UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00675
IPR2024-00679

U.S. Patent No. 7,523,484

DECLARATION OF DR. ERIC COLE IN SUPPORT OF THE PATENT OWNER'S RESPONSE TO THE PETITION

55001110.2

TABLE OF CONTENTS

PAGE

I. INTRODUCTION 1

II. QUALIFICATIONS 2

III. SCOPE OF WORK 8

IV. BASIS FOR OPINIONS 9

A. Validity and Infringement 10
B. Level of Ordinary Skill in the Art 11
C. Anticipation 12
D. Obviousness 15

V. OVERVIEW OF THE 444 PATENT 17

VI. THE ASSERTED PRIOR ART REFERENCES 24

A. U.S. Patent No. 2004/0111520 ("Krantz") 24
B. U.S. Patent No. 2004/0107360 ("Herrmann") 28

VII. OPINION AND ANALYSIS 33

A. Krantz's disclosure of VLAN tag headers does not teach "configuring the access point." as is recited by 444 Patent claims 2, 22, and those depending thereon. 33
B. Krantz does not disclose a "less restricted subset of the network." 38
C. Krantz does not teach or suggest the claimed "method for auditing a device." 41
D. The Challenged Claims of the 444 Patent (1-7, 10, 12, 17, and 22) are valid because it would not be obvious to combine Krantz with Herrmann. 46
E. Herrmann confirms that "applying a security policy that includes at least one requirements pertaining to the audit data" would not have been "minimal," "simple", or merely an "additional check" for Krantz's Server. 51
F. Herrmann's client-side system teaches away from a combination with Krantz's server-side system. 63

G. Claims 5–7 and 22 are valid because neither Krantz nor Herrmann discloses the claimed "receiving, from the agent, updated audit data pertaining to the device after configuring the access point . . ." and the like. 66

H. Claim 17 of the 444 Patent is valid because Krantz's disclosure of "provisioning files" does not meet claim 17's "bringing a software on the device up to date in response to applying the security policy." 69

VIII. CONCLUSION 74

I, Eric Cole, of Ashburn, Virginia, declare that:

I. INTRODUCTION

1. I have been retained by InfoExpress, Inc. ("InfoExpress" or "Patent Owner") to offer opinions regarding claims 1–6, 11–13, 15–19, 23–25, 28, 38–39, 41–43, 53, 57–59, 61–63, and 65–68 ("the Challenged Claims") of U.S. Patent 7,523,484 (the "484 Patent"). I submit these opinions in support of InfoExpress's claim that the Challenged Claims of the 484 Patent are patentable under 35 U.S.C. §103, even in view of the references asserted by Petitioner. I am prepared to testify about the matters set forth herein. All the facts and my opinions herein are understood to be true and correct and are within my personal knowledge.

2. As stated, I have been requested by counsel for InfoExpress to provide opinions regarding patentability of the Challenged Claims of the 484 Patent in response to the claims made by Petitioner in the Petition.

3. This declaration and my opinions contained herein are based on information currently available to me. I may continue my investigation as new information is provided. Accordingly, I reserve the right to supplement and/or amend my opinions contained herein. I also reserve the right to provide opinions regarding any other patents at a later date.

II. QUALIFICATIONS

4. My academic credentials include a master's degree in computer science and a doctorate in information security, and I have worked in the cyber and technical information security industry for over twenty-five years. The details of my education and experience are summarized in my curriculum vitae ("CV"), which is provided as Exhibit A. My CV also includes a list of my publications over the past ten years.

5. I have worked in computer security for over twenty-five years. To briefly summarize my career, I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; 6) continually taught and written about cybersecurity.

6. I am the founder and president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia. Secure Anchor Consulting provides cybersecurity consulting services and lead research and development initiatives to advance information systems security. Many of the clients I work with are responsible for protecting sensitive client and/or consumer information and implementing effective security.

7. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls, and I have detailed knowledge of the effort that is required to implement various remediation measures.

8. I worked for the U.S. government for eight years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have worked for a wide range of government organizations, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department of Energy, the Department of Defense (DOD), the Treasury Department, the Secret Service, and the Nuclear Regulatory Commission (NRC). I have held various top-secret security clearances with the DOD, the CIA, and the NRC. I was also involved in funded research from the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new intrusion detection technologies for use by the military. During this time, I have reviewed, edited, and created numerous security policies. On several occasions, I have also reviewed the reasonableness of measures

intended to protect and secure Confidential Information through various types of documentation to include policies, procedures, standards, and baselines.

9. While serving as a Senior Officer for the CIA as Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team which designs, develops, tests, and deploys Internet security products in three- to six-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security, I evaluated and performed security assessments of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with an automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured. I was also one of the principal leads on research funding from DARPA. In this role, I was responsible for understanding the current state of the art in intrusion detection

and designing and building a new cybersecurity system that could catch attacks that were targeting organizations.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as a technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting clients' information and helping them implement effective security solutions.

14. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security

professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people, and I have taught more than 50% of these students via live and online training. The courses that I have written have multiple modules and lessons on security policies, employee agreements, and protection of intellectual property. As one of the top-rated instructors at SANS, I have delivered keynote addresses around the world.

15. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

16. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

17. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a Commissioner on cybersecurity for President Obama. My Nine books on cybersecurity include "Online Danger," "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. They are used in many

classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

18. The focus of my work over the last ten years has been on data protection for commercial organizations. I am very familiar with best practices in cybersecurity and have developed many of the standard practices.

19. Today, my consulting efforts help organizations properly protect client information and relate to various alternative methods of security that can be implemented. This includes hardening of systems, securing servers, proper configuration, patching, and compensating controls. In cases where a fix cannot be made because it would negatively impact the business, I have extensive experience in understanding various compensating controls as an alternative to minimize the risk to an acceptable level and how to implement those controls.

20. I routinely help clients develop and implement company-wide policies, training, and best practices to prevent potential cybersecurity incidents. My work addresses threats from both internal and external sources, including accidental and intentional incidents.

21. I have led, and been involved in working on, responses to many cybersecurity incidents. This includes performing root cause analysis, verifying the reasonableness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to responding to breaches post detection. I have a very detailed understanding of what is and is not a reasonable level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

III. SCOPE OF WORK

23. I have been retained as a technical expert by Saul Ewing LLP, counsel for InfoExpress Inc. ("InfoExpress" or "Patent Owner"), to provide my expert opinions as to four patents, which Petitioner Cisco Systems, Inc. and Fortinet, Inc. have challenged as unpatentable in this and related *inter partes* review proceedings. These patents include U.S. Patent Nos. 7,523,484 (the '484 Patent); 8,051,460 (the '460 Patent); 8,677,450 (the '450 Patent); 8,578,444 (the '444 Patent) collectively, the "Challenged Patents"). These Challenged Patents are also asserted by InfoExpress in related, co-pending district court litigations against Petitioner.[1]

---

[1] *InfoExpress Inc. v. Cisco Systems, Inc.*, Case No. 4:23-cv-2698-YGR (N.D. Cal.); *InfoExpress Inc. v. Fortinet, Inc.*, Case No. 4:23-cv-4389-YGR (N.D. Cal.).

Two other patents—U.S. Patent Nos. 8,347,350 (the '350 Patent); and 8,117,645 (the '645 Patent)—have also been asserted in district court litigation. Petitioner filed IPR petitions against them, but the Board declined to institute those IPRs.

24. I have been asked to consider and provide my opinions on the Challenged Claims of the 484 Patent, including the technical subject matter and the application of various references relied upon by the Petitioner. In particular, I have been asked to consider what a person of ordinary skill in the art would have understood from the claims and specification of the 484 Patent at the time it was invented and whether certain references disclose or suggest the features recited in the claims of the 484 Patent.

25. I am compensated at a rate of $800/hour for my work. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of any proceeding.

IV. BASIS FOR OPINIONS

26. My opinions set forth below are based on my education, training, experience, and the content of the references considered. My opinions are further based on the Petition and materials submitted by Petitioner.

Cisco Systems, Inc. v. InfoExpress Inc., IPR2024-00540, Paper No. 13 (PTAB Sept. 24, 2024) (declining to institute review of the '350 Patent) and No. 15 (PTAB Dec. 13, 2024) (denying Petitioner's request for Director Review); *Cisco Systems, Inc. v. InfoExpress Inc.*, IPR2024-00678, Paper No. 14 (PTAB Oct. 11, 2024) (declining to institute review of the '645 Patent) and No. 16 (PTAB Dec. 31, 2024) (denying Petitioner's request for Director Review).

A. Validity and Infringement

27. I have been informed that the Challenged Patents, including the 484 Patent, are presumed to be valid by virtue of having been issued by the United States Patent and Trademark Office on April 21, 2009. Accordingly, I understand that Fortinet and Cisco, as IPR Petitioner, bear the burden of proving by a preponderance of the evidence that the InfoExpress Patents, including the 484 Patent, are unpatentable. I am not presently aware of any contention by Fortinet or Cisco that any of the Challenged Claims are invalid, other than their general allegation the claims are unpatentable as obvious under 35 U.SC. § 103 in view of references Krantz and/or Herrmann (the "Asserted References"). If Fortinet or Cisco later offer any additional contentions that the 484 Patent is invalid, I reserve the right to address any such contentions and provide my responsive opinions.

28. I have been informed that the claims of a patent measure its scope and that each patent claim defines a separate invention. I have been further informed that a patent includes a written description of one or more preferred embodiments of the invention. With respect to the 484 Patent, I have considered the scope of the patent claims according to the plain and ordinary meaning of the claims when read in view of the specification and drawings.

B. Level of Ordinary Skill in the Art

29. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the purported invention would have understood at the time of the purported invention of the Challenged Patent.

30. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of the invention of the patent. I understand that the person of ordinary skill is a hypothetical concept referring to one who thinks along the lines of conventional wisdom at the time.

31. I was asked to provide an opinion as to the level of one of ordinary skill in the art pertinent to the subject matter set forth in the Challenged Patent at the time of the priority date. Around the time of filing of the 484 Patent, it is my opinion that a person of ordinary skill in the art in the field of the Challenged Patent would have been a person with a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields. Throughout this declaration, I use the term "POSITA" to refer to a person with these or similar qualifications. To have similar qualifications, an individual with additional education or additional industrial

experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above.

32. The basis for my familiarity with the level of ordinary skill is my interaction with large numbers of workers in the computer security industry who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field.

C. <u>Anticipation</u>

33. I understand and have been informed that in order for an inventor to be entitled to a patent, the invention must be "new," and the inventor must not have lost his or her right to a patent by delaying filing of a patent application directed to the invention. There are a number of ways that an invention can be "anticipated"—that is, not new.

34. One such way is when the invention was already patented or described in a printed publication anywhere in the world before the date of invention by the inventor or more than one year before the earliest effective filing date of the patent application. Additionally, a patented invention may not be new

if it was on sale or publicly used more than one year before the filing of an application for patent. A patented invention is also not new if it was "known" or used by others in the United States before it was invented by the patent applicants. To invalidate a patent claim based on knowledge, I understand that the knowledge must be accessible to the public. If the subject matter covered by a patent claim is found within the "four corners" of a prior art reference, the claim is said to be anticipated by that reference.

35. A patent claim can be said to be anticipated if each and every limitation of the patent claim is found either expressly or inherently in a single item of prior art. While a prior art reference need not use the same words as a patent claim to anticipate the claim, the prior art reference must describe the requirements of the claim with sufficient clarity such that a POSITA would have been able to make and use the claimed invention based on the reference and his or her knowledge in the applicable technical field.

36. The disclosure of a feature of a claimed invention can be either "express," meaning that the text, figures, or other content of a reference actually teaches the aspects of the patent claim, or the disclosure can be "inherent." An express disclosure does not need to use the same words as the patent claim being considered and does not need to be depicted in exactly the same way, but the disclosure must actually convey the claimed invention to a POSITA using some

combination of words, figures, data, or other portions of the patent. I have been informed and understand that in order to establish that an element of a claim is "inherent" in the disclosure in a prior art reference, it must be clear to a person skilled in the art that the missing element is an inevitable part of what is explicitly described in the reference, and that it would have been recognized as necessarily present by a person skilled in the art. Inherency cannot be established by probabilities or possibilities, and the mere fact that something may result from a given set of circumstances is not enough to establish inherency.

37. Finally, I further understand that to anticipate a claim, the elements of the claim must be found in the prior art reference "arranged as in the claim." I have been informed that this means that the elements of the prior art reference may not be recombined in a way that is not taught in the prior art to arrive at the invention; instead, the prior art must teach the claimed subject matter in the arrangement required by the claims.

38. While I understand that Petitioner's grounds for unpatentability are not based on anticipation, but instead, are based on obviousness, I provide the above the understanding that any disclosure which anticipates a claim also renders that claim obvious.

D. Obviousness

39. I have been informed and understand that subject matter claimed in a patent is obvious under 35 U.S.C. § 103 if a person of ordinary skill in the art at the time the alleged invention was made would have had reason to combine or modify the disclosures of one or more prior art references to arrive at the claimed subject matter. A claim may be unpatentable even if each and every claim limitation is not present or disclosed in a single prior art item.

40. I have been informed and understand that, under the doctrine of obviousness, a claim is unpatentable if the differences between the 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 person having ordinary skill in the art to which the subject matter pertains. A person of ordinary skill in the art is presumed to have knowledge of the relevant prior art at the time of the claimed invention.

41. I have been informed and understand that obviousness is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and secondary indicia of obviousness and non-obviousness to the extent such indicia exist.

42. I have been informed and understand the determination of whether the asserted claims would have been obvious to a person of ordinary skill in the art and, therefore, invalid is not governed by any rigid test or formula. A

determination that a claim is obvious is, instead, based on a common-sense determination that the claimed invention is merely a combination of known limitations to achieve predictable results. Any of the following rationales are acceptable justifications to conclude that a claim would have been obvious: (1) the claimed invention is simply a combination of known prior art methods to yield predictable results; (2) the claimed invention is a simple substitution of one known element for another to obtain predictable results; (3) the claimed invention uses known techniques to improve similar devices (methods or products) in the same way; (4) the claimed invention applies a known technique to a known device (method or product) ready for improvement to yield predictable results; (5) the claimed invention was "obvious to try"—choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; (6) there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (7) there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference to combine prior art teachings to arrive at the claimed inventions.

43. I have been informed and understand that a claim may be obvious in light of a single reference, without the need to combine references, if the elements

of the claim that are not found in the reference can be supplied by the common sense or knowledge of one of ordinary skill in the art or taught in different areas of the single reference.

44. I have been informed and understand that an analysis of whether a claimed invention is obvious must not rely on a hindsight combination of prior art. The analysis must proceed in the context of the time of the invention or claimed priority date and consider whether the invention as a whole would have been obvious to a person of ordinary skill in the art, taking into consideration any interrelated teachings of the prior art, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine any known elements in the fashion claimed by the patent at issue.

V. OVERVIEW OF THE 484 PATENT

45. The 484 Patent is directed to an approach to improve upon computer network security methods that existed in the prior art. The patent itself explains that attempts to safeguard networks from unauthorized access and potential malware, viruses, and the like had been contemplated, but that approaches that existed at the time of the invention presented other problems. The patent then

explains that it was the shortcoming of the identified existing approaches that were overcome by the claimed invention.

46. According to the patent, by the time of the invention it had been recognized that enabling a user to access a protected network could first require authorization of that user or device. Examples of this authorization included checking the user's or the device's credentials against a database of authorized users or devices, such as by checking user ID and password or MAC address. EX1501, 1:31-40. In other words, the ID/Password (user) or MAC address (device) would cause the system to check whether the user was who they said they were or the device was what it purported to be. *Id.*

47. While authentication provided security is one context, the patent explains that there are other concerns for a protected network not addressed by authentication of a user/device. *Id*., 1:41-52. For example, because of concerns related to viruses or other malware, checking whether an access device had the necessary software or firmware to protect it from such would be a beneficial further analysis. This would be akin to checking if a child's vaccinations are up to date prior to going to school. The patent explains "[i]n addition to authenticating users who wish to access secure Network 100 using an Access Device 160, GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy, before granting access to Secure Network 100." *Id*.,

2:15-19. "Once GateKeeper 110 has verified that Access Device 160 is allowed to communicate through GateKeeper 110 to LAN 125, Access Device 160 is allowed to communicate through GateKeeper 110 to LAN 125." *Id*., 2:22-25.

48. The patent then teaches that these existing approaches required one or more "gatekeepers" placed directly between clients, i.e., users, and the protected network. EX1501, Fig. 1, 2:31-42. The computer architecture where an element was always between two other elements was often referred to as being inline. Following the child attending school analogy, the child and parent would have to provide identification documents and vaccination records to school administrators before they could attend class. The preexisting solutions required individual checking of each user's ID and password or device's ID, as well checking the device's software, e.g., virus protection and operating systems, before granting access to the protected network. This consumed substantial network resources, resulting in a bottleneck. EX1501, 2:39-45. In addition, because multiple gatekeepers were required for each access point to a network, scalability proved prohibitively expensive. *Id*.

49. An example of the prior art architecture having the identified shortcomings is shown in annotated FIG. 1 of the 484 Patent.

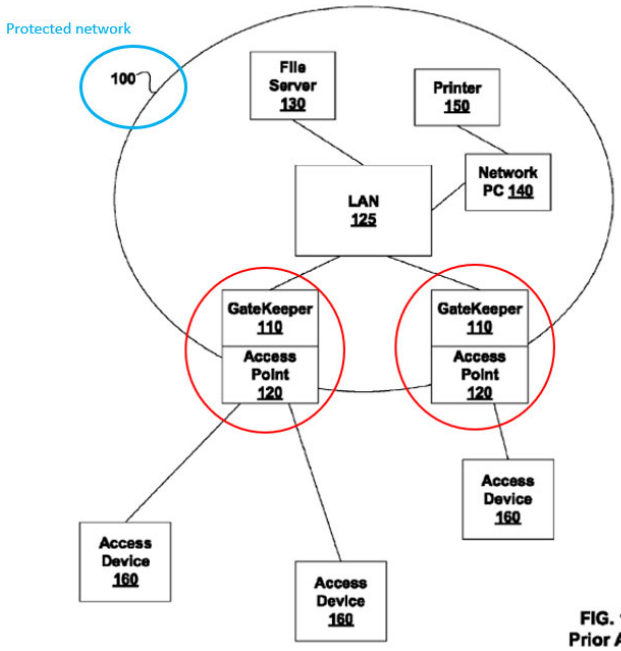


FIG. 1
Prior Art

50. While only two access points are shown, the patent explains that the protected network 100 may include many access points, and that each of the access points included a Gatekeeper 110. In this inline architecture, all access devices attempting to connect to the protected network must pass through a gatekeeper. The 484 Patent then explains that large protected networks may include many access points, and the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110." EX1501, 2:31-44. The inline gatekeeper then becomes a limiting bottleneck on the bandwidth of the system. EX1501, 2:34-42.

51. Based on my experience in the network security field, at the time of the invention, what is stated in the patent as being the state of the art is correct. At

the time of the invention, it was not known how to accommodate both authorization and device configuration checking, i.e., auditing, while also minimizing computing resources and avoiding bandwidth problems.

52. As disclosed in greater detail below, the state of the art disclosed in the patent of network security utilizing only authentication is the same as the cited Krantz reference, and the state of the art of network security also incorporating checking compliance of the access device with a security policy is the same as the Herrmann reference. The 484 Patent improved on the acknowledged problems with these prior art approaches to network security. The 484 Patent addressed these particular problems with the prior art by making the gatekeeper not inline and providing for reconfiguring of a previously configured access point, such as during initial setup, for data from previously authorized devices to access a protected network.

53. The 484 Patent discloses a protected network 200 that includes both a restricted subset 205 of the protected network with a gatekeeper 225 therein, as well as a less-restricted subset 210 of the protected network with other network resources. These two levels of access within a protected network by having a restricted subset with a gatekeeper and a less-restricted subset with other computer resources was exemplified in Fig. 2.

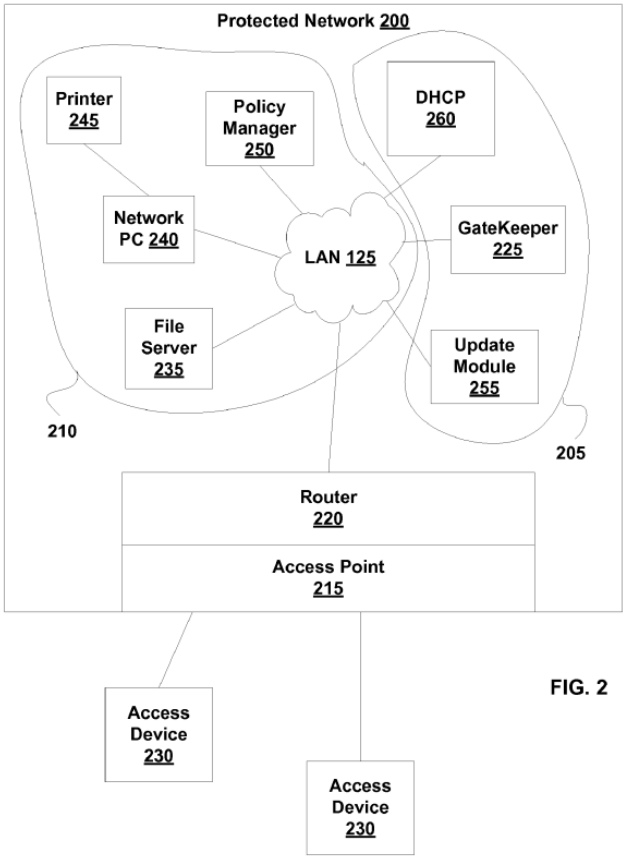


FIG. 2

54. Before an access device is granted access to a less-restricted subset 210, its request is first passed to the restricted subset (in this embodiment indicated as 205) of the protected network 200. EX1501, 2:49-52, 5:36-40. A gatekeeper in the restricted subset of the protected network checks whether the access device satisfies security policies, and if so, the access device is granted access to a less-restricted subset of the protected network. EX1501, 2:53-56.

55. The patent also teaches that, unlike the prior art, the shortcomings related to bandwidth and scalability are addressed through changes to the architecture of the system that were not found in the prior art. Claimed features of the 484 Patent include "[a] network gatekeeper comprising: . . . a policy auditor

configured to audit the access device using the at least one security policy" (claim 1), "applying a security policy to the access device" (claims 28, 41 and 56), and/or "a gatekeeper configured to enforce a security policy" (claim 57). Another claimed feature lies in "reconfigur[ing] the communication device" or "communication port" thereupon. *Id.* The 484 Patent specification provides as an example a network "characterized by Virtual Local Area Networks (e.g., VLANs)…." EX1501, 2:62–3:4. In this common example embodiment, the 484 Patent explains that "reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." *Id.*, 3:22-25. This involves basically changing the programming for the access point. The Detailed Description further explains reconfiguring the communication ports of an access point of a computer network comprising multiple VLANs.

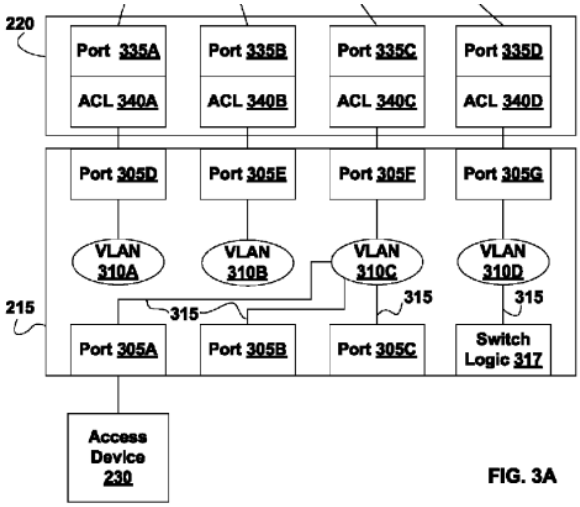


FIG. 3A

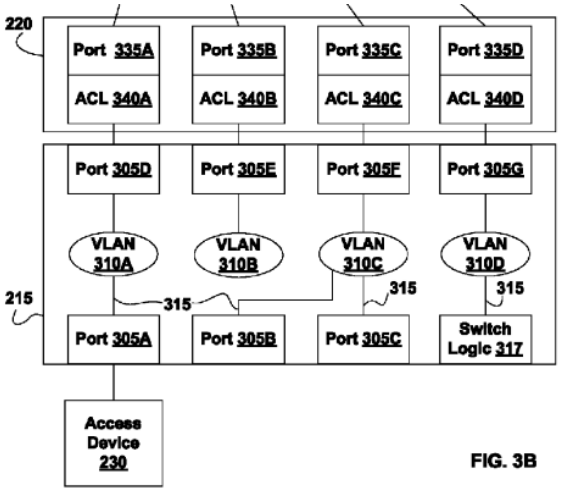


FIG. 3B

Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN

> 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-23.

56. As discussed, access points are configured by the gatekeeper enabling the reprogramming of the port associations. In other words, the access point itself is changed. Other manners of configuring an access point are known, which include but are not limited to access control lists. By configuring the access point, network traffic for certain devices can pass from the access device to the less-restricted subset of the network without needing to pass through the gatekeeper on the restricted subset of the protected network. This alleviates bandwidth demands while also not requiring the expense of numerous access points and gatekeepers as the 484 Patent teaches was required by the prior art.

VI. THE ASSERTED PRIOR ART REFERENCES

A. U.S. Patent No. 2004/0111520 ("Krantz")

57. Petitioner's primary reference, Krantz, is directed to computer related systems and methods to enable a user to access a network exemplified as a user accessing the internet. EX1505 ("Krantz"). Krantz explains that "before a computer system can communicate electronically on the Internet, a user of the computer system is often required to register with an Internet Service Provider … that can authorize access to the Internet." Krantz, ¶5. "[U]sers wishing to access

the Internet are subjected to contacting an ISP telephonically and waiting for appropriate access software and/or hardware to be delivered." *Id*. ¶8. Krantz further notes that "many [ISP] services are proprietary and each service may require different computer system configurations and/or registration information for authorizing access to the Internet" *Id*. ¶11.

58. To address these issues, Krantz discloses a server that may authorize a user to access a network, which is exemplified in Krantz as the Internet. *Id*. ¶16. A user must first send "credentials" to the server, which can be a "Remote Authentication Dial-In User Service ("RADIUS") server." *Id*. Such credentials are explained as being "user identifier and password." *Id*. ¶76. A RADIUS server was a known authentication server. RADIUS servers did not perform device auditing.[2] In order to provision a user's device with the ISP's software, Krantz discloses downloading provisioning files. *Id.*, ¶¶32, 85.

59. Depending on whether a user is authorized, Krantz further teaches how the user's data is directed in the context of VLANs.

> [A]ccess to resources located on network 413 can be restricted by the use of Virtual Local Area Networks ("VLANs"). In these embodiments, ***networks 411, 412 and 413*** may each be a portion of a different VLAN. ***VLAN aware devices in network architecture 400 can "Tag" data frames*** to indicate to data routing device 414 where the data frames are to be routed. For example, when client 405 is not

[2] Notably, Petitioner's other reference, Herrmann, evidences that RADIUS servers did not audit devices. Instead, additional servers were required for this separate function. This is discussed in further detail below.

> 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.

Id. ¶52.

60. It is important to understand the state of the art at the time of Krantz. As is stated in Krantz, at that time, when most people accessed the Internet it was by way of a dial up type service or Internet Service Provider (ISP), e.g., AOL, Netscape. To that end, Krantz discloses a system and method for enabling a user to access the Internet by setting up an account, paying for access, and then after being authorized by way of user ID and password being able to access the Internet. As described, with such authorization data from the client is tagged. As discussed below, a tag is data that may be included in a data frame. When an access point reads the incoming data frame, it directs the data frame to where the access point is configured to send data with such a tag. If a data frame does not include the tag header that the access point is configured to allow access to the Internet, the data frame is sent, as per the access point configuration, to the RADIUS server. After the user/device is authenticated, e.g., ID and password match a database entry, the

VLAN aware device (access point) follows its programming and inserts a different tag into the data from the user device so data from it is directed to the Internet.

61. The access point itself is not altered, however. Rather the VLAN aware device is configured, i.e., programmed to follow particular rules. One rule is that if the incoming data is not authenticated it is directed to the RADIUS server. Another rule is that if the RADIUS server authorizes the user, the VLAN aware device receives directions from the RADIUS server to insert a tag in that user's data so it is directed to the Internet. If the user is not authorized, VLAN aware device is programmed to reject the data frame. Krantz does not disclose, however, configuring the VLAN aware device itself. In other words, the programming of the VLAN aware device is not changed. Rather, it continues to operate according to its rules, and the tag on the user's data is changed. This is basically changing the routing information on the data.

62. It is further notable, that in all instances, Krantz discloses only user or device authorization. Throughout Krantz, user credentials such as user ID and password are provided, and relabeling of the user's data is based on evaluation of these credentials.

63. Notably, there is some disclosure in Krantz of "provisioning" a device. The context of Krantz, as discussed, is to enable a user to access the Internet via an ISP. As discussed in Krantz, typically, this involved installing an

ISP's software on the user's device. Those who tried to access the Internet in the late 1990s and early 2000s will no doubt recall the almost daily delivery of AOL compact disks that would enable one to access the Internet through America Online. Krantz's provisioning is automatically providing this software as part of signing up with the ISP. Notably, however, this provisioning has nothing to do with whether a user's device complies with a security policy, such as virus software status or operating system status.

64. Krantz's architecture is also notable. Krantz discloses a network to be accessed, e.g., the Internet, and then a separate network for authenticating the user before granting access. The authenticating network includes the aforementioned RADIUS server. Krantz does not disclose an embodiment of computer architecture where the network to be accessed includes different subsets where the authenticating element is found on one subset that is separated from other parts of the network.

B. <u>U.S. Patent No. 2004/0107360 ("Herrmann")</u>

65. Herrmann discloses a system and method for policy enforcement during authentication of client device for access to a network. Herrmann in many respects is what the 484 Patent explains to be the prior art. Herrmann discloses an access point called a Network Access Server (NAS) positioned outside of a protected network and between a client device attempting to access the protected

network resources and the protected network resources. *See* EX1506 ("Herrmann"), Fig. 4.

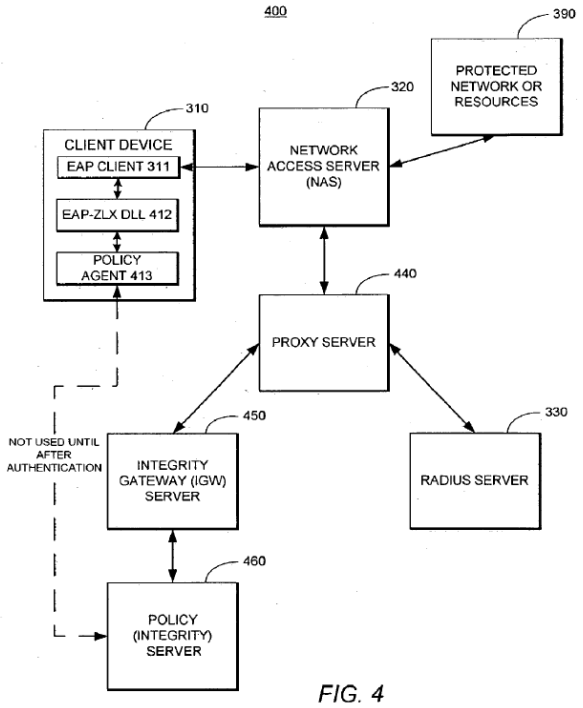


FIG. 4

66. Herrmann explains that in order for a client device to access a protected network, it must first go through a Network Access Server (NAS). Herrmann, ¶53. The NAS then, through a Proxy Server, must authenticate the user with a Radius Server. *Id.*, ¶59. After authenticating the identity of the user, an agent on the client must then gather information about the client device, which is communicated to the NAS, then to the Proxy Server, which communicates the device information to the Integrity Gateway Server (IGW). *Id.*, ¶¶63-68. The IGW then formats and packages the data for transmission to the Policy (Integrity) Server. *Id.* This Policy (Integrity) Server then unpacks the data and determines if the client device includes anti-virus software. *Id.*

67. As shown, all requests from a client to access the protected network must first pass through the NAS, the authentication server (RADIUS server), and then the policy server before the client is permitted to access the protected network. This presents the precise shortcomings detailed in the 484 Patent of requiring the evaluating element (e.g., gatekeeper) at the access point. Each time the device attempts to access the network, it must go through this evaluation.

68. After the session is approved, there is no further explanation in Herrmann of any further monitoring of the client device during the session or modifications to the system components in view of the approval process. In other words, Herrmann does not disclose any further monitoring of the client device for compliance with the security policy.

69. Petitioner also alleges that the 484 Patent is rendered obvious in view Krantz in further view of Herrmann, which was filed on March 3, 2003, and published on June 3, 2004. As stated, and explained with detail elsewhere, it is my opinion that ***no claims*** of the 484 Patent are rendered obvious by Krantz in combination with Herrmann.

70. The alleged prior art, Herrmann, is described as follows:

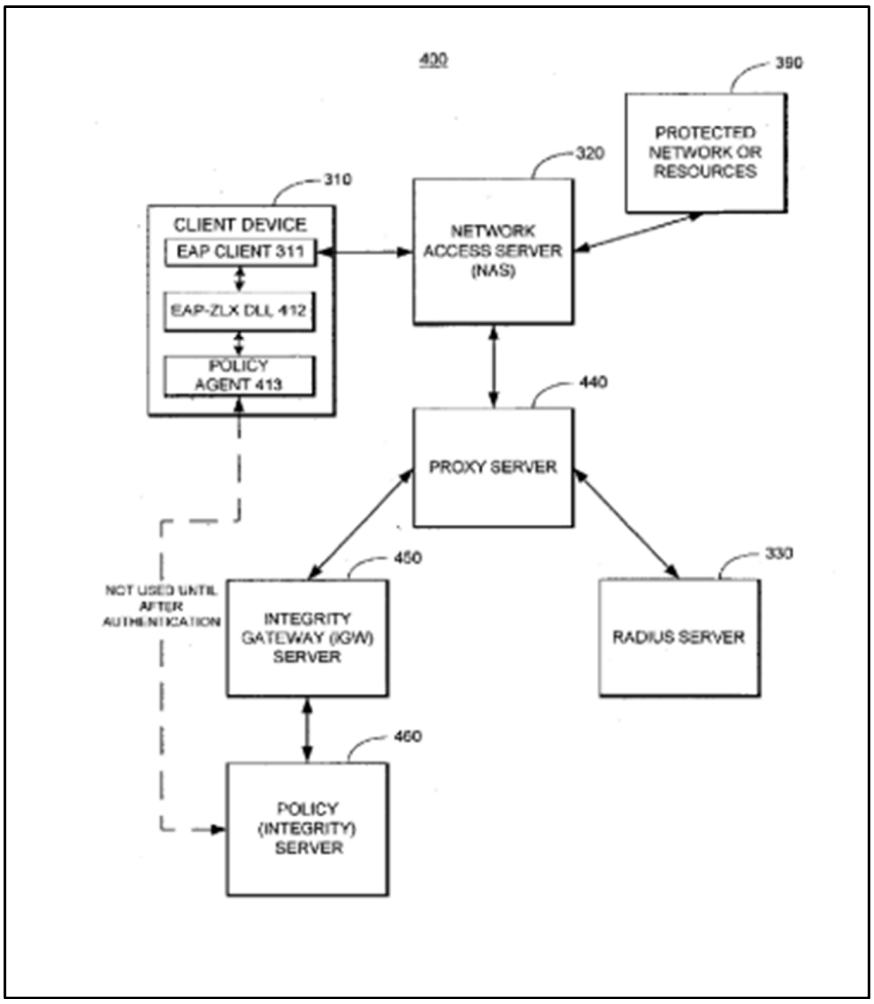
> A system and methodology for policy enforcement during authentication of a client device for access to a network is described. A first authentication module establishes a session with a client device requesting network access for collecting information from the client device and determining whether to authenticate the client device for access to the network based, at least in part, upon the collected information. A second authentication module participates

> in the session with the client device for supplemental authentication of the client device for access to the network. The supplemental authentication of the client device is based, at least in part, upon the collected information and a policy required as a condition for network access.

Herrmann, Abstract.

71. In short, Herrmann merely describes a system and methodology for policy enforcement in addition to authentication of a client device for access to a network, which generally requires the device attempting to connect to pass a generic security protocol. Herrmann does not provide active security policy enforcement, does not perform continual audits on devices connected to the network, and is unlike the 484 Patent.

72. The stark contrast between the technology described in the 484 Patent and the generic authentication method described in Herrmann is further illustrated by the Figure provided in Herrmann.



Herrmann, Fig. 4; *cf.* 484 Patent, Figure 2. Similar to Krantz, Herrmann discloses the use of a Network Access Server (NAS) placed between a client device and a restricted network, i.e., inline. Also similar to Krantz, Herrmann includes no disclosure of any modification or changes to the NAS to allow data from a client to pass to the restricted network based on approving the audit data of a device.

VII. OPINION AND ANALYSIS

A. Krantz's disclosure of VLAN tag headers does not teach "reconfigur[e/ing] . . ." as recited by 484 Patent independent claims 1, 28, 41, 56, 57 and those depending thereon.

73. Independent claims 28, 41, 56, and 57 require "reconfigur[e/ing]" a "communication port"; claim 1 similarly requires "access control configured to reconfigure the communication ***device***."[3] On their faces, these claim require "reconfiguring." As discussed below, Krantz does not disclose this feature.

74. With regard to the "reconfiguring . . ." requirement, Petitioner and Dr. Houh offer three "Mappings." In my opinion, none of these Mappings establishes reconfiguring of the communication ports of the access point.

75. Petitioner's Mapping #1: Petitioner's Mapping #1 argues that (1) "access point 209 is initially configured to allow access only to VLAN B—the restricted subset of the protected 'network[,]'" the access point 209 (including port 251) are "reconfigured" by virtue of the fact that it can be made to "transfer [] data between client 205 ('the access device') and ultimately VLAN C (the 'less-restricted subset of the network.'" -675 Petition at 44; *see also* -679 Petition at 35 ("'[P]ort 251' ('the communication port') is 'configured for communicating

[3] Dependent claims 16–19, 25, and 61–63 further specify the "communication device" or device to which the "communication port" is coupled. Claim 58 (dependent on 57) recites "wherein configuring the communication port includes associating the communication port with a VLAN."

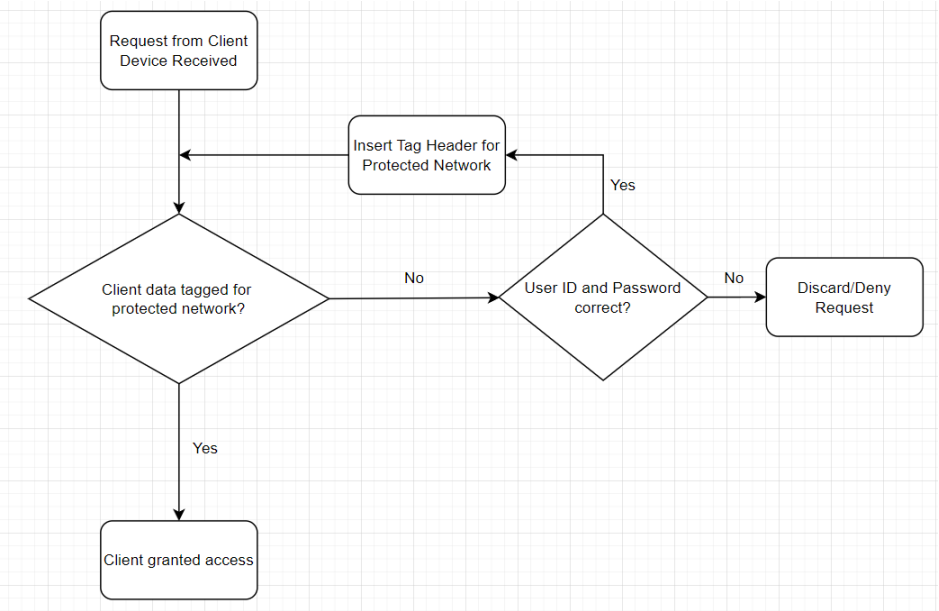
between the access device and restricted subset of the protected network' because it facilitates the transfer of data between client 205 ('access device') and VLAN B (the 'restricted subset of the protected network.')"). In mapping 1, Petitioner does not identify a change to Krantz's communication port. In essence, Mapping 1 merely looks at whether data from a client device that initially went to one VLAN ends up at another. This mere fact does not demonstrate any change to the communication port. There are different ways within a VLAN to cause data originally directed to one set of computer resources and then a different one that have nothing to do with reconfiguration of a communication port. One example is tag headers. In my opinion, as the Board properly determined in its Institution Decisions,[4] Mapping #1 does not teach making changes to a communication port 251 of access point 209.

76. Petitioner's Mapping #2: Petitioner's second argument is that Krantz's disclosure of access point 209 . . . "'as a VLAN aware device [that] can insert Tag Headers into data frames received from client 205 . . . that are to be transferred to VLAN B and/or VLAN C'" is a disclosure of reconfiguring the communication port. -675 Pet. at 46; -679 Pet. at 35-36. Petitioner also argues "port 251 is 'reconfigured' by Access Point 209 because it was previously tagging

[4] *Cisco Systems, Inc. v. InfoExpress Inc.*, IPR2024-00675, Paper No. 14 at 15 (PTAB Oct. 23, 2024); *Cisco Systems, Inc. v. InfoExpress Inc.*, IPR2024-00679, Paper No. 14 at 15 (PTAB Oct. 23, 2024).

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 'the communication device' is 'reconfigured' because Port 251 tags incoming data for transfer to VLAN C rather than VLAN B." -675 Petition at 48 (cleaned up); -679 Pet. at 51.

77. Petitioner's argument is incorrect. As discussed above, in enabling a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation. The format of VLAN-tagged frames is defined in IEEE 802.1Q issued by the Institute of Electrical and Electronics Engineers (IEEE) in 1998. EX1507. A network device handles an incoming frame depending on whether the frame is VLAN tagged, and information about the VLAN tags, if any. A VLAN tag includes a TPID field, a priority field, a CFI, and a VLAN ID field. The VLAN ID field identifies the VLAN that the frame belongs to. The basic logic is set out below:



78. In Krantz, after a user is authenticated (user ID and password), data fields from the user's device are tagged to allow access to the Internet. The communication ports of the access point are not changed. Rather, data with a particular VLAN ID is directed to the preprogrammed VLAN based on this new tag. EX2566 at 5-8 (Tanenbaum).

79. When a data frame from a device is received, the VLAN aware device first checks to see if it has a VLAN tag that is in the VLAN database. If it does, the data is sent to the assigned VLAN, which in Krantz is VLAN C. If the VLAN does not have a tag the data frame is sent to where the access point is configured, i.e., pre-programmed to send untagged (or unmatched tagged) data. In Krantz, the data goes to VLAN B. If server 215 determines that data frame is from an authorized user (user ID and password) then the access point may insert a different Tag Header into the data frame to label it as corresponding to VLAN C. Essentially,

this changes the label on the data. With this different Tag Header, the data routing device 214 then directs the data frame to VLAN C.

80. The configuration of the communication ports of the access point in Krantz is not changed. If one considers access point 209 as being the claimed "access point," the association of ports 251 and 252 remain unchanged. Even if one includes the data routing device 214 as part of the claimed "access point," there is no change to the port associations. Instead, data bearing a Tag Header assigned to VLAN B or untagged will go to VLAN B, and data bearing a Tag Header assigned to VLAN C will go to VLAN C, just as was the case before the client data was authorized. It is the data frame itself that is changed, not the communication port associations. Essentially, the Tag Header is routing information that is attached to the data from the client, and the rerouting of data occurs because of the different routing information, not because of a change to the access point itself.

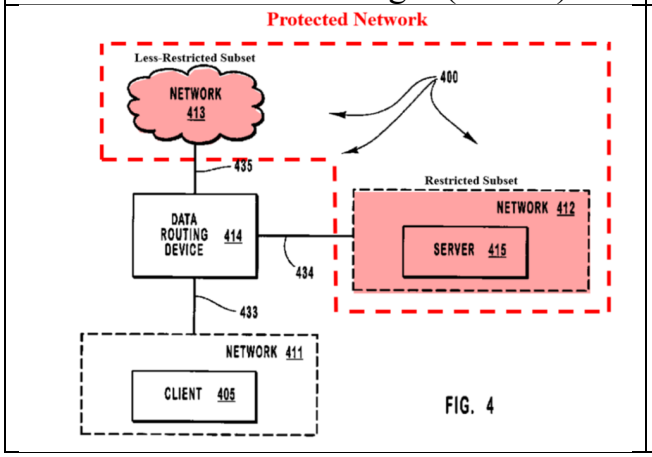
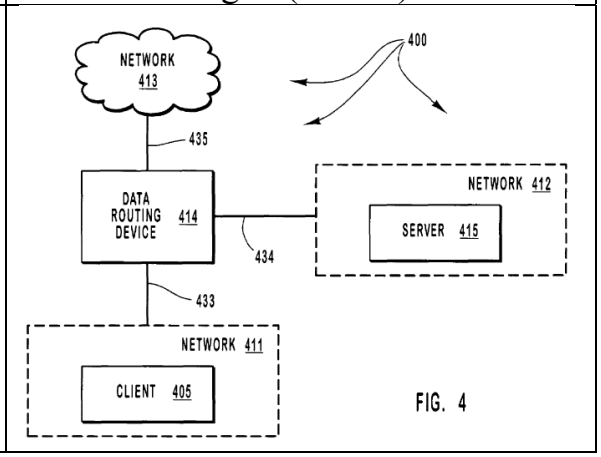
81. The Challenged Claims, however, are specific to "reconfiguring" the communication devices and communication ports themselves. It was well understood to POSTA at the time of the invention, that reconfiguration of the communication devices and ports themselves could be done by changing the instructions that correspond to a particular tag header. For example, incoming data without a tag header, rather than being sent to a RADIUS server for user

authentication, the communication devices or ports could be reprogrammed so that incoming data without a tag header are simply ignored.

82. While Krantz teaches changing a data frame's label, the Challenged Claims require something different, namely, changing how the communication devices or ports operate. This is missing in from Krantz.

B. <u>Krantz does not disclose a "less restricted subset of the protected network."</u>

83. Independent Challenged Claims 1, 28, 41, 56 and 57 each recite a "protected network" including a "less-restricted subset" and a "restricted subset." EX1501. These same claims also recite that the "restricted subset" "include[s] a gatekeeper." *Id*. Petitioner relies on Krantz's teaching of multiple networks that may communicate with one another. Dr. Houh improperly changes what Krantz actually discloses with his "annotated" figures from Krantz.

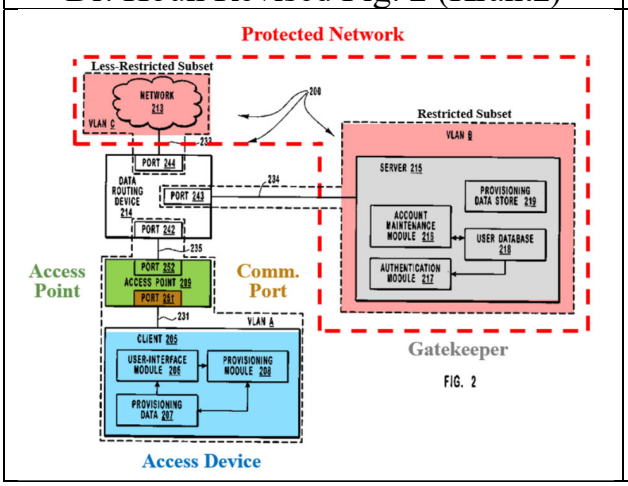
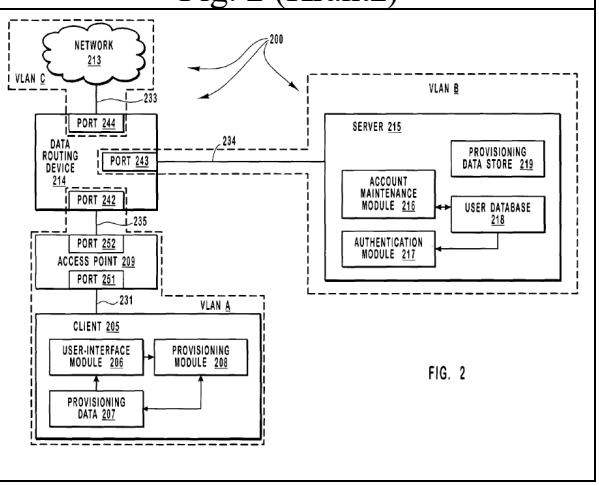
Dr. Houh Revised Fig.4 (Krantz)	Fig. 4 (Krantz)
	

-675 Pet. at 22 (citing EX1503, ¶72); -679 Pet. at 23-24 (citing EX1503, ¶241).

84. Dr. Houh changes Krantz's teaching of multiple networks so that "Network 413" and "Network 412" are falsely portrayed as a single network. It is my understanding that it is improper to consider the prior art with the benefit of hindsight, and particularly, the teachings of the patent at issue. It appears, however, that is what Dr. Houh did.

85. There is no disclosure in Krantz of a protected network with a less-restricted subset (and, by implication, a restricted subset). Indeed, it is notable that Petitioner describes Krantz's Fig. 4 as illustrating "a network architecture 400 that can provide access to a first network while restricting access to a second network." Pet. at 44. This is correct in that disparate networks are disclosed, not a protected network with subsets.

86. Dr. Houh changes what Krantz actually discloses, and uses the 484 Patent as a roadmap to redraw Fig. 2 of Krantz to portray a single network with two subsets, despite Krantz not teaching this.

Dr. Houh Revised Fig. 2 (Krantz)	Fig. 2 (Krantz)
	

55001110.2

87. Just as with Krantz's Figure 4, Krantz's Figure 2 recites separately "Network 213" and "Server 215." Petitioner is unable to point to any teaching in Krantz of ***different subsets*** (of a single, protected network). Instead, Krantz teaches only ***different networks*** that may communicate with one another. Moreover, my review of Krantz establishes that Krantz never even recites a "protected network" or "subsets" is recited. Krantz expressly teaches distinct networks, not a protected network with subsets as is claimed.

88. With Krantz's Fig. 2, server 215 is disclosed as authenticating a user, and is particularly a RADIUS server. Krantz, ¶58. Server 215 is not a subpart of network 213. Instead, Krantz states that data routing device 214 has been configured to separate network architecture 200 into VLAN's A, B, and C, i.e., three distinct networks. Krantz, ¶60.

89. Petitioner argues in the alternative that if the claimed "protected network" is a single network, Krantz discloses this. In my opinion, such an argument is based on a mischaracterization of claims, which require the "protected network" include a "restricted subset" and a "less-restricted subset" and wherein the gatekeeper is on the less-restricted subset. Even if Krantz discloses a single network embodiment, which is not explained in any detail with either Fig. 2 or Fig. 4, there is no disclosure of a restricted subset of the single network and a less restricted subset of the single network, where a gatekeeper is on the less restricted

subset. Further, Krantz's disclosure of authorizing a user to access a "selected computer system" says nothing about whether the network has restricted or less restricted subsets.

90. Petitioner fails to explain how the disclosure of a single network teaches that a less restricted subset of a protected network includes a gatekeeper. Petitioner references Krantz's Fig. 2 for a gatekeeper on a less restricted subset of a protected network. As discussed, however, Fig. 2 only discloses separate networks VLAN B (Server 215) and VLAN C (Network 213), and it is only Dr. Houh revised drawing based on hindsight that revises the prior art to disclose a "protected network." Nowhere in Krantz, however, are server 215 and network 213 described as a "protected network" or a "network" at all. Moreover, even with Krantz's passing reference to a single network, there is no disclosure of placing the gatekeeper inside the network, as opposed to outside the network.

91. Finally, Krantz's disclosure of the internet at large (e.g. at paragraph 77) does not constitute a "protected network."

C. <u>Krantz does not teach or suggest the claimed "policy auditor," "audit," or "enforcing" or "applying a security policy" claim elements.</u>

92. The Challenged Claims recite numerous limitations related to auditing the access device (i.e. the endpoint), including:

- "at least one security policy including requirements that must be satisfied before an access device is granted access" and "a policy auditor configured

to audit the access device using the at least one security policy." Claim 1,

- "applying a security policy to the access device." Claims 28, 41, and 56, and
- "a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network." Claim 57.

93. Krantz fails to disclose these "audit[ing] the access device," or "enforcing" or "applying a security policy to the access device" elements because Krantz is only directed to user "authentication." Krantz, ¶¶58, 66-68, 71-73, 76-77. "Auditing the access device" and the like are not "authentication," which relates to the user.

94. Certain dependent claims of the 484 Patent recite an authentication process that is separate and apart from device auditing. *E.g.*, claim 23 ("the network gatekeeper is further configured to authenticate a user"), 29, 53 and 65 ("further including authenticating a user of the access device"). Nevertheless, Petitioner resists this, and suggests that Krantz's disclosures of auditing meet the preamble's claimed "auditing." *E.g.*, -675 Pet. at 32 ("***Credentials*** supplied by the access device in the Krantz system are used to control access to the 'protected network' resources ('configured to audit the access device using the at least one security policy')."); -679 Pet. at 66 (arguing with respect to claim 39's recitation of "an audit" that "[c]redentials supplied by the 'access device' in Krantz are used to control access to the 'protected network' resources ('wherein the security policy includes an audit of the access device')."') (citing EX1503, ¶331).

95. The 484 Patent expressly distinguishes between user "authentication " and "auditing." "Auditing" of a device is explained at length in the 484 Patent as being directed to ensuring the **device** attempting to access the protected network meets certain software and/or hardware criteria as required to comply with the security policy.

96. The 484 Patent explains that "applying a security policy" and the like concern the access device information that is necessary to comply with a security policy, such as "operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230[.]" EX1501, 11:45-49.

97. Authentication is a different technical concept, process, and implementation from the claimed "auditing." The 484 Patent describes authentication of a user as merely confirming the identity of the user. EX1501, 1:31-37 ("A first level of access control is achieved by requiring authentication of a user. This may be accomplished by requiring the user to enter a username and password or by reading a MAC address or other identifying information from an access device. In some systems, a network switch is programmed to grant access to a secure network only after proper authentication is achieved.") Indeed, a user can

be properly authenticated, but if the access device does not have the proper antivirus software, then the network can be at risk. EX1501, 1:42–46.

98. Yet, Krantz only discloses user authentication, and fails to disclose anything about "applying a security policy that includes at least one requirements pertaining to the audit data." The Petitions and Krantz admit this:

- "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.'" -675 Pet. at 63 (quoting Krantz, ¶76); -679 Pet. at 74 (claim 53's "authenticating"); *see also* -679 Pet. at 15 (background on Krantz), 49 (claim 28's "requirements of the security policy"), 72 (claim 43's "applying the security policy");
- "If an **authenticated user** of the client 205 is authorized to access resources . . ." -675 Pet. at 40 (citing Krantz, ¶76); -679 Pet. at 74; *see also* -675 Pet. at 49, -679 Pet. at 49;
- "Krantz explains that 'a client sends credentials to the server to attempt to authenticate with the server.'" EX1503, ¶¶68, 237 (quoting Krantz, ¶16)
- "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." Krantz, ¶104 (cited in EX1503, ¶84, -675 Pet. at 29, -679 Pet. at 28).

99. With no evidence for Krantz disclosing or suggesting "auditing" or "audit data," Petitioner repeatedly cites to user authentication protocols. *See* -675 Pet. at 34 (referencing Extensible Authentication Protocol ("EAP"); including EAP-TLS and EAP-MSChapV2); -679 Pet. at 46 (same). But these are not "auditing." Rather, they are related to user authentication.

100. For example, "EAP," by definition, is an "Extensible Authentication Protocol." It says nothing about device compliance with a security policy.

101. As explained by the 484 Patent, user authentication and security policy compliance are different:

> [A]n AP (e.g., a switch or wireless access point (WAP) which is used to connect end points to the corporate network) may be programmed to prohibit access by the PC (e.g., notebook, desktop PC, PDA, or similar computing device) to the corporate network until authentication with **the authentication server passes AND an audit with the software agent with the GK** (e.g., software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria) passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

EX1501, 13:57–14:3 (ALL CAPS emphasis of "AND" in original).

102. Furthermore, the 484 Patent even explains that mere reliance on authentication techniques, including the conventional EAP authentication credentials discussed in Krantz such as usernames, passwords, etc., is insufficient to ensure that a device attempting to access a protected network meets network security policies. See EX1501, 1:41-52. That is why the 484 Patent teaches the separate security evaluation for the device by expressly claiming "a policy auditor configured to audit the access device using the at least one security policy," "applying a security policy to the access device," and "a gatekeeper configured to enforce a security policy."

103. Accordingly, Krantz does not disclose the preamble's recited "auditing a device" or the other "audit data" and "auditing" limitations of the Challenged Claims. Petitioner's three Grounds must fail.

D. **The Challenged Claims of the 484 Patent (1–6, 11–13, 15–19, 23–25, 28, 38–39, 41–43, 53, 57–59, 61–63, and 65–68) are valid because it would not be obvious to combine Krantz with Herrmann.**

104. It would not be obvious to combine Krantz with Herrmann to meet the limitations in independent Challenged Claims 1, 28, 41, 56 and 57 (and their respective dependent claims) which recite:

- "at least one security policy including requirements that must be satisfied before an access device is granted access" and "a policy auditor configured to audit the access device using the at least one security policy." Claim 1,
- "applying a security policy to the access device." Claims 28, 41, and 56, and
- "a gatekeeper configured to enforce a security policy for access to a less-restricted subset of the protected network." Claim 57.

This is so because Herrmann's techniques for enforcing security policies and obtaining audit data from an access device would not work with the proposed gatekeeper (server 215) of Krantz to control access.

105. As discussed above in Section VII.C, Krantz does not teach or suggest the claimed "policy auditor," or steps of "enforcing" or "applying a security policy."

106. With respect to combining of Krantz with Herrmann, the Petitions and/or Dr. Houh conclude the following:

- "A POSITA would recognize that checking for antivirus software based on a security policy would merely be an additional item for server 215 ("gatekeeper") and its components (e.g., authentication module 217) to check in the authentication process already disclosed by Krantz." -675 Pet. at 66; *see also* -675 Pet. at 68, 70; -679 Pet. at 13, 48, 72; EX1503, ¶¶52, 167 (citing Herrmann, Fig. 3, ¶68).

- "Krantz's server 215/authentication module, which compares the credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would additionally compare a virus protection program on an access device against approved antivirus programs. Information regarding approved antivirus software and approved connected devices could be stored in the User Database or an additional Database could be added." -675 Pet. at 15 (citing EX1503, ¶54); -679 Pet. at 15; *see also* -675 Pet. at 69; -679 Pet. at 73.

- "[A] POSITA would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as doing so would involve minimal changes to the existing Krantz system." -675 Pet. at 19 (citing EX1503, ¶64); -679 Pet. at 20 (citing EX1503, ¶64).

107. These conclusions, however, are not correct for several reasons as set forth below.

108. As an initial matter, it would not be obvious to combine Krantz with Herrmann to meet these limitation because Krantz is directed to "automation" and "provisioning"; not network security. In particular, Krantz is about reconciling "software incompatibilities" between a user device and network. In one example, Krantz seeks to enable a user device to automatically download ISP software. Krantz, ¶19. In another example, Krantz seeks a solution to modifying "HyperText

Markup Language" (HTML) "as part of Web based interface for receiving registration information." *Id.*, ¶13.

109. While Krantz does disclose user authentication, Krantz merely references established authentication paradigms of user-names, passwords, and RADIUS protocols, as a backdrop for its "provisioning" and "configuring" system. Indeed, Krantz's touchpoints on authentication are little more than checking whether the user has an paid-up account with the ISP. Krantz, ¶103. ("It may be that a presented user-interface includes only "YES" and "NO" controls for authorizing further credit card payments or other electronic payment options."); Krantz, ¶10 ("A user may be presented with an interface to enter information for registration (e.g., name, room number, credit card number, etc.). If the registration information is appropriate, the user can be authorized to access the Internet using the service.").

110. None of this these Krantz teachings are related to the claimed invention including (1) "a policy auditor configured to audit the access device using the at least one security policy (Claim 1), (2) "applying a security policy to the access device (Claims 28, 41, and 56), and (3) "a gatekeeper configured to enforce a security policy."

111. Additionally, the 484 Patent explains: "The method used to support auditing functionality over the existing 802.1x protocol implementations is

complicated and not an obvious variation of the 802.1x protocol." EX1501, 14:1-3.

112. This statement is correct because at least for the reason that the infrastructure and components for authentication were wholly different than that for auditing or policy enforcement.

113. For example, authentication generally required three key components: (1) an endpoint side ***supplicant*** that requests to be authenticated, and ***authenticator*** (i.e. an access point), which facilitates authentication, and (3) and ***authentication server***, i.e. RADIUS server, which "determines from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator." *See* IEEE 802.1X (2001) (EX2567) at 13, 15 and 19.

Figure 6-5 illustrates the relationship among the Supplicant, Authenticator, and Authentication Server, and the exchange of information among them. In this illustration, the Authenticator's controlled Port is in the unauthorized state and is therefore disabled from the point of view of access to the services offered by the Authenticator's system. The Authenticator PAE makes use of the uncontrolled Port to communicate with the Supplicant PAE, using EAPOL protocol exchanges, and communicates with the Authentication Server using EAP.

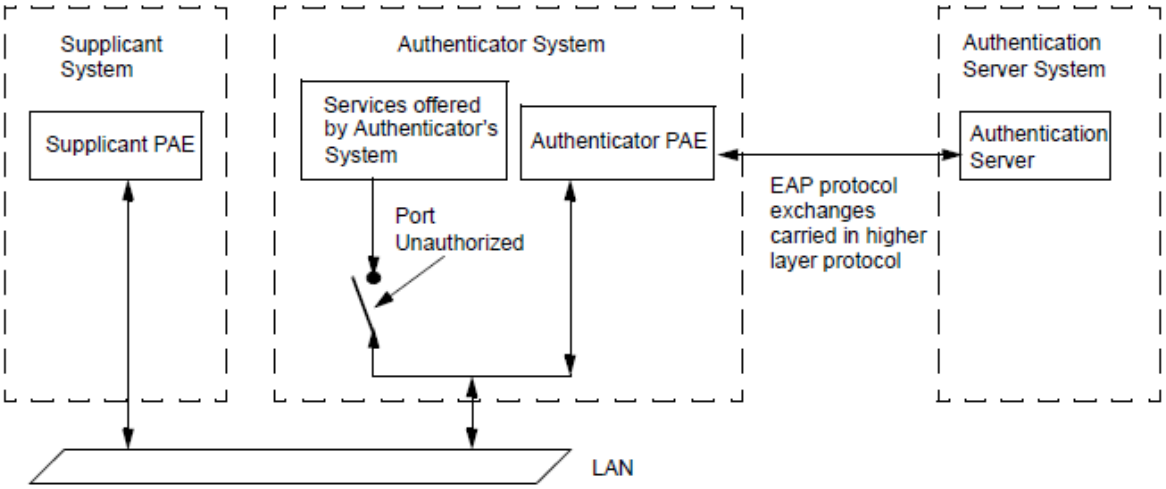


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

NOTE—The situation shown in Figure 6-5 could be found, for example, where the Supplicant's System was an end station and the Authenticator's System was a Bridge at the edge of a Bridged LAN.

IEEE 802.1X (2001) at 19; *see also id.* at 12 (citing to RFC2865, 2866, 2867, 2868, and 2869, which pertain to RADIUS).

114. In authentication using 802.1X and RADIUS server the supplicant is capable of sending a data packet carrying very simple information—that is, a username and password. This data packet is then be transmitted to the ***authenticator*** (i.e. the access point) and then to the ***authentication server*** (i.e. RADIUS server).

115. The RADIUS server is capable of making a simple determination about whether username and password are correct. The RADIUS server ***is not*** capable of processing and analyzing, and handling ***policy information***, i.e. audit

data. Audit data is very different. Rather than a simple username-password combination, audit data comprises, for example, "operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device [], Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like." EX1501, 11:45-50. Information concerning, for example, the applications ***present*** and/or ***running*** on an endpoint device takes a very different form than a simple user-password combination. From this different form, it follow that transporting and analyzing audit data required a separate and distinct infrastructure and modes of analysis.

116. At the time of invention, a RADIUS server (such as server 215 in Krantz) could not be used for auditing or policy enforcement. Accordingly, it would not have been obvious to combine Krantz and Herrmann to meet the "applying a security policy that includes at least one requirements pertaining to the audit data" and "audit data" limitations.

E. Herrmann confirms that "applying a security policy . . ." and the like would not have been "minimal," "simple", or merely an "additional check" for Krantz's Server.

117. As set forth above, the Petition and Dr. Houh conclude that combining Krantz and Herrmann would only require "minimal changes" or "simple" substitutions, EX1503., ¶¶30, 64, or that applying a security policy for antivirus

software would "merely be an additional item" for Krantz's server 215, *id.*, ¶¶90, 167; -675 Petition at 13, 66; -679 Petition at 48, 72.

118. But Dr. Houh is incorrect. As will be shown in further detail below, the information from Herrmann's client is not in a format that Krantz's alleged gatekeeper (server 215) can understand. More specifically, Herrmann's data encoded in an extended EAP protocol is not in a format that Krantz's RADIUS server can understand.

119. Krantz's server 215 is a simple RADIUS server. Krantz, ¶58. But, a RADIUS server cannot work with all formats of messages.

120. Indeed, Herrmann includes its own RADIUS server 330 (Herrmann, FIG. 4).

121. Tellingly, even Herrmann does not use RADIUS server 330 for policy enforcement. Rather than make "minimal" changes to the RADIUS 330, Herrmann designs its own unique policy evaluation infrastructure. Herrmann (FIG. 4) ("Policy (Integrity) Server 460," IGW server, proxy server, NAS). Herrmann's new policy infrastructure also adds a "policy agent 413." *See* Herrmann, FIG. 3 and FIG. 4.

122. The reason that Herrmann needs to come up with this new policy infrastructure is because you cannot modify the RADIUS server to evaluate a security policy of the access device.

123. Indeed, the RADIUS Specification RFC 2865, which Herrmann incorporates by reference (Herrmann, ¶9, states "A forwarding server MAY need to modify attributes to enforce local policy. ***Such policy is outside the scope of this document***…." EX2522. Accordingly, this is explaining that enforcement of "local policy" is outside the scope of the RADIUS specification. Thus, a POSITA would not even be able to consult the RADIUS specification to make such a modification.

124. Further, if the modifications to Krantz's server 215 would have been "minimal" or "simple," then Herrmann would have used its own RADIUS server 330 to perform the policy enforcement.

125. Instead, Herrmann creates a complex infrastructure of servers, components, and its own proprietary protocols to conduct a policy evaluation.

126. For example, Herrmann creates its own proprietary data packet and protocol called EAP-ZLX to transmit "antivirus" information. Herrmann, ¶58 ("The present invention takes advantage of the extensibility of EAP by extending EAP to support policy-based authentication systems. More particularly, an extended EAP protocol (referred to as ***EAP-ZLX***) is utilized to provide support for endpoint security negotiation in additional to typical authentication services.").

127. EAP-ZLX is a non-standardized and not recognized in the industry. As Herrmann explains, RFC2284 includes information regarding EAP. *See*

Herrmann, ¶9 (citing RFC 2284: PPP Extensible Authentication Protocol, *available at* www.ietf.org/rfc/rfc2284.txt). But nothing in RFC2284 address "EAP-ZLX" or any "extended" EAP packet.

128. Additionally, I searched for "EAP-ZLX" and found nothing to suggesting to me that it was a standard and/or widely accepted EAP protocol.

129. Even Dr. Houh agreed that "EAP-ZLX" was not and is not known. EX2449 at 264-66.

130. This is a problem because if the protocol is not known or standardized, then it will not be compatible with the RADIUS server. In this case, the policy data in EAP-ZLX would be rejected by Krantz's RADIUS server 215. *See* EX2522 ("A NAS is not required to implement all of these service types, and ***MUST treat unknown or unsupported Service-Types as though an Access-Reject*** had been received instead.").

131. As such, Herrmann's EAP-ZLX would not be compatible with Krantz's server 215.

132. Given that Herrmann's policy data in EAP-ZLX is not compatible with the RADIUS server, Herrmann then constructs a system of interconnected servers including a "Proxy Server," "Integrity Gateway Server," and "Policy Server." Herrmann, FIG. 4. All of these are specifically designed to work with one another to "unwrap," (*Id*., ¶¶82-83, FIG. 7A, 708) "wrap," (*Id*., ¶90, FIG. 7A,

705) "transform" (*Id*., ¶95, FIG. 7B, 714), "reformat" (*Id*., ¶96, FIG. 7C, 718), and send and receive various data packet transmission and messaging.

133. These specialized components include Proxy Server 440, Integrity Gateway Server (IGW) 450 and Policy (Integrity) Server 460.

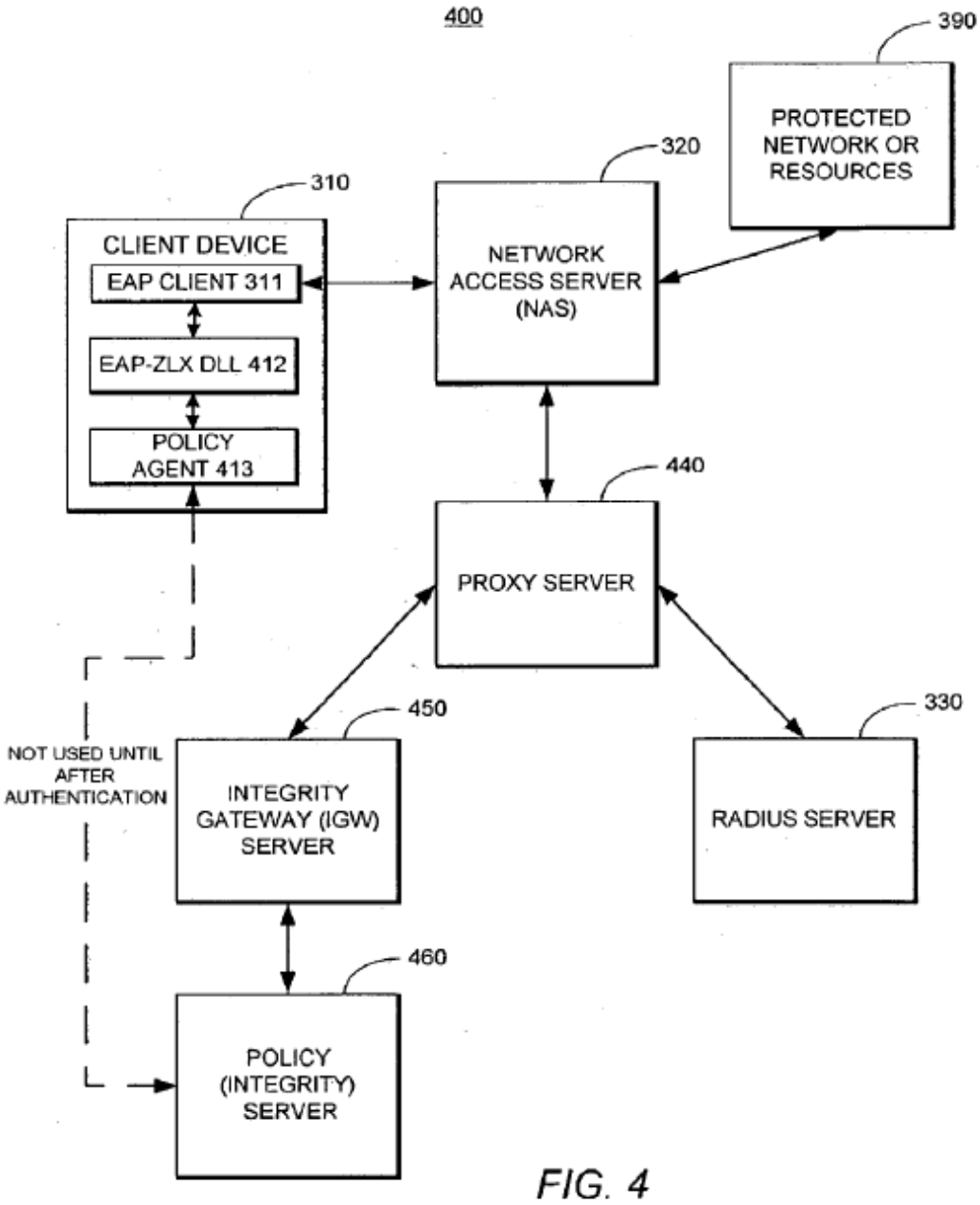


FIG. 4

134. The fact that the Proxy Server 440, Integrity Gateway Server (IGW) 450 and Policy (Integrity) Server 460 include specialized infrastructure for encapsulating and de-encapsulating the EAP-ZLX data is evident from Figure 7A–C:

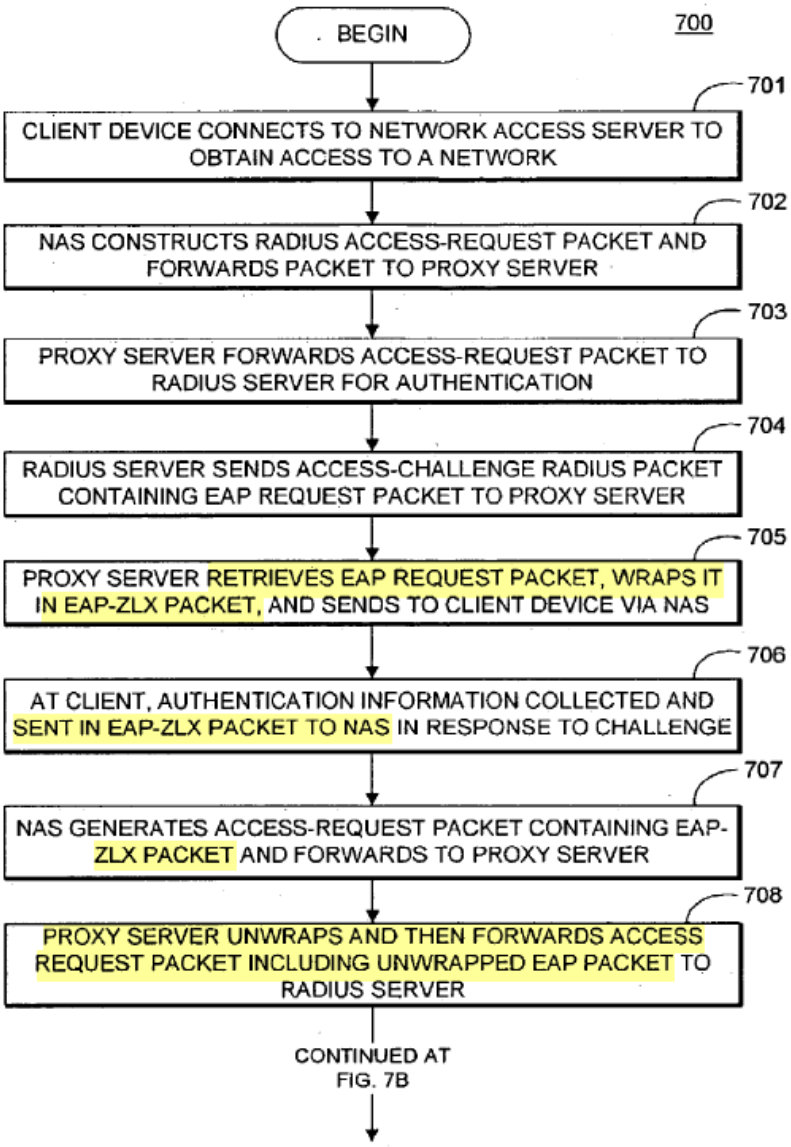


FIG. 7A

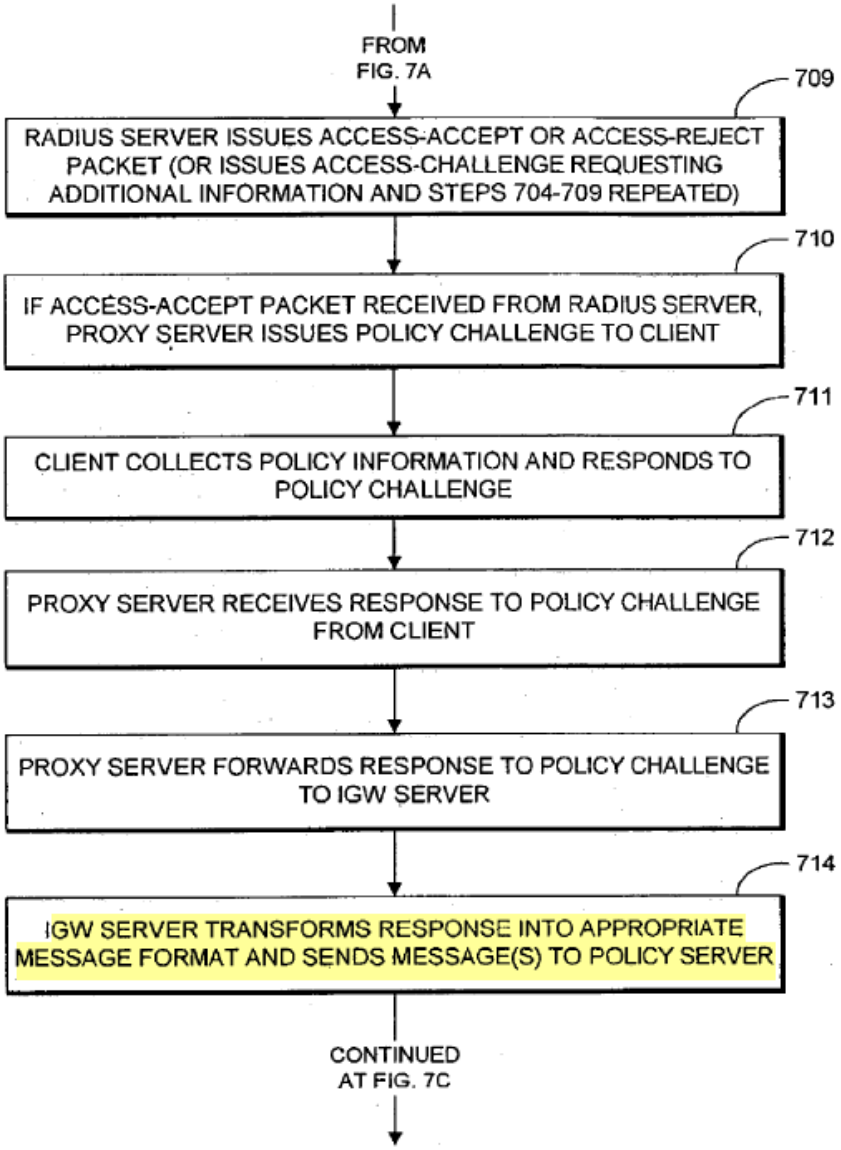

FROM
FIG. 7A
709
RADIUS SERVER ISSUES ACCESS-ACCEPT OR ACCESS-REJECT PACKET (OR ISSUES ACCESS-CHALLENGE REQUESTING ADDITIONAL INFORMATION AND STEPS 704-709 REPEATED)
710
IF ACCESS-ACCEPT PACKET RECEIVED FROM RADIUS SERVER, PROXY SERVER ISSUES POLICY CHALLENGE TO CLIENT
711
CLIENT COLLECTS POLICY INFORMATION AND RESPONDS TO POLICY CHALLENGE
712
PROXY SERVER RECEIVES RESPONSE TO POLICY CHALLENGE FROM CLIENT
713
PROXY SERVER FORWARDS RESPONSE TO POLICY CHALLENGE TO IGW SERVER
714
IGW SERVER TRANSFORMS RESPONSE INTO APPROPRIATE MESSAGE FORMAT AND SENDS MESSAGE(S) TO POLICY SERVER
CONTINUED
AT FIG. 7C

FIG. 7B

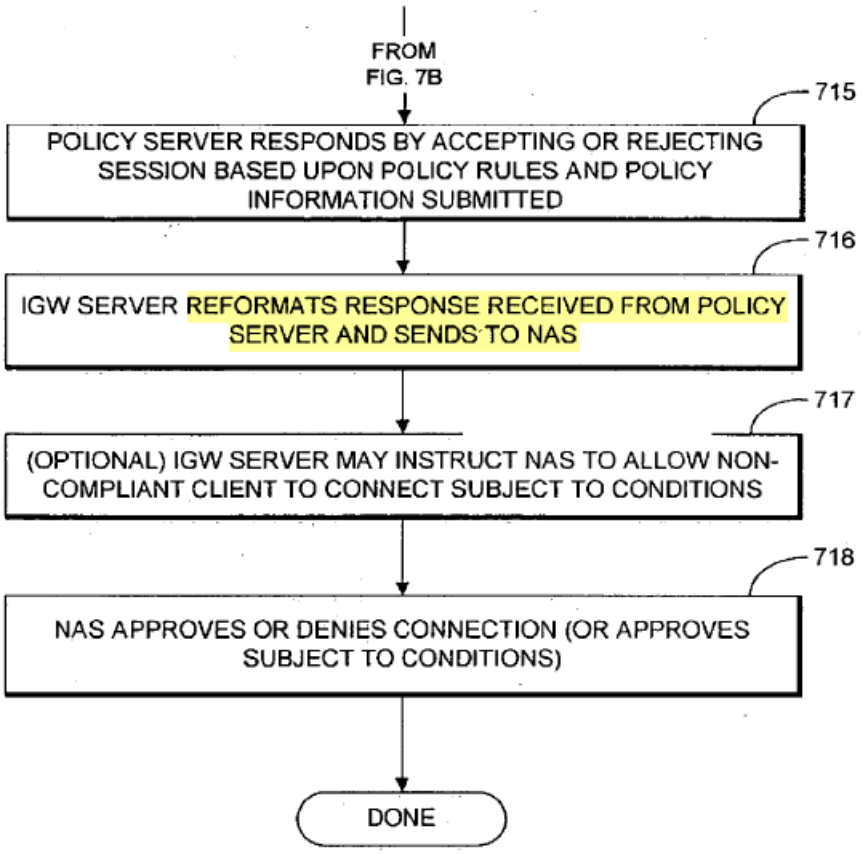


FIG. 7C

135. Herrmann Figures 7A–C and the corresponding description in the text reaffirm that Herrmann needs specialized components for processing EAP-ZLX data:

- In step 705, "Proxy server [440] retrieves EAP request packet, ***wraps it in EAP-ZLX packet***, and sends to client device via NAS [320]."
- In step 706, "At client, authentication information collected and sent in EAP-ZLX packet to NAS in response to challenge[.]"; *see also id.* at 91 ("After this authentication information has been collected, a ***wrapped EAP***

packet (EAP-ZLX type EAP packet) containing the authentication information . . . is generated and sent in reply.")

- In step 707, "NAS ***generates*** access-request packet containing EAP ZLX packet and forwards to proxy server[.]"
- In step 708, "Proxy server ***unwraps*** and then forwards access request packet including unwrapped EAP packet to RADIUS server[.]", *see also id.* at ¶92 ("On determining that the EAP packet is a wrapped packet, at step 708 the proxy server ***unwraps*** it and forwards the EAP packet that was wrapped in the EAP-ZLX packet in an Access Request RADIUS packet ***to the primary RADIUS server*** for authentication.");
- In step 714, "IGW *server* ***transforms response [to policy challenge from client, in EAP-ZLX format] into appropriate message*** format and sends message(s) to policy server[.]"; *see also id.* ¶95 (At step 714, the IGW server **transforms (i.e., converts)** the response into a message having a format that is appropriate for transmission to the policy server using the ZSP protocol.");
- In step 716, "IGW server ***reformats response*** received from policy server and sends to NAS[.]"; *see also id.* ¶96 ("At step 716, the IGW server ***reformats the response message*** received from the policy server (e.g., as a RADIUS packet) and passes the reformatted response back to the NAS.");

and

- Herrmann paragraphs 108–10 describe, "As shown at lines 30-36, if the wrap field is equal to one, the ***proxy server unwraps the packet*** and forms a new EAP packet with an EAP attribute constructed from the identity response information contained in the packet received from the client. This ***newly constructed EAP packet*** is then forwarded to the primary RADIUS server for authentication of the client. . . . The ***RADIUS server*** then evaluates the identity information contained in the EAP packet received from the proxy server.

136. These portions of Herrmann confirm that one needs specialized infrastructure to format, modify, and re-format the EAP-ZLX data to work with its "policy (integrity) server". Simply taking Herrmann's teaching EAP-ZLX packet would not be operable with a conventional RADIUS server, like Krantz's server 215.

137. User authentication is a relatively straightforward proposition, that requires checking a user ID and password against a database having authorized user ID's and passwords. By contrast, policy evaluation is highly complex. Security policy evaluation involves much more than simply checking user supplied information with a database. A stored security policy is applied to the device. This can include determining what software, such as operating system or anti-virus

software, is running on the device and whether it has the necessary updates, e.g., patches. Instead of merely relying on the device or agent on the device to simply affirm that the device complies with the security policy, the claims require the gatekeeper on the restrict subset of the network to make this determination for itself. Whereas Herrmann pushes checking security policy compliance out to the client devices, the 484 Patent specifies that the gatekeeper makes this evaluation. The 484 Patent provides the additional benefit of reducing the possibility of spoofing by the client.

138. Around the 2002-04 timeframe, traditional NAC's did not and could not counteract spoofing. In a typical posture spoofing scheme, NAC running on a central server would query the endpoint (via an agent thereon) about its overall health, e.g. operating system; in turn, the endpoint or agent would respond to that request with information. Now, if that endpoint were infected with malware, it would return "false" data depicting the endpoint's health. Having a central NAC server receive the information and perform the analysis itself (as opposed to having the agent analyze the information and return to the server a verdict) reduced some of the risks of being spoofed by malware.

139. Even if it would be simple to make a "minimal" or "simple" modification to Krantz's server 215, checking for anti-virus software as part of a security policy would not "merely be an additional item for authentication module

217 (of server 215) to check in the authentication process already disclosed by Krantz," EX1503, ¶52, as asserted by the Petition and Dr. Houh.

140. As discussed, a "check" would be insufficient. Rather, "applying a security policy . . ." per claims 28, 41 and 56 requires *an evaluation* that the anti-virus software is actually running and cannot be bypassed. Similar can be said for claim 1's "policy auditor configured to audit the access device using the at least one security policy" and claim 57's "gatekeeper configured to enforce a security policy." In fact, mere "checking" results in the industry-wide problem of spoofing or the presenting of deceptive policy information. *See* EX2445, 1 (Cisco: "RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature."). EX2446 ("Cisco's NAC can be fooled into thinking non-compliant PCs actually meet the security posture NAC is designed to enforce…); EX2447.

141. Accordingly, there would need to be an evaluation of not only the type of antivirus software, but an evaluation of the fact that the software is in fact running and not bypassed by the user or any other individual. To check if antivirus software is installed is a far different inquiry from checking whether it is running (i.e. "executing" per claim 13). For the NAC gatekeeper to determine whether

antivirus is installed, it would check the endpoint device's ***registry key*** for indicators that the software had been installed (at some point in time). But determining that the software had been installed is no guarantee that it is ***running***. To make that determination, the NAC gatekeeper would need to check the endpoint device's memory and see whether the drivers are presently loaded. This is a more intensive analysis that just checking if the software was ever installed.

142. Accordingly, a POSITA would not be motivated to combine Krantz with Herrmann.

F. <u>Herrmann's client-side system teaches away from a combination with Krantz's server-side system.</u>

143. Herrmann discloses a client-side solution which teaches away from any combination with Krantz's centralized server-side system.

144. In particular, Krantz discloses that "[n]etwork architecture 200 includes client 205 and server 215, which can each be structured as described above for computer 120." Herrmann, ¶57.

145. Further, Krantz states that "In some embodiments, server 215 logically represents a Remote Authentication Dial-In User Server ("RADIUS") server. Krantz, ¶58. Krantz's server 215 is a centralized server because the server receives data originating from various sources, such as user credentials from the 217 authentication module and credentials obtained from entries in the wider user database.

146. In contrast, Herrmann discloses a client-side solution with a client device 310 having an "EAP client 311, an EAP-ZLX extension DLL 412, and a policy (or integrity) agent 413" installed on the "client device 310." Herrmann, ¶62.

147. Herrmann incorporates by reference U.S. Patent No. 5,987,611 for explaining the "***policy definition and enforcement"*** for, *inter alia*, ***anti-virus policies***. Herrmann, ¶70. As such, the '611 Patent (EX2567) explains that "The present invention provides system and methods for client-based monitoring and filtering of access, which operates in conjunction with a centralized enforcement supervisor. **In accordance with the present invention, a central filter is not employed. Instead, the present invention provides a client-side filter** that is controlled by the centralized authority as long as the centralized authority has a way of enforcing non-compliance[.]" '611 Patent, 3:51-58.

148. The disclosure further states: "Both strategies are based on a centralized filter mechanism, with most of the filtering work being performed at the server (as opposed to the individual client PCs). Such an approach is problematic, however. Because of the centralized nature of firewalls and proxy servers, each approach extracts **significant performance penalties**. During operation of a typical system employing either approach, a single server might have to do the filtering work for hundreds or even thousands of PCs or

workstations. **This represents a major bottleneck to overall system performance.**" *Id.*, 2:38-47.

149. The disclosure further states: "As another problem, centralized filter architectures are missing vital information to correctly interpret the data packets because the underlying protocols were designed for effective data transfer and not for data monitoring and interception. '611 Patent, 2:59-63.

150. Additionally, the disclosure states: "There are still other disadvantages to centralized filtering. The approach is difficult to configure and administer. The task of setting up different rights for different users, workstations, or workgroups, for instance, is particularly difficult." '611 Patent, 3:4-8.

151. As explained above, Krantz's server 215 is centralized. Thus, it would not be obvious to combine Herrmann's client-side approach (including its infrastructure) into Krantz.

152. ***Client-side code*** is meant for code that requires user input. It needs to be kept local to minimize security risk and is lightweight in nature. Therefore, it is very common for authentication to be client side code. It requires user input, does not require a lot of computational resources, and wants to be isolated to an individual user. Sending sensitive client data to a server could be intercepted by an attacker, and thus represents a security risk.

153. ***Server side code*** is more applicable to centralized functions that require a lot of processing power and need to be done independent of the client—such as policy auditing. At the time of invention, it would not make sense to perform client-side auditing of an endpoint, because it would be resource-intensive and would negatively impact the client. Moreover, the policies to be complied with may change on a daily basis (or an even shorter timeframe). When policies need to be updated, it is easier to control server-side code than client-side code.

154. Accordingly, a POSITA would not be motivated to combine Krantz and Herrmann to meet the missing claim limitations including "applying a security policy that includes at least one requirements pertaining to the audit data."

G. Krantz and Herrmann Do Not Disclose "communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port"

155. Claim 28 is further valid is because neither Krantz nor Herrmann teaches or suggests claim 28's "communicating between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port."

156. The -679 Petition relies on Krantz's "re-authenticate" disclosure for this limitation, stating: "[i]t may be that the server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to ***re-authenticate***[.]" Pet. at 59-60. As discussed, Krantz's authentication is not

"applying the security policy" or the like. *See, e.g.*, 484 Patent, claim 28, 41, 46; *see also* claims 1, 57. Indeed, merely "re-authentication" (asking someone once again for a username and password) based on a predetermined "timeout" period would have nothing to do with "updated audit data pertaining to the ***device***" or "re-auditing" a device.

157. In the alternative, the -675 Petition relies on Herrmann's IA_HEARTBEAT to meet "re-auditing." *Id.* at 60. This argument too fails on the merits. Indeed, Herrmann does not make such a disclosure because a heartbeat is nothing more than a "status message." Herrmann, ¶80. It does not relate to "monitor security status of the access device after reconfiguring the communication port."

158. Additionally, Herrmann has a specific architecture for its policy approval process. This includes a proxy server, IGW server, and policy server that requires the policy data to be transmitted, "transform[ed]", and "reformat[ed]". EX1506, FIG. 7B-7C, 711-715. And once this process is complete, there is no indication of any additional audits.

159. Herrmann's heartbeat "status message" is separate from the policy approval process. *See* EX1506, FIGS. 7B-7C and [0080]. For one thing, the "heartbeat" is "sent from the client directly to the policy server." EX1506, [0080]; *see also* Herrmann FIG. 4 (annotated below).

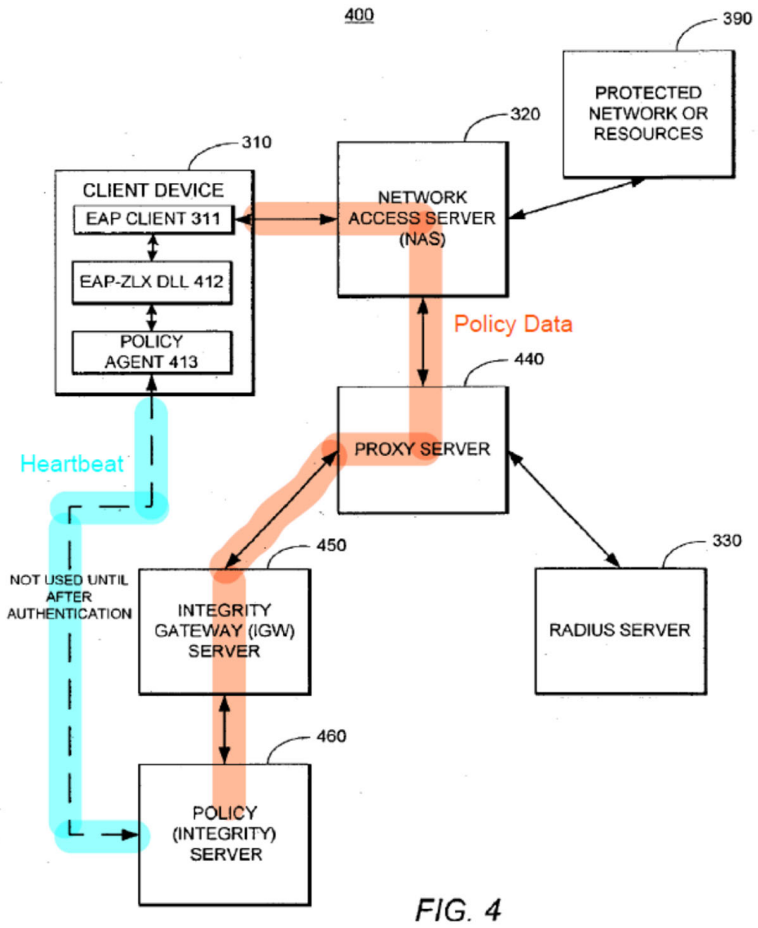


FIG. 4

160. A heartbeat message does not contain substantive policy data. Rather, it only carries minimal information to confirm if an access point is connected and active (i.e., proof of life). A status message does not contain substantive policy data but only carries minimal information to confirm an endpoint is connected. And this information is not used for evaluation or determining compliance with a security policy. Indeed, as the term "heartbeat" suggests, it is known in the art to be merely an indicator that the client device is still active and has not left the network. *See, e.g.*, EX2569.

161. Herrmann's actual "policy data 616" is something else (EX1506, [0082], FIG. 6A), and is "collect[ed]," "receiv[ed]," "transform[ed]," and "reformat[ted]" in a very different way. *Id.*, FIGS. 7B-7C. Accordingly, neither reference discloses the claimed "monitor[ing] security status of the access device after reconfiguring the communication port."

162. By contrast, the claimed "monitor[ing]" relates to whether the device configuration is still compliant with the security policy. EX1501, claim 5. A heartbeat message confers no such information.

163. Accordingly, this is an additional reason for the validity of claim 28.

H. Dependent Claims 3, 24, 38, and 41 are valid because Krantz and Herrmann do not disclose "updat[ing] the access device" and other limitations

164. For claims 3, 24, 38, and 41, Petitioner and Dr. Houh first rely on Krantz's disclosure of "provisioning files." -675 Petition at 59-60 (claim 3), 64 (claim 24); -679 Petition at 62-65 (claim 38), 68 (claim 41, referring to claim 38 and citing EX1503, ¶345); EX1503, ¶¶154-62 (claim 3) (citing Krantz, ¶¶32, 56), ¶¶221-230 (claim 24), ¶¶317-27 (claim 38), ¶¶410-413 (claim 41, and referring back to claim 38). But "provisioning files" are not relevant to whether "requirements of the security policy are not satisfied" as recited by claims 24, 38, 41.5. *See also* claim 1 (reciting a "security policy").

165. A provisioning file is a configuration file that contains details about how a device or system should be set up, including information like necessary software, network settings, user access, and other parameters. Indeed, provisioning files are merely used to configure devices with the necessary settings to connect to and operate on a network. These files ensure that the device can access network services without requiring manual configuration by the end-user.

166. Krantz itself verifies that "provisioning files" (i.e. "configuration files") are related to establishing and maintaining a communication link between the endpoint and the network. For example, Krantz explains, "[d]uring the registration process with the ISP, the computer system may download ***provisioning files*** for the wireless hotspot. Thus, upon connecting to the wireless hotspot, the computer system may already be appropriately ***configured*** for accessing the Internet through the wireless hotspot." Krantz, ¶112. This relates only to connectivity, not to security.

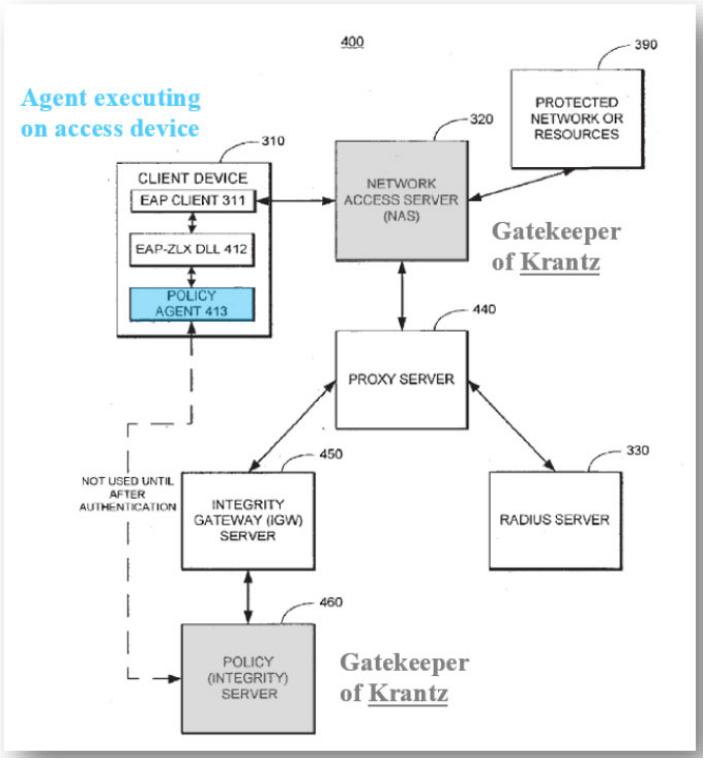
167. Similarly, Krantz also states, "A location sub-file can be an XML document defined in accordance with an XML location schema that is accessible to the computer systems depicted in network architecture 200. A location sub-file can contain a ***list of HSPs and corresponding postal addresses, hotels and airports where the [hot spot providers] HSPs are located***. Thus, a user going to a particular location may be able to ***download provisioning files for accessing a network*** (e.g.,

the Internet) from a particular location before arriving at the particular location." Krantz, ¶87. Again, this relates only to connectivity, not to security.

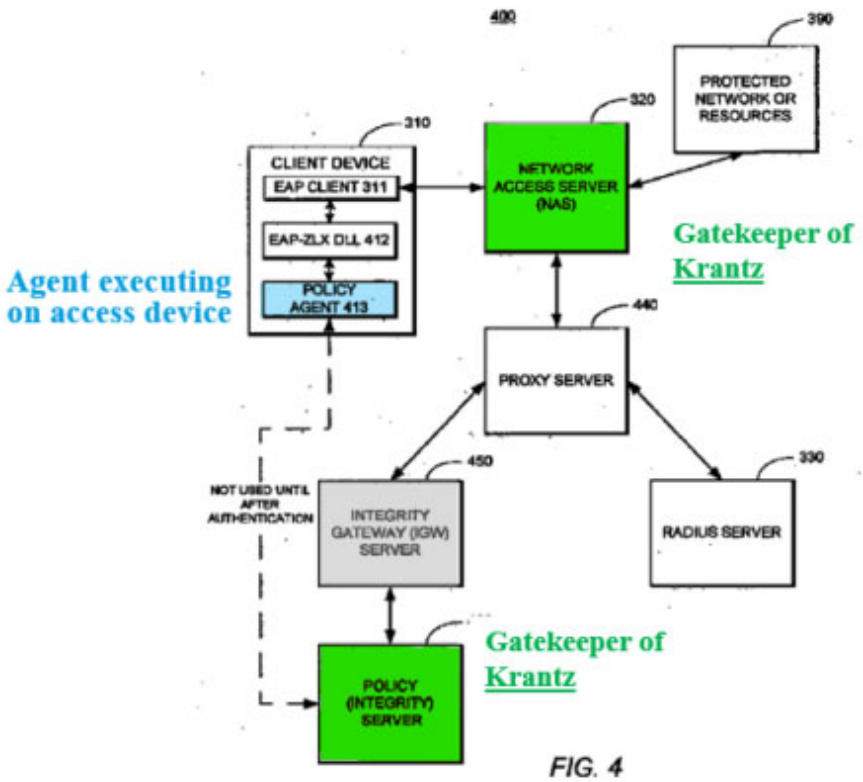
Even if "provisioning" files were related to a "security policy," claims 3 and 24 further require that "the network ***gatekeeper*** is configured to update the access device." Petitioner's proposed gatekeeper of Krantz (e.g. RADIUS server 215) takes no part in administering them and the Petitions do not say it does. -675 Petition at 59-60, 64. Nor for that matter does Herrmann disclose this. All that Herrmann does disclose is that "[i]t 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" (Herrmann, ¶12) and 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 (Herrmann, ¶71) (cited in -675 Petition at 67). Just like in Krantz, Herrmann does not teach or suggest how a "network gatekeeper" would conduct the "update" limitation.

168. As to claims 38 and 41, which recite "updating the access device if ***requirements of the security policy are not satisfied***," Petitioner tries to combine Krantz with Herrmann, arguing that "Policy server 460 of Herrmann is similar to the 'gatekeeper' (server 215) of Krantz.' -679 Petition at 63-64; *see also* EX1503,

¶325. But then the Petition and Houh go on to identity ***two*** "Gatekeeper[s] of Krantz" within Herrmann:



-679 Petition at 64;



EX1503, ¶325.

169. This defies logic. Petitioner cites Krantz's RADIUS server as the gatekeeper. Then, rather than identify Herrmann's RADIUS server 330, the Petition identifies the first "Gatekeeper of Krantz" as Herrmann's "Network Access Server (NSA)." The second "Gatekeeper of Krantz" is Herrmann's "Policy (Integrity Server)." Having two separate gatekeepers is nonsensical. Furthermore, Petitioner's recasting of Herrmann's "Network Access Server" as the claimed gatekeeper would preclude satisfaction of another limitation—"without passing data through the gatekeeper" limitation—which is present in claims 28 (on which 38 depends) and 41. Thus, there would be no reason to combine Krantz and Herrmann.

170. Accordingly, claims 3, 24, 38 and 41 are valid for these additional reasons.

VIII. CONCLUSION

171. For the foregoing reasons, it is my opinion that the Challenged Claims of the 484 Patent are valid and enforceable, as not obvious in view of Krantz, alone or in combination with Herrmann.

Date: January 29, 2025

Dr. Eric Cole

EXHIBIT A

Dr. Eric Cole

Cybersecurity, Networking, Computer, and IT Expert

44651 Provincetown Drive,
Ashburn, VA 20147

Cell Phone: (703) 909-2998
Email: ecole@secure-anchor.com
www.secure-anchor.com/expert-witness

Expert Overview

Dr. Eric Cole is a cybersecurity, networking, computer, and information technology (IT) expert who has built a solid reputation in the information technology industry over the last three decades. His educational experience includes a master's degree in computer science from the New York Institute of Technology, and a doctorate in professional studies from Pace University. Dr. Cole's expert involvement in the information technology industry is demonstrated by his appointment as the commissioner on cybersecurity for the 44th president, holding a position as a senior fellow at SANS, and being elected to the Purdue University Executive Advisory Board. The accomplishments he has earned include an induction into the Information Security Hall of Fame, and he has been awarded as a Cyber Wingman from the US Air Force. Aside from his seasoned technical expertise, he is an author of various publications, like his recently released book, Cyber Crisis, which debuted at #1 on the Wall Street Journal's BestSellers List. Dr. Cole's expertise and experience includes working with both plaintiff and defense counsel as a cybersecurity, networking, computer, and IT expert.

Types of Cases

As an expert witness, Dr. Cole provides valuable insights and technical expertise for several types of cases. Below is a list of selected, sample case types:

- Apportionment
- Infringement & Non-Infringement
- Validity & Invalidity
- Trade Secrets
- Data Breaches

Areas of Expertise

As an industry-recognized expert, with over 30 years of firsthand experience, he has built a solid background and knowledgeable insight in several areas of technology. Below is a list of selected, sample areas of expertise:

- Cybersecurity
- Networking
- Operating Systems
- E-Commerce
- Web Technologies
- Protocols and Communications

Professional Experience

Secure Anchor Consulting Services: 2005-Present
Founder and CEO
Provides consulting services to Fortune 500, Fortune 50, financial institutions, international organizations, and the federal government. Employs innovative technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide security solutions.

SANS (Sysadmin Audit Network Security): 1999-2019
Director of the Cyber Defense Initiative
Lead instructor and course developer for several security courses, including the top selling courses. One of the highest rated instructors and one of the few instructors teaching a variety of courses. Executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW). Responsible for staying up on technology and developing new course material covering the state of the art in networking, information technology, and security. Created and led several key efforts including the Level One Notebook, Top 10/20 Vulnerability List, and the Cyber Defense Initiative, which included authoring the Critical Controls for Effective Cyber Defense. Developed business plans and created new technological initiatives. Constantly researched, assessed, and evaluated new security products and research efforts.

STI (SANS Technology Institute): 1999-2015
Dean of Faculty
A member of a five-person team tasked with creating a degree-granting educational institution and obtaining certification from the state of Maryland. Offered two master's degree programs focused on technical people needing managerial skills and managers needing technical skills. Designed and implemented curriculum and provided leadership to faculty. STI successfully received accreditation from the state of Maryland.

McAfee: 2009-2011
SVP, CTO of the Americas
As McAfee's visionary and evangelist, responsible for strongly influencing the company's strategic and technical direction, development, and growth as the global leader in digital security solutions. Key leader in the execution of technology strategy for platforms, partnerships, and external relationships. Worked closely with CEO, EVP of Product Operations, and other key stakeholders to establish a product vision and road map to achieve McAfee's goals and focused on identifying and capturing intellectual property and driving innovation across the company.

Lockheed Martin: 2005-2009
IS&GS Chief Scientist LM Senior Fellow
The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. Dr. Cole was selected by Lockheed Martin for its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. As a Lockheed Martin Senior Fellow (the first Fellow within Lockheed Martin's Information Technology Division), he was a frequently invited speaker at a variety of conferences and security events. As Lockheed Martin Chief Scientist, performed research and development to advance the state-of-the art in information systems security. Specialized in secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. Played a lead technical advisory role in many high-profile, security-focused projects for Federal clients to include civil, Intel and Department of Defense, including the FBI Sentinel, DHS Eagle, JPL, Hanford, and FBI IATI programs.

The Sytex Group, Inc. (TSGI): 2001-2005
Chief Technology Officer (CTO)
Positioned the company to achieve corporate growth and meet financial targets by utilizing and enhancing technology. Worked as an executive team member to determine and implement technical direction and focus of company. Experience with running projects including managing development

efforts to exceed client requirements. Created an intellectual property portfolio that included patents, journals, books, and white papers, resulting in an overall increase in market value and customer engagement. The efforts of the research team's intellectual property increased advertising, market share and customer satisfaction through conferences, proposals, and magazine articles. Maintained full accountability for revenue of $55 million and was indirectly involved in revenue of over $80 million. Provided continuous leadership to a research team of over twenty people creating intellectual property that surpassed teams twenty times their size. Yearly patents were in line with the top one thousand producing patent companies in the United States.

Developed and executed creative techniques for influx of technology into non-technical business units to drive revenue and profit. Interfaced with government officials, including the Pentagon, The White House and Capitol Hill, and corporate executives to identify critical network security problems that needed to be addressed and researched.

GraceIC: 2000-2001
Chief Security Officer (CSO)
Designed and executed strategy for establishing GraceIC as a leader in the network security arena. Developed the product line and built the services. Managed and directed security employees. Provided leadership and implemented internal security infrastructure, such as secure email, proper protection of data and security policies. Presented at national and international conferences and authored several articles. Performed and documented research into the area of future applications and solutions to the network security problem existing in the current market. Trained salespeople, program managers and engineers on how to sell, manage, and deliver security services. Maintained a pulse on technology in the marketplace to produce market plans.

American Institutes for Research: 1999-2000
Chief Information Officer (CIO)
Brought in to fix and revamp the entire IT infrastructure based on the organization having experienced several security breaches, virus outbreaks and unreliable performance on the network. Within three months, stabilized the entire IT infrastructure and within nine months rebuilt the entire infrastructure. Designed the network to achieve a balance between functionality and security while minimizing the monetary impact to the organization. After one year, there were no severe security breaches, and all attempted breaches were contained prior to causing any significant monetary loss. Virus problems were contained and controlled, and network uptime was 99.999%. Security and performance increased while overall IT costs were reduced by 15%. In addition, provided technical support for DARPA-sponsored research projects. Helped invent technology and innovation that lead to a spin-off company, Pynapse, which created a state-of-the-art intrusion detection system known as Checkmate that was later sold to SAIC.

Vista Information Technologies: 1998-1999
VP of Enterprise Security Services
Developed the Enterprise Security Services Group and was responsible for all internal and external security issues. Tracked and managed separate profit and loss center for security. Grew the team from one person to over twelve people and executed several million in annual revenue in less than a year. Set up the security and other monitoring services for the NOC/SOC. Created all security services offerings and generated all necessary marketing and sales material. Followed and assured compliance with business plan and financial tracking of security group. Performed security assessments and consulted on all areas of security. Designed, implemented, and monitored security solutions including firewall design, intrusion detection, vulnerability assessment and penetration testing. Performed evaluation and analysis of security tools and provided technical recommendations and product improvements for VC funded startups. Key presenter at Cisco sponsored security seminars around the country and performed partnership activities with Fortune 500 organizations.

Telligent: 1996-1998
Director of Security
Created and managed IT Corporate Security Department. Pivotal point of contact for all security

concerns. Evaluated strategic plans and operational activities by performing risk assessment and determining how it might impact corporate security. Designed security solutions to meet operational needs. Integrated security and helped create NOC to provide proper monitoring of network. Developed the company's security policy and all required security guidelines. Set up lab to accurately assess and enhance the security features of the network. Performed and executed several computer investigations. Assisted and advised the legal department on laws, regulations, and policies relating to computer and information security. Evaluated several secure email solutions and installed PGP company wide. Established and set up web traffic monitoring and password tracking systems.

Central Intelligence Agency: 1991-1996
Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services
A Senior Officer of the agency that implemented the Internet Program Team that specialized in rapid development and in exploiting the latest Internet technologies to meet customers' requirements. The team designed, developed, assessed, and deployed products over three-to-six-month intervals. Designed and developed several secure communication systems. Responsible for providing technical direction, technical design, security assessment, and programming modules. Secured internal servers, continually performed intrusion detection, and reviewed audit logs. Performed independent security reviews and penetration testing of Internet servers (World Wide Web) for other offices. Identified several weaknesses and devised ways to fix those problems and secure the system. Received letter of appreciation from the Director of Central Intelligence (DCI) and six Exceptional Performance Awards.

Computer Engineer with Office of Security
Member of the information security assessment team. Evaluated and performed security assessment of network operating systems. Identified potential vulnerabilities and ways to secure the holes. Designed a large-scale auditing system with automated review capability. Worked on several virus investigations.

Education

Doctorate in Professional Studies, Pace University (2004)
Master of Science in Computer Science, New York Institute of Technology, Honors. (1994)
Bachelor of Science in Computer Science, New York Institute of Technology, Honors. (1993)

Certifications

Certified Information Systems Security Professional (CISSP)
Created several of the Global Information Assurance Certification (GIAC) programs and exams.

Organizations / Associations

Association for Computing Machinery (ACM)
Institute of Electrical and Electronics Engineers (IEEE)
Computer Security Institute (CSI)
Information Systems Security Association (ISSA)
International Computer Security Association (ICSA)
International Who's Who in Information Technology Common Vulnerability and Exposures (CVE)
HoneyNet Project - member (by invitation only)

Publications

1. Eric Cole. *Cyber Crisis.* BenBella Books, 2021.
2. Eric Cole. *Online Danger: How to Protect Yourself and Your Loved Ones from the Evil Side of the Internet.* Morgan James Publishing, 2018.
3. Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress, 2012.
4. Eric Cole. *Network Security Bible.2nd Edition.* Wiley, 2009.
5. Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollman, and Rachelle Reese. *Wiley Pathways Network Security Fundamentals Project Manual.* Wiley, 2007.
6. Eric Cole and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress, 2006.
7. Eric Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* Wiley, 2003.
8. Eric Cole. *Hackers Beware: The Ultimate Guide to Network Security.* New Riders/Sams Publishing, 2001.

Recent Expert Witness Experience

Providence Publications LLC v. NBCUniversal, United States District Court for the Central District of California,

C.A. No. 2:23-cv-8551

Provided expert report services to plaintiff Providence Publications LLC.

Infinite Media v. John Hancock Life Insurance Company (U.S.A.), Ontario, Superior Court of Justice

Case No. CV-18-000610487-0000; CV-19-00622400-0000

Provided expert report services to defendant/counterclaimant John Hancock Life Insurance Company (USA).

CosmoKey Solutions GMBH & CO. KG v. Duo Security, Inc. n/k/a Duo Security LLC and Cisco Systems, Inc., United States District Court for the District of Delaware,

C.A. No. 18-1477-CFC

Provided expert report services for plaintiff CosmoKey Solutions.

Proxense, LLC v. Google LLC and Google Payment Corp., United States District Court for the Western District of Texas,

C.A. No. 6:23-cv-320

Provided expert report and deposition services for plaintiff Proxense.

Carbyne Biometrics, LLC, v. Apple Inc., United States District Court for the Western District of Texas (Austin Division),

C.A. No. 1:23-cv-00324

Provided expert report, rebuttal report, and deposition services to plaintiff, Carbyne Biometrics.

Gemedy Inc. v. The Carlyle Group Inc., Carlyle Investment, Management LLC, L.P. Carlyle Partners VII, L.P. Carlyle Partners VIII, L.P. Two Six Labs holdings, Inc., Two Six Labs, LLC, 1st Research, LLC, Two Six Topco Holdings, Inc., and Two Six Technologies Holdings, Inc., United States District Court for the District of Delaware,

Case No.: 23-cv-157-CFC

Provided expert report, reply report, and deposition services to plaintiff, Gemedy.

Smith v. Bluewater Health, Transform Shared Service Organization, Chatham-Kent Health Alliance, and Erie Shores HealthCare, and HOTEL-DIEU Grace Healthcare, and Windsor Regional Hospital, Ontario Superior Court of Justice,

Court File No. CV-00000199-00CP

Provided expert report services to defendant Bluewater Health.

Cisco Systems, Inc. and Fortinet, Inc., v. InfoExpress, Inc., United States Patent and Trademark Office,

IPR2024-00540

Provided IPR Response Declarations in support of defendant, InfoExpress Inc.

United States of America ex rel., Alex Permenter, Eric Rodighiero, and Chris Wheeler, v. eClinicalworks, LLC, United States District Court for the Middle District of Georgia (Macon Division),

Case No. 5:18-CV-382

Provided expert report, supplemental report, rebuttal report, and deposition services for plaintiffs Relators, Alex Permenter, Eric Rodighiero, and Chris Wheeler.

Greater New York Mutual Insurance Company v. SKOUT Monitoring, LLC and Consolidated Technologies, Inc., Supreme Court of the State of New York, County of New York,

Index No. 650539/2022

Provided expert report services for plaintiff Greater New York Mutual Insurance Company.

Video Solutions PTE. LTD. v. Cisco Systems, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Civil Action No. 2:23-cv-222-JRG

Provided expert declaration, expert report, rebuttal report, and deposition services for Plaintiff Video Solutions, PTE. LTD.

Correct Transmissions, LLC v. Juniper Networks, Inc., United States District Court for the Eastern District of California,

Case No. 3:21-cv-09284-RFL

Provided expert report services for Plaintiff Correct Transmissions, LLC.

I-Mab Biopharma v. Inhibrx, Inc. and Brendan Eckelman, United States District Court for the District of Delaware,

C.A. No. 22-276 (VAC) (CJB)

Provided expert report and testimony services for Defendant, Inhibrx, Inc.

Acceleration Bay LLC v. Amazon Web Services, Inc. United States District Court for the District of Delaware

Case No. 22-904-RGA-SRF

Provided expert report and testimony services for Plaintiff, Acceleration Bay LLC.

Kidd v. Springhill Hospitals, Inc., et al., In the Circuit Court of Mobile County, Alabama,

Case No. CV-20-900171-BBH 2-5

Provided expert deposition services for Defendant, Springhill Hospitals, Inc.

K.Mizra LLC v. Hewlett Packer Enterprises Company and Aruba Networks, LLC, United States District Court for the Eastern District of Texas (Marshall Division),

Civil Action No. 2:21-cv-305

Provided expert report, supplemental report, and deposition Services for Plaintiff, K.Mizra LLC.

Lionra Technologies Ltd. v. Fortinet, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:22-cv-00322-JRG-RSP (Lead Case)

Expert report, declaration, and deposition services for Plaintiff, Lionra Technologies, Ltd.

Lionra Technologies Ltd. v. Cisco Systems, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:22-cv-00305-JRG-RSP (Member Case)

Expert report, declaration, and deposition services for Plaintiff, Lionra Technologies, Ltd.

Lionra Technologies Ltd. v. Palo Alto Networks, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:22-cv-00334-JRG-RSP (Member Case)

Expert report, declaration, and deposition services for Plaintiff, Lionra Technologies, Ltd.

Correct Transmissions, LLC v. Nokia Corporation, Nokia Solutions and Networks OY, and Nokia of America Corporation, United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:22-cv-0343-JRG-RSP

Provided expert report and deposition services for Plaintiff, Correct Transmissions, LLC.

Identity Security v. Apple, United States District Court Western District of Texas (Austin Division)

Case No. 22-cv-58-ADA

Provided expert report, supplemental report, deposition and testimony services for Plaintiff, Identity Security LLC.

United States of America ex rel., Alex Permenter, Eric Rodighiero, and Chris Weeler v. eClinicalWorks, LLC, United States District Court for the Middle District of Georgia, Macon Division,

Case No. 5:18-CV-382

Provided expert report services to Plaintiffs, Permenter et al.

Smart Path Connections LLC v. Nokia, Corp., United States District Court for the Eastern District of Texas (Marshall Division)

Case No. 2:22-cv-00296-JRG-RSP

Provided expert report and testimony services for Plaintiff, Smart Path Connections LLC.

AlphaSense v. Tegus & BamSEC, United States District Court for the District of Delaware,

Case No. 1:23-cv-0103

Provided expert declaration and deposition services for Plaintiff, AlphaSense.

Novadine, Inc. v. Panda Restaurant Group, Inc., JAMS Arbitration,

Ref. No. 5220000746

Provided expert report, deposition, and trial testimony services for Plaintiff, Novadine, Inc.

R.N Nehushtan Trust Ltd. v. Apple Inc, United States District Court for the Northern District of California, San Francisco Division,

Case No. 3:22-cv-01832-WHO

Provided expert report and deposition services to Plaintiff, R.N. Nehushtan Trust Ltd.

Centripetal Networks, LLC v. Palo Alto Networks, Inc., United States District Court for the Eastern District

of Virginia (Norfolk Division),

Case No. 2:21-cv-00137-EWH-RJK

Provided expert report, deposition, and testimony services to Plaintiff, Centripetal Networks, LLC.

Google LLC v. Valtrus Innovations Limited, United States Patent and Trademark Office,

Case IPR2022-01545, IPR2022-01497

Provided patent holder Valtrus Innovations Limited with IPR expert declaration and deposition services.

Option3 Cyber Investments, LLC, v. Centripetal Networks, Inc., Circuit Court for the County of Fairfax, Virginia,

Case Nos. 2021-10652, 2021-15490

Provided expert report and deposition services to Defendant, Centripetal networks, Inc.

Optionality Consulting Pte. Ltd. v. Edge Technology Group LLC, James Nekos, and John Pecoraro, United States District Court for the Southern District of New York,

Case No. 18-cv-05393

Provided expert report and deposition services for Defendant, Edge Technology Group, LLC.

Adventist Health System Sunbelt Healthcare Corporation v. RxCrossroads, LLC, d/b/a Covermymeds, LLC, United States District Court for the Middle District of Florida (Orlando Division),

Case No. 6:22-cv-880-PGB-LHP

Provided expert declaration services for Plaintiff, Adventist Health System Sunbelt Healthcare (2023).

Celgard, LLC v. Shenzhen Senior Technology Material Co., et al., United States District Court for the Northern District of California,

Case No. 19-cv-05784-JST

Provided expert report services for Plaintiff, Celgard, LLC.

Unisys Corporation v. Leon Gilbert, Michael McGarvey, Atos SE, and Atos IT Solutions and Services, Inc., United States District Court for the Eastern District of Pennsylvania

Case No. 2:23-CV-00555-PD

Provided expert report and deposition services to Plaintiff, Unisys Corporation.

K.Mizra, LLC, v. Cisco Systems, Inc., United States District Court for the Western District of Texas (Waco Division),

Case No. 6:20-cv-01031-ADA

Provided expert report and deposition services for Plaintiff, K.Mizra LLC.

Janssen Products, L.P. v. eVenus Pharmaceuticals Laboratories, Inc., United States District Court for the District of New Jersey,

Case No. 3:20-cv-09369-ZNQ-LHG

Provided expert declaration services for Plaintiff, Janssen Products, L.P.

Future Field Solutions, LLC, et al. v. Erik Van Norstrand, Circuit Court for Howard County, Maryland,

Case No. C-13-CV-22-000581

Provided expert report and deposition services and participated in hearing for plaintiff Future Field Solutions, LLC.

In the Matter of Certain Computer Network Security Equipment and Systems, Related Software, Components Thereof, and Products Containing Same, United States District Court for the Eastern District of Virginia (Norfolk Division),

Inv. No. 337-TA-1314 (ITC).

Provided an expert report, declaration, and testimony on behalf of Plaintiff, Centripetal Networks (2023).

Virtru Corporation v. Microsoft Corporation, United States District Court for the Western District of Texas (Waco Division),

IPR No. IPR2023-00019

Provided expert declaration services for Plaintiff, Virtru Corporation.

Ivanti, Inc. v. Patch My PC, LLC, United States District Court for the District of Colorado,

Case No. 1:22-cv-00643-RMR-SKC

Provided declaration and deposition services for Plaintiff, Ivanti, Inc.

Genesis 1 Oil Services, LLC v. Wismann Group LLC, United States District Court for the Central District of California,

Case No. 8:20-cv-02114-SSS-ADS

Provided expert declaration services for Plaintiff, Genesis 1 Oil Services LLC.

Palantir Technologies Inc. v. Marc L. Abramowitz, United States District Court for the Northern District of California (San Jose Division),

Case No. 5:19-cv-06879-BLF

Provided expert reports, trial prep, and deposition services for Plaintiff, Palantir Technologies Inc. (2022).

CUPP Cybersecurity LLC, et al. v. *Trend Micro, Inc., et al.*, United States District Court for the Northern District of Texas (Dallas Division),

Case No. 3:18-cv-01251-M

Provided expert reports and deposition services for Plaintiff, CUPP Cybersecurity LLC.

Sarah Freele v. ADT, LLC, United States District Court for the Northern District of Texas (Dallas Division),

Case No. 3:21-cv-01104-X

Provided expert report data breach and data compromise for Plaintiff, Freele (2021).

Unified Patents, LLC v. Monarch Networking Solutions, LLC, United States Patent and Trademark Office,

Case No. IPR2020-01708

Provided expert declaration for Plaintiff, Unified Patents (2022).

Sunstone Information Defense v. International Business Machines Corporation, United States District Court for the Western District of Texas (Waco Division),

Case No. 6:20-cv-01033-ADA

Provided expert reports, depositions, demonstrations, and testimony on behalf of Plaintiff, Sunstone Information Defense (2022).

Boston Scientific Corp., et al. v. Nevro Corp., United States District Court for the District of Delaware (Wilmington),

Case No. 1:18-cv-00644-CFC-CJB

Provided opening report and deposition services for Plaintiff, Boston Scientific Corp. (2018).

Shana Doty v. ADT, LLC d/b/a ADT Security Services, United States District Court for the Southern District of Florida (Fort Lauderdale Division),

Case No. 20-cv-60972

Provided expert witness consulting services, expert report, and deposition services on behalf of Plaintiff, Shana Doty (2020).

United States of America v. Lucy Xi, United States District Court for the Eastern District of Pennsylvania,

Criminal Action: 16-22-5

Provided expert witness consulting services on behalf of Defendant, Lucy Xi (2021).

Centripetal Networks, Inc. v. Lookingglass Cyber Solutions, Inc., et al., United States District Court for the Eastern District of Virginia (Richmond Division),

Case No. 3:21-cv-000597

Provided expert witness consulting services on behalf of Plaintiff, Centripetal Networks, Inc. (2022).

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. v. Communication Technologies, Inc., United States Patent and Trademark Office,

Docket No. 9843-0140IP1

Provided expert declaration services for Plaintiff, Samsung Electronics Co., Ltd.

WSOU Investments, LLC d/b/a Brazos Licensing and Development v. F5 Networks, Inc., United States District Court for the Eastern District of Virginia (Alexandria Division),

Case No. 3:20cv724

Provided expert reports and deposition services for Plaintiff, WSOU Investments.

Trustees of Columbia University in the City of New York v. Nortonlifelock, Inc., United States District Court for the Eastern District of Virginia (Richmond Division),

Case No. 3:13-cv-00808

Provided expert reports, depositions, demonstrations, and testimony on behalf of Plaintiff, Trustees of Columbia University in the City of New York (2022).

Appian Corporation v. Pegasystems Inc. and Youyong Zou, Fairfax County Circuit,

Court Case No. 2020-07216

Provided expert reports, depositions, demonstrations, and testimony on behalf of Plaintiff, Appian Corporation (2022).

Sprint Communications L.P. v. Charter Communications Inc., et al., United States District Court of Kansas (Kansas City),

Case No. 2:20-cv-02161

Provided expert witness consulting services on behalf of Defendant, Charter Communications Inc. (2021).

Root Insurance Co. v. Genpact (UK) Ltd., JAMS Arbitration

REF. No. 1450007525

Provided expert reports, depositions, and arbitration support on behalf of Respondent, Genpact (UK) Ltd. (2022).

Securities and Exchange Commission v. Zhoubin Hong, et al., United States District Court for Central District of California,

Case No. 2:20-cv-04080-MCS

Provided expert report on behalf of the Plaintiff, Securities and Exchange Commission (2021).

Synopsys, Inc. v. Risk Based Security, Inc., United States District Court for the Eastern District of Virginia (Richmond Division),

Case No. 3:21-cv-00252

Provided expert report, deposition, and demonstration on behalf of Plaintiff, Synopsys, Inc. (2022).

Cox Automotive, Inc., et al. v. The Reynolds and Reynolds Company, American Arbitration Association,

AAA Case No. 01-19-0000-4548

Provided expert report on behalf of Respondent, The Reynolds and Reynolds Company (2021).

Fortinet, Inc., v. Forescout Technologies, Inc., United States District Court for the Northern District of California (San Francisco Division),

Case No. 3:20-cv-03343-EMC

Provided expert declaration, expert report, and deposition services for Defendant, Forescout Technologies, Inc.

Bitglass, Inc. v. Netskope, Inc. et al., United States District Court for the Northern District of California (San Francisco Division),

Case No. 3:20-cv-005216

Provided expert report on behalf of Plaintiff, Bitglass, Inc. (2020).

802 Systems, Inc. v. Cisco Systems, Inc., United States District Court for the Eastern District of Texas (Marshall Division),

Case No. 2:20-cv-00315-JRG

Provided expert declaration infringement and validity for Plaintiff, 802 Systems, Inc. (2020).

Fourth Dimension Software v. Der Touristik Deutschland GMBH, United States District Court for the Northern District of California,

Case No. 19-CV-05561-CRB

Provided expert report, deposition, and trial testimony services for Plaintiff, Fourth Dimension Soft

ware.

Energy Intelligence Group, Inc. v. *Kirby Inland Marine, L.P.*, United States District Court for the Southern District of Texas (Houston Division),

Case No. 4:19-cv-03520

Provided expert report and deposition services for Plaintiff, Energy Intelligence Group, Inc.

Freshub, Inc., et al. v. Amazon.com, Inc., et al., United States District Court for the Western District of Texas (Austin Division)

Case No. 1:19-CV-00885-ADA

Provided expert report, deposition, and trial testimony services on behalf of Plaintiff, Freshub Inc.,

et al. (2021).

Finjan, Inc. v. Cisco Systems, Inc., United States District Court for the Northern District of California,

Case No. 5:17-cv-00072-BLF-SVK

Provided expert report and deposition testimony on behalf of Plaintiff, Finjan, Inc. (2020).

NexStep, Inc. v. Comcast Cable Communications, LLC, United States District Court for the District of Delaware,

Case No. 19-1031 (RGA)(SRF)

Provided expert reports and deposition services to Plaintiff, NexStep, Inc.

Unified Patents, Inc. v. Kioba Processing, LLC, US Patent Trial, and Appeals Board,

Case No. IPR2020-01695

Provided expert declaration on behalf of Plaintiff, Unified Patents, Inc. (2020).

Unified Patents, LLC, v. Biometric Associates, L.P., United States Patent and Trademark Office,

File No. 4910-101

Provided expert declaration services for Plaintiff, Unified Patents, LLC.

Mark Voelker v. BNSF Railway Company, United States District Court of Montana Missoula Division,

Case No. 9:18-CV-00172-DLC

Provided expert report on behalf of Defendant, BNSF Railway Company (2020).

Finjan, Inc. v. Qualys, Inc, United States District Court for the Northern District of California

Case No. 4:18-cv-07229-YGR

Provided expert report and deposition services for Plaintiff, Finjan, Inc.

BrandRep, LLC v. Ruskey, et al., Court of Chancery of the State of Delaware,

Case No. 2018-0541-SG

Provided expert report and deposition testimony on behalf of Defendant, Ruskey, et al. (2020).

Association of Owners of Kukui Plaza v. American Savings Bank FSB, Circuit Court of the First Circuit, State of Hawai‘i,

Case No. 18-1-0660-05

Provided expert report on behalf of Defendant, American Savings Bank FSB (2020).

Finjan, Inc. v. SonicWall, Inc., United States District Court for the Northern District of California

Case No. 5:17-cv-04467-BLF

Provided expert report and deposition services for Plaintiff, Finjan, Inc.

Finjan, Inc. v. Rapid7, Inc. and Rapid7, LLC, United States District Court for the District of Delaware

Case No. 1:18-cv-01519-MN

Provided expert report and deposition services for Plaintiff, Finjan, Inc.

Centripetal Networks, Inc. v. Cisco Systems, Inc., United States District Court for the Eastern District of Virginia,

Case No. 2:18-cv-00094

Provided expert report, deposition testimony, and trial testimony on behalf of Plaintiff, Centripetal Networks, Inc. (2020).

Unified Patents v. TransactionSecure, LLC, United States Patent Trial and Appeals Board,

Case No. IPR2020-00321

Provided written declaration on behalf of the Petitioner, Unified Patents (2019).

Glenn Winder v. Marriott International, Inc., et al., Ontario Court of Superior Justice,

Case No. CV-1800611365-00CP

Provided written opinion on behalf of the Plaintiff, Glenn Winder (2019).

Fortinet, Inc. v. British Telecommunications Public Limited Company, United States Patent Trial, and Appeals Board,

Case No. IPR2019-01327 and IPR 2019-01328

Provided written declaration on behalf of the Patent Owner, British Telecommunications (2019).

Finjan, Inc. v. Juniper Network, Inc., United States District Court for the Northern District of California,

Case No. 3:17cv5659

Provided expert report, deposition testimony, and trial testimony on behalf of Plaintiff, Finjan, Inc. (2019).

Vivian Deveroux V. Apple, Inc., Superior Court of the State of California County of Santa Clara,

Case No. 1-14-cv-271773

Provided expert report and deposition testimony on behalf of Plaintiff, Vivian Deveroux (2019).

United States of America v. Shan Shi, et al., United States District Court for the District of Columbia,

Case No. 1:17-cr-00110-CRC

Provided trial testimony on behalf of Defendant, Shan Shi, et al. (2019).

Colortokens, Inc. v. Medovich, United States District Court for the Northern District of California,

Case No. 3:18-cv-2444

Provided expert opinion on behalf of Defendant, Medovich. (2019).

Avepoint, Inc. v. Onetrust, LLC., Patent Trial and Appeals Board, Post Grant Review,

Case No. PGR 2018-00056

Provided expert report on behalf of Plaintiff, Avepoint, Inc. (2019).

Finjan, Inc. v. *ESET, LLC, et al.,* United States District Court for the Southern District of California,

Case No. 3:17-cv-0183-CAB-BGS

Provided expert report, deposition, and trial services for Plaintiff, Finjan, Inc.

Centripetal Networks, Inc. v. Keysight Technologies, United States District Court for the Eastern District of Virginia,

Case No. 2:17-cv-3836

Provided expert report, deposition testimony, and trial testimony on behalf of Plaintiff, Centripetal Networks, Inc. (2018).

Gubarev, et al. v. Buzzfeed, Inc., et al., United States District Court for the Southern District of Florida,

Case No. 0:17-cv-60426

Provided expert report on behalf of Plaintiffs, Gubarev, et al. (2018).

Daniel Bennett v. Lenovo (Canada), Inc., et al., Ontario Superior Court of Justice,

Court File No. CV-15-00523714-00CP

Provided expert consultation on behalf of Plaintiff, Daniel Bennett (2018).

Finjan, Inc. v. Blue Coat Systems, Inc., United States District Court for the Northern District of California,

Case Nos. 5:15-cv-3295; 5:13-cv-3999

Provided expert report, deposition testimony, and trial testimony on behalf of Plaintiff, Finjan, Inc. (2018).

Zscaler, Inc. v. Symantec Corporation, United States Patent Trial, and Appeals Board,

Case No. IPR2018-00929

Provided written declaration on behalf of the Patent Owner, Symantec Corporation (2018).

YLD Limited v. The Node Firm, LLC, et al., United States District Court for the Northern District of California (San Francisco),

Case No. 3:16-cv-399

Provided expert report and deposition testimony on behalf of the Defendants(2017).

Phishme, Inc. v. Wombat Security Technologies, Inc., United States District Court of Delaware,

Case No. 1:16-cv-403

Provided expert report, deposition testimony, and supplemental expert report on behalf of Plaintiff, Phishme, Inc. (2017).

Smith, et al. v. Federal Title & Escrow Company, et al., United States District Court for the District of Columbia,

Case No. 1:17-cv-1580

Provided expert opinion on behalf of Plaintiffs (2017).

Unified Patents, Inc. v. Universal Secure Registry, LLC, US Patent Trial, and Appeals Board,

Case No. IPR2018-00067

Provided expert declaration, deposition testimony, and supplemental expert declaration on behalf of Plaintiff, Unified Patents, Inc. (2017).

BASCOM Global Internet v. AT&T Mobility, LLC, United States District Court for the Northern District of Texas,

Case No. 3:14-cv-03942

Provided expert report on behalf of the Defendant, AT&T Mobility, LLC. (2017).