it would have been obvious to combine the functionality of the Data Routing Device and Access Point of Krantz in the same device.

132. In such a combined device, as Krantz explains, "when a portion of data, such as, for example, a data frame, is transferred in at a first port . . . **based on configuration rules**, that the frame is to be transferred out at a second port (e.g., port 243). For example, data routing device 214 can determine that a data frame received from access point 209 is to be sent to server 215. **It may also be that a data frame is transferred in and out of data routing device 214 at the**

same port." Ex.1005, [0059]. The combined device would be further enabled to "*reconfigure*" as necessary the "*communication port*" for transfer of data from an authenticated client to VLAN C. Ex.1005, [0060] ("Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2."); Ex.1005, [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.").

133. Accordingly, Krantz discloses or renders obvious "*reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied*" for this additional reason as well.

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

2. Claim 2

a. [2.0] The method of claim 1, further comprising authenticating a user of the access device.

135. Krantz discloses this limitation for the same reasons I discuss above with respect to claim limitation [1.4]. For instance, Krantz discloses that "[w]hen credentials are sent to server 215, authentication module 217 can receive the credentials **(e.g., user-identifier and password)** and compare the credentials to

entries in **user database** 218. If credential information matches an entry in user database 218, **the identity of a user is authenticated** (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 [i.e., the user of the access device] is authorized to access resources located on VLAN C (e.g., **the user is up to date on payments for their account**), client 205 can then be authorized to access resources located on VLAN C." *See also* Ex.1005, [0074] (describing using EAP to authenticate user, including through exchange of "certificates, keys, and supported cipher suites." Ex.1005, [0076].

136. Accordingly, Krantz discloses "[t*]he method of claim 1, further comprising authenticating a user of the access device*."

3. Claim 3

a. [3.0] The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.

137. To the extent that Krantz does not expressly disclose "*obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy*," it would have been obvious in view of Herrmann.

138. A POSITA would have been motivated to combine Krantz with Herrmann for the reasons described above. *See* § VIII.C. In particular, 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. 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.1005, [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.1005, [0076].

139. A POSITA would recognize that checking for anti-virus software would merely be an additional item for authentication module 217 (*i.e.,* the "*gatekeeper*") to check in the authentication process already disclosed by Krantz. Like Krantz, Herrmann discloses that a "policy server 460 [which] may enforce a variety of different types of security policies or rules." Ex.1006, [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). Moreover, 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.1005, [Abstract].

140. Krantz's authentication module, which compares the credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would additionally compare a virus protection program on an access device against approved antivirus programs ("*using the system data to determine that the access device satisfies the requirements of the security policy*"). Information regarding approved antivirus software and approved connected devices could be stored in the User Database or an additional Database could be added. *See, e.g.,* Ex.1005, Fig 2 (and corresponding description). A POSITA would have had a reasonable expectation that this additional provision would be successful because Krantz already discloses conditions for client access, such as "signup" or "renewal" conditions to authorize access to network resources. Ex.1005, [0019].

141. Accordingly, Krantz in view of Herrmann discloses *"[t]he method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy*."

4. Claim 4

a. [4.0] The method of claim 3, wherein the system data includes antivirus software status.

142. Claim 4 is obvious over Krantz in view of the disclosures in Herrmann. 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].

143. 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.1005, [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.1006, [0079], although Krantz does not explicitly mention antivirus software as the kind of "*system data.*" However, it would have been obvious in view of Herrmann for the reasons already stated above with respect to claim 3.

144. 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.1006, [0012].

145. 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 (i.e., confirming the "*antivirus software status*"). *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**."). In other words, checking "*system data*" to confirm the "*status*" of required "*antivirus software*" on the "*access device*."

146. As discussed with respect to claim 3, 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.1005, [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.1005, [0019]. Requiring the client to update antivirus software would merely be an additional condition.

147. Accordingly, Krantz in combination with Herrmann renders obvious "*[t]he method of claim 3, wherein the system data includes antivirus software status*."

5. Claim 5

a. [5.0] The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and

148. Claim 5 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 system 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 5.

149. The 460 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

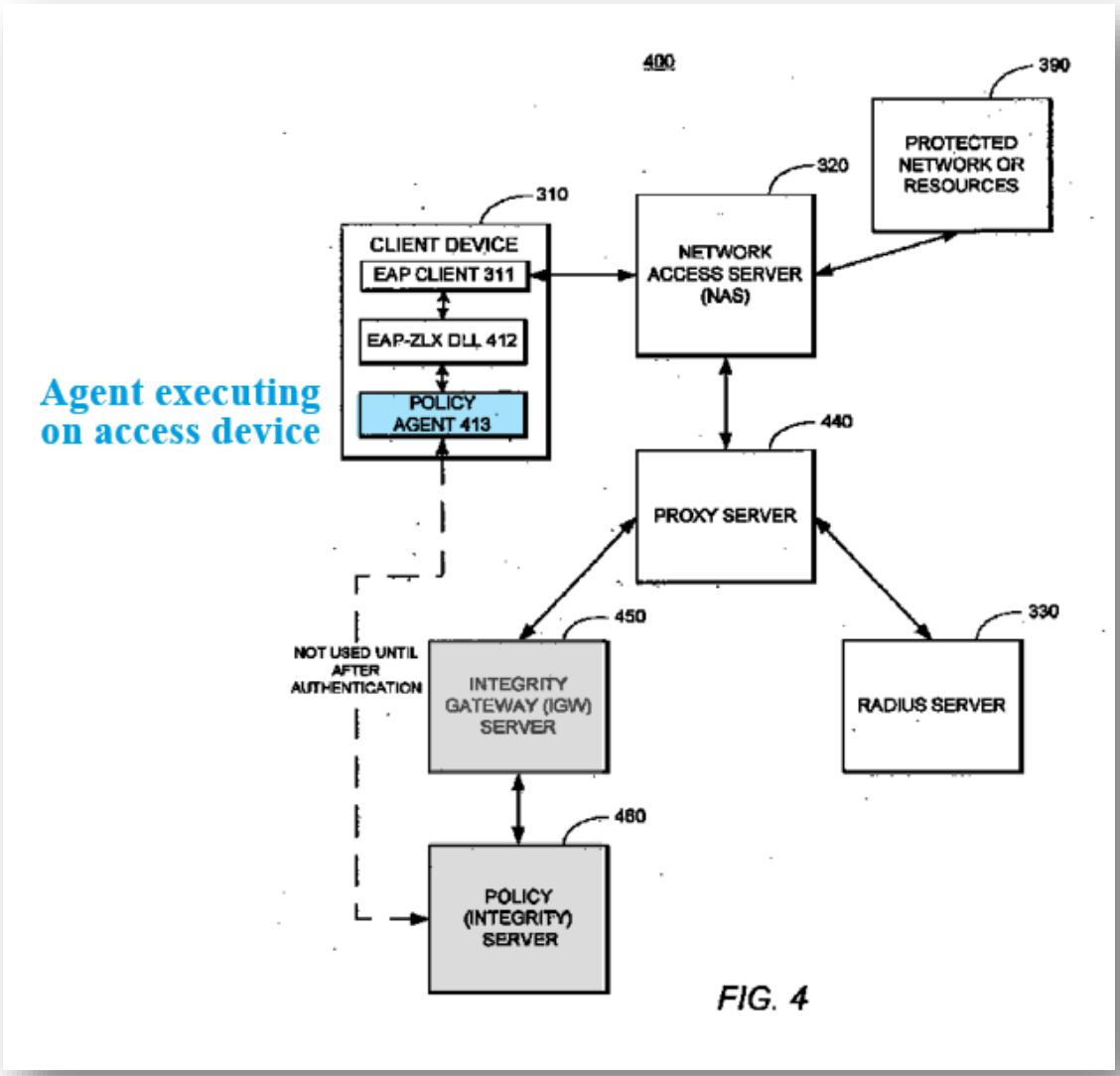
Access Device 230 and to report information about these devices (e.g., their security statuses or MAC addresses) to GateKeeper 225." Ex.1001, 7:21-30.

150. For example, 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.1005, [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. Ex.1005 [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.") (i.e., "*communicating between the gatekeeper and …*")*.*

151. A POSITA would have understood that one way that credentials (e.g., operating system credentials, certificates, keys, and supported cipher suites, etc.) such as those disclosed in Krantz would be retrieved and/or sent would be by

utilizing a client agent, although Krantz does not expressly state that such an agent is used. 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.

152. For example, Herrmann discloses a "POLICY AGENT 413" (i.e., an "*agent*") (emphasized in blue) executing on the client device (*i.e.,* "*executing on the access device*"), interacting with a "POLICY (INTEGRITY) SERVER 460" and "INTEGRITY GATEWAY (IGW) SERVER 450" (collectively emphasized in gray) as shown below.



Ex.1006 (Herrmann), Fig. 4 (annotated)

153. Herrmann discloses that "policy agent (or integrity agent) 413 to **retrieve information about the current security policy in operation on the client device 310** [i.e., "*to obtain system data from the access device*"]**."** Ex.1006, [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.1006, [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.1006, [0080], [0098].

154. 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.1005, [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 to the system of Krantz, as it would provide an automated means of providing network security.

155. 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.1006, [0064]; *see also, id.*, [Fig. 4]. This is the same protocol utilized in Krantz. *See, e.g.*, Ex.1005, [0018] ("Sending credentials can include sending an Extensible Authentication Protocol ('EAP') Response/Identity message from the client to the server.").

156. Accordingly, Krantz in combination with Herrmann renders obvious "[t*]he method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device*."

b. [5.1] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.

157. *See* claim [3.0] *above*.

6. Claim 6

a. [6.0] The method of claim 5, wherein the system data includes information regarding devices connected to the access device.

158. As I explain above with respect to claims 1 and 3, Krantz in view of Herrmann discloses obtaining system 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.

159. Krantz does not expressly disclose "*wherein the system data includes information regarding devices connected to the access device*," but 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. It would have been obvious to include Herrmann's techniques for obtaining system data from an access device (e.g., 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.1006, [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*.

160. 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.*, [0067]; *see also, e.g.,* Ex.1015,

12:46-13:15 (describing additional security features to include "alarm/lockout functions" and "audit trail[s]" "of all systems to which the device is attached.")

161. 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.1014 ("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.

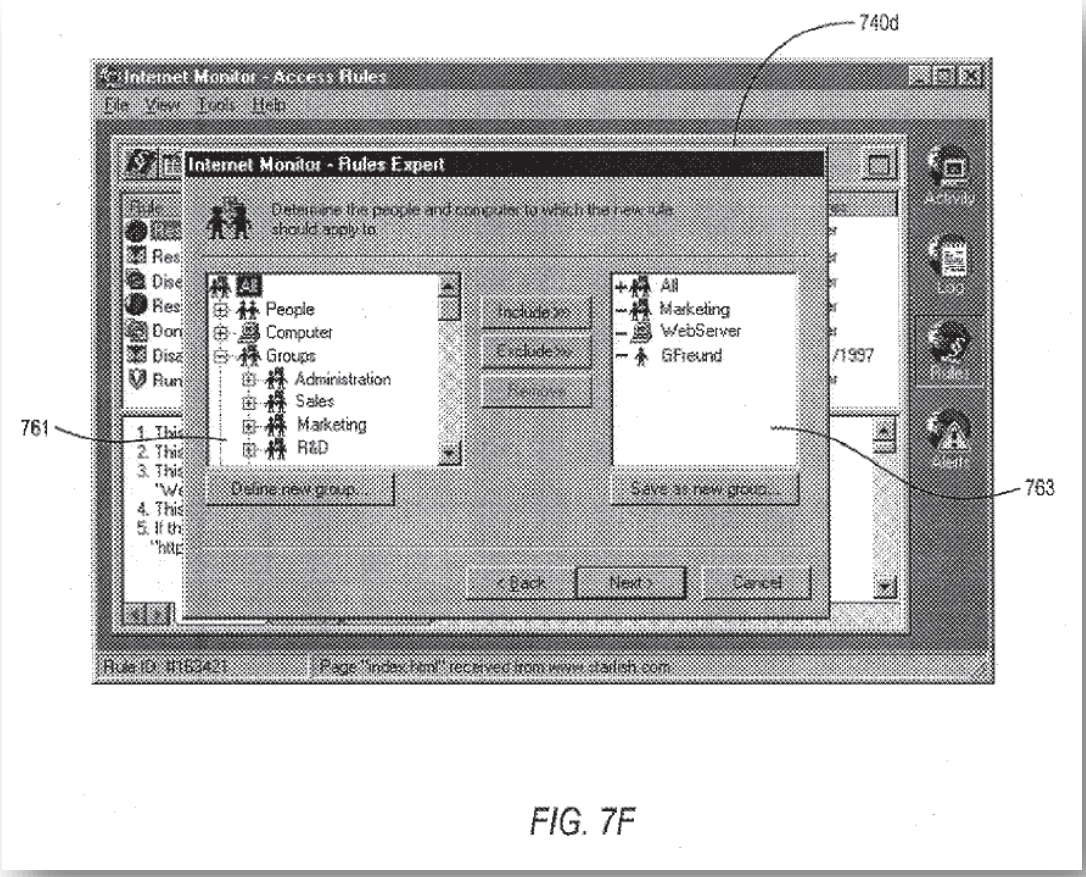


FIG. 7F

Ex.1014 (Freund), Figure 7F (incorporated by reference in Herrmann)

162. 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.

163. Accordingly, Krantz in combination with Herrmann renders obvious "[*t]he method of claim 5, wherein the system data includes information regarding devices connected to the access device*."

7. Claim 10

a. [10.0] The method of claim 1, wherein the access point is a network switch.

164. Krantz renders obvious claim 10. With respect to Krantz's "*access point*"—*i.e.,* the obvious combination of Access Point 209 and Data Routing Device 214 described above, *see* § IX.A.1.f—Krantz explains 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.1005, [0059].

165. Accordingly, Krantz renders obvious *"[t]he method of claim 1, wherein the access point is a network switch*."

8. Claim 11

a. [11.0] The method of claim 1, wherein the access point is a wireless access point.

166. Krantz discloses claim 11. With respect to Krantz's "*access point*"—*i.e.,* Access Point 209—Krantz explains that "Network architecture also includes access point 209. **Access point 209 can be a wired or wireless access point** that facilitates communication between client 205 and data routing device 214." Ex.1005, [0059]; *see also* Ex.1005, [0064] ("In some embodiments, **access point 209 is a wireless access point** that enables access to wired computer systems on VLAN B (e.g., server 215) and VLAN C (e.g., computer systems included in network 213).

167. Accordingly, Krantz discloses "[*t]he method of claim 1, wherein the access point is a wireless access point*."

9. Claim 12

a. [12.0] The method of claim 1, wherein the access point is a remote access virtual private network.

168. Krantz renders obvious claim 12. With respect to Krantz's "*access point*"—*i.e.*, Access Point 209—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.1005, [0017]. Krantz, however, does not expressly disclose that the access point could

comprise a "*remote access virtual private network,*" but it would have been obvious to implement that functionality in view of Krantz itself. Krantz recognizes the importance of security and access-control techniques, and a VPN was a well-known technique for preventing unauthorized access. Ex.1013 (a virtual private network is "a network where data is transferred over the Internet **using security features preventing unauthorized access**.") (emphasis added); Ex.1012 (a virtual private network is [a] highly secure network for transmitting sensitive data . . . that used the public Internet as a transmission medium….VPNs use encryption and protocol tunnelling."). Krantz explicitly states that any secure methods, including VPNs, can be used to restrict access consistent with the disclosed methods. Ex.1005, [0055] ("It would be apparent to one skilled in the art, after having reviewed this description, that other techniques, in addition VLAN, IP filtering, and VPN techniques, can be used to allow access to one network, while restricting access to another network."). Thus, it would have been obvious for the access point to be a "*remote access [VPN]*" because of the emphasis in Krantz on the use of security techniques and preventing unauthorized access as well as its actual disclosure of VPNs for components of the disclosed network. *Id.*, [0017], [0032], [0038] ("Logical communication links may also include portions of a virtual network, such as, for example, Virtual Private

Network …"), [0054] ("In yet other embodiments, access to resources on network [] can be restricted by use of a Virtual Private Network …").

169. Accordingly, Krantz renders obvious "*[t]he method of claim 1, wherein the access point is a remote access virtual private network*."

10. Claim 13

a. [13.0] The method of claim 1, wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network.

170. *See* claim [1.0] above.

171. In addition, I note that the 460 Patent explains that "[l]ess-Restricted Subset **210** includes **those elements of Protected Network 200 not included in Restricted Subset 205.** Less-Restricted Subset **210** optionally includes **devices such as a File Server 235, a Network PC 240, a Printer 245, or the like**." Thus, in the context of the 460 Patent and claim 13, "*elements*" are those devices that exist on the "*less-restricted subset of the protected network.*" Such devices—or "*elements*" in Krantz would include, for example, "computer systems included in network 213." Ex.1005, [0064]. Krantz further 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** (*i.e.,* "computer systems included in network 213") **to re-authenticate [**with Authentication Module 217 ("*gatekeeper*")]. Ex.1005, [0108]. Thus, "*the gatekeeper is accessible to elements*

of the less-restricted subset of the protected work" (*i.e.,* "computer systems included in network 213") at least to re-authenticate their subscription.

172. Accordingly, Krantz renders obvious "[*t]he method of claim 1, wherein the gatekeeper is accessible to elements of the less-restricted subset of the protected network*."

11. Claim 14

a. [14.0] The method of claim 1, wherein the restricted subset of the protected network is characterized by an access control list.

173. Krantz discloses or at least renders obvious "*wherein the restricted subset of the protected network is characterized by an access control list*."

174. For example, Krantz explains that "access to resources located on network 413 can be restricted by the use of Internet Protocol ("IP") filtering. Data routing device 414, components in network 411, or components in logical communication link 433 can filter Internet Protocol ("IP") address to limit client 405's access to resources with particular IP addresses**. When client 405 is not authorized to access resources located on network 413, IP addresses can be filtered such that client 405 is exposed to IP addresses of resources located on network 412** but is not exposed to IP addresses of resources located on network 413. When client 405 is authorized to access network 413, IP addresses can be filtered such that client 405 is exposed to IP addresses of resources located on both

networks 412 and 413. Alternately, when client 405 is authorized to access network 413 IP filtering may cease altogether." Ex.1005, [0053].

175. Krantz further explains 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** [*i.e.*, the restricted subset]. 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]. A POSITA would have understood that limiting access to server resources for specific clients through IP filtering is a form of an "*access control list*." A POSITA would have similarly found it obvious to use an "*access control list*" in a VLAN embodiment because such an embodiment has client access control considerations. *See, e.g., id.*, [0052] ("For example, **when client 405 is not authorized to access resources** located network 413, components in network 411 or logical communication link 433 can Tag data frames from client 405 indicating that the data frames are to be routed to server 415 (or other resources located on network 412). **When client 405 is authorized to access network 413**, components in network 411 or logical communication link 433 can Tag data frames from client 405 indicating that the data frames are to be routed to resources on network 413

(e.g., to the Internet) or to resources on network 412 (e.g., server 412) as appropriate.").

176. Accordingly, Krantz renders obvious "[*t]he method of claim 1, wherein the restricted subset of the protected network is characterized by an access control list*."

12. Claim 16

a. [16.0] A non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor to perform a method for controlling access to a computer network, the method comprising:

177. *See* [1.0] *above*.

178. Additionally, Krantz discloses "[a] non-transitory computer-readable storage medium having stored thereon a program, the program being executable by a processor" to perform the functionality I have already discussed with respect to claim 1.

179. As discussed in Krantz, this can include "computer program products, and data structures" that can increase the level of automation for provisioning and configuring an access device (e.g., a computer system) to access a computer network. Ex.1005, [0014]. Numerous forms of non-transitory computer readable storage media are described in Krantz such as floppy disk and flash cards (*id*, [0021]) as well as "RAM, ROM, EEPROM, CD-ROM or other optical disk

storage, magnetic disk storage or other magnetic **storage devices**, or any other medium which can be used to carry or store desired program code." *Id.*, [0036].

180. Krantz uses the term "computer-readable medium" as it is commonly understood. For instance, Krantz articulates that "[w]hen information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer system, the computer system properly views the connection as a **computer-readable medium**. Thus, any such connection is properly termed a computer-readable medium." *Id.*, [0037].

181. Krantz discloses that "[t]he drives and their associated **computer-readable media provide nonvolatile storage** of computer-executable instructions, data structures, program modules and other data for the computer 120" as seen in Fig. 1. *Id.*, [0043].

182. Krantz explains how "portions of such modules and portions of associated program data may be included in operating system 135, application programs 136, program modules 137 and/or program data 138, for storage in **system memory** 122 … [and] [e]xecution of such modules may be performed in a distributed environment as previously described." *Id.*, [0049].

183. Accordingly, Krantz renders obvious "[*a] non-transitory computer-readable storage medium having stored thereon a program, the program being*

executable by a processor to perform a method for controlling access to a computer network, the method comprising."

b. [16.1] receiving a request for access to a less-restricted subset of the protected network from an access device,

184. *See* [1.1] *above*.

c. [16.2] the request being received through a communication port of an access point,

185. *See* [1.2] *above*.

d. [16.3] the communication port configured for communicating between the access device and a restricted subset of the protected network,

186. *See* [1.3] *above*.

e. [16.4] the restricted subset including a gatekeeper; applying a security policy to the access device in response to the request; and

187. *See* [1.4] *above*.

f. [16.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when requirements of the security policy are satisfied.

188. *See* [1.5] *above*.

13. Claim 17

a. [17.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable by a processor to authenticate a user of the access device.

189. *See* [2.0] *above*.

14. Claim 18

a. [18.0] The non-transitory computer readable storage medium of claim 16,

190. *See* [16.0] *above*.

b. [18.1] wherein the program is further executable by a processor to obtain system data from the access device, and

191. *See* [5.0] *above*.

c. [18.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.

192. *See* [3.0] *above*.

15. Claim 19

a. [19.0] *The* non-transitory computer readable storage medium of claim 18, wherein the system data includes antivirus software version data.

193. See [4.0] above.

16. Claim 20

a. [20.0] The non-transitory computer readable storage medium of claim 16,

194. *See* [16.0] *above*.

b. [20.1] wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and

195. *See* [5.0] *above*.

c. [20.2] wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.

196. *See* [3.0] *above*.

17. Claim 21

a. [21.0] The non-transitory computer storage readable medium of claim 20, wherein the system data includes information regarding devices connected to the access device.

197. *See* [6.0] above.

18. Claim 22

a. [22.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.

198. See [16.0] above regarding *the non-transitory computer readable storage medium of claim 16*.

199. See [5.0] above regarding the limitation: *wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device*.

200. Krantz further discloses that *the security status of the access device is monitored after reconfiguring the communication port for communicating between the access device and the less-restricted subset*.

201. 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., *the security status of the access device is monitored*]. 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**." Ex.1005, [0108]. Because the security status is continually monitored in the background, as just discussed, a POSITA would understand that this includes

monitoring the security status *after reconfiguring the communication port for communicating between the access device and the less-restricted subset. See also*, [1.5] and [16.5] *above* regarding the reconfiguring element.

202. Similarly, Herrmann discloses continuous monitoring, including after reconfiguration. Herrmann explains that "Alternatively, 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**). 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.1006, [0080]. Similarly to Krantz, because Herrmann discloses that the security status is continually monitored through an IA_HEARTBEAT, as just discussed, a POSITA would understand that this includes monitoring the security status *after reconfiguring the communication port for communicating between the access device and the less-restricted subset.*

203. A POSITA would have been motivated to combine Krantz and Herrmann for the reasons stated above in section VIII.C. Because of known risks in a networked environment, a POSITA would have looked to some of the well-known security techniques disclosed in Herrmann such as an "agent [that] monitors and controls the interaction of the local machine **with other machines and devices that are connected on a LAN** or a larger wide area network (WAN), such as the Internet, in order to provide security to the machine." Ex.1006, [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.*, [0067].

204. Accordingly, Krantz in combination with Herrmann renders obvious "*[t]he non-transitory computer readable storage medium of claim 16, wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset*."

19. Claim 27

a. [27.0] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.

205. Krantz discloses this limitation.

206. For example, Krantz explains that "[w]hen full access to resources located on the second network is not authorized, the server can authorize limited access to the first network or second network such that the client can download provisioning files for gaining full access resources located on the second network. Ex.1005, [0032]; *see also* Ex.1005, [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.1005, [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 [*the program is further executable*]. 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 [*update the access device when requirements of the security policy are not satisfied*]. Provisioning module 208 can retrieve previously downloaded XML

documents, such as, for example, a configuration sub-file, from provisioning data 207."

207. Accordingly, Krantz discloses "*The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied*."

20. Claim 29

a. [29.0] The non-transitory computer readable storage medium of claim 16, wherein the restricted subset of the protected network is characterized by an access control list.

208. *See* [14.0] *above*.

21. Claim 30

a. [30.0] The non-transitory computer readable storage medium of claim 29, wherein access to the restricted subset of the protected network is responsive to a VLAN configured to communicate with the protected network subject to the access control list.

209. *See* [14.0] *above*.

210. Krantz further describes that client 205 is a component of VLAN A. Ex.1005 [0052]; FIG 2. Thus, a POSITA understood that when client 205 accesses VLAN B using an access control list as described in claim [14.0], VLAN A is "*configured to communicate with the protected network subject to the access control list*."

B. Additional Obviousness Analysis of Claims 1-2, 10-14, 16-17, 27 and 29-30 based on Krantz and Herrmann

211. As I demonstrate above, Krantz teaches or suggests each element of claims 1-2, 10-14, 16-17, 27 and 29-30. To the extent one may assert that Krantz does not teach or suggest "*applying a security policy . . .*" or "*using the gatekeeper to determine if requirements of the security policy are satisfied by the access device*" in claim elements [1.4] (and [16.4] with respect to "*applying a security policy . . .*"), those element would have been obvious based on the teachings of Krantz and Herrmann. A POSITA would have combined the teachings of Krantz and Herrman for the reasons I have already stated above. *See* ¶¶51-64, *above*.

212. In the combined Krantz/Herrmann system, server 215 ("*gatekeeper*") of Krantz would include within its own "*security policy*"—*i.e.,* the authentication of both the client device and the user—a requirement for a virus protection program as taught by Herrmann. In the Krantz/Herrmann system, server 215 would make determination as to whether the client is in compliance with the security policies.

213. Accordingly, Krantz and Herrmann render obvious claims 1-2, 10-14, 16-17, 27, and 29-30 for this reason as well.

X. CONCLUSION

214. 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.

Henry H. Houh.

Dated: March 1, 2024
Henry Houh, Ph.D.