

CISCO SYSTEMS, INC. AND FORTINET, INC.

PETITIONERS

v.

INFOEXPRESS INC.

PATENT OWNER

IPR2024-00539 (U.S. PAT. No. 8,051,460)

IPR2024-00675 (U.S. PAT. No. 7,523,484)

IPR2024-00676 (U.S. PAT. No. 8,677,450)

IPR2024-00677 (U.S. PAT. No. 8,578,444)

IPR2024-00679 (U.S. PAT. No. 7,523,484)

PETITIONERS' HEARING DEMONSTRATIVES – JULY 17, 2025

Challenged Claims and Grounds

Patent	Claims	Basis	Reference(s)
460 Patent	1-6, 10-14, 16-22, 27, 29-30	103	Krantz
	1-6, 10-14, 16-22, 27, 29-30	103	Krantz, Hermann
484 Patent (1)	1-6, 11-13, 15-19, 23-25	103	Krantz
	1-6, 11-13, 15-19, 23-25	103	Krantz, Hermann
484 Patent (2)	28, 38-39, 41-43, 53, 56-59, 61-63, 65-68	103	Krantz
	28, 38-39, 41-43, 53, 56-59, 61-63, 65-68	103	Krantz, Hermann
450 Patent	1-4, 7-10 ,14, 16, 22-23, 25, 27	103	Krantz
	1-4, 7-10 ,14, 16, 22-23, 25, 27	103	Krantz, Hermann
444 Patent	1-7, 10, 12-17, 22	103	Krantz
	1-7, 10, 12-17, 22	103	Krantz, Hermann

E.g., Paper No. 13 (ID), 6 (460 Patent)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539

Roadmap

- **Challenged Patents Overview**

- **Prior Art Overview**

- **Motivation to Combine**

- **Disputed Patentability Issues**

- Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
- Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
- Krantz teaches “applying a security policy” and related elements
- Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
- Krantz teaches “updat[ing] the access device . . .” and related elements

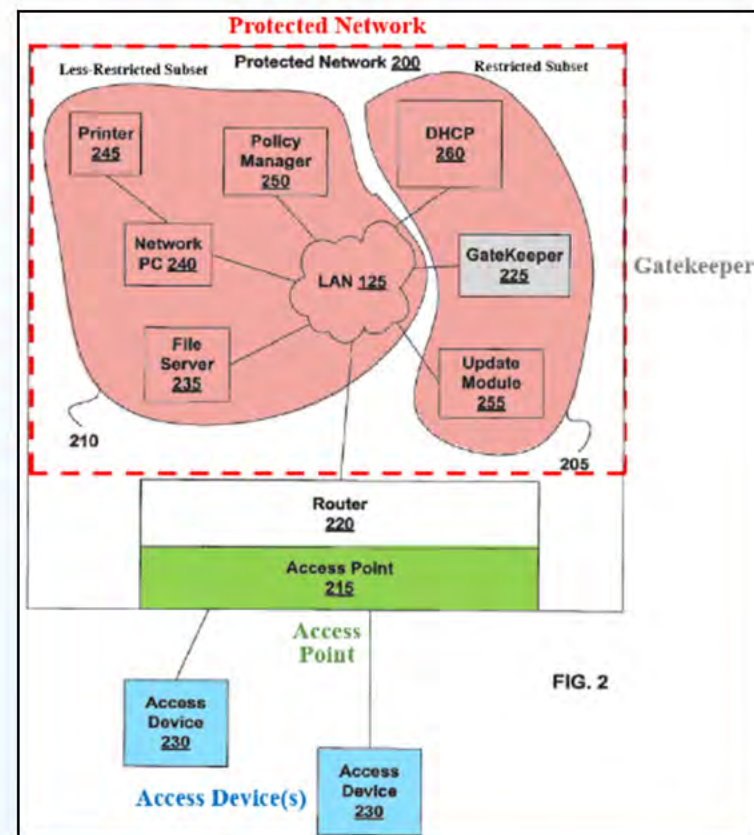
- **Secondary Considerations**

- **Conception & Diligent Reduction to Practice**

Challenged Patents Features

Systems and methods of the invention include a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets. Requests from an access device for access to the less-restricted subset are first passed to the restricted subset. Elements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network. The passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point. After access is granted, further communication between the access device and the protected network can include access to the less restricted subset.

Ex. 1001, 2:52-65

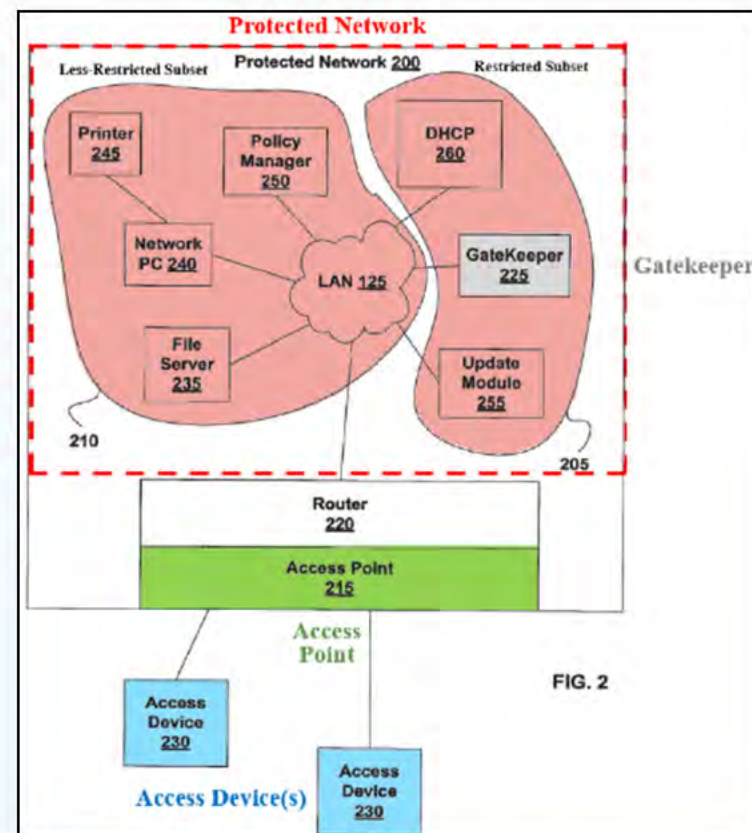


Ex.1001, Fig. 2 (annotated)

Challenged Patents Features

Systems and methods of the invention include a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets. Requests from an access device for access to the less-restricted subset are first passed to the restricted subset. Elements (e.g., a gatekeeper) of the restricted subset are then used to apply security policies to the access device and if security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network. The passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point. After access is granted, further communication between the access device and the protected network can include access to the less restricted subset.

Ex. 1001, 2:52-65



Ex.1001, Fig. 2 (annotated)

Challenged Patents Features (Cont'd)

Security Policy

GateKeeper 225 is configured to enforce one or more security policies against an instance of Access Device 230 attempting to access Protected Network 200. The security polices may include requirements for user identification such as user names and passwords, configuration requirements relating to the configuration of Access Device 230, application requirements relating to applications running on Access Device 230, or the like. For example, in one embodiment

collection of third party data regarding Access Device 230. In some embodiments, Authenticate User Step 440 is considered part of the security policy audit.

In optional Authenticate User Step 440, Policy Auditor 325 authenticates the identity of Access Device 230 and/or a user of Access Device 230. This authentication may be required by a member of Security Policies 330A-330B. In various

Reconfiguring

Logic 317. For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. In response, Access Control 320 sends appropriate commands to Switch Logic 317. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310. In alternative

Claim 1 of the '460 Patent

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

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

[1.2] the request received through a communication port of an access point;

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

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

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

Disputed Limitations – Claim 1 of the '460 Patent

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

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

[1.2] the request received through a communication port of an access point;

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

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

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

Additional Disputed Claims – 22 and 27 of the '460 Patent

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

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

Claim 1 of the '484 Patent

[1.0] 1. A network gatekeeper comprising:

[1.1] at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;

[1.2] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and

[1.3] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy,

[1.4] the restricted subset of the protected network including the gatekeeper.

Disputed Limitations – Claim 1 of the '484 Patent

[1.0] 1. A network gatekeeper comprising:

[1.1] at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;

[1.2] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and

[1.3] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy,

[1.4] the restricted subset of the protected network including the gatekeeper.

Additional Disputed Claims – Claims 3 and 24 of the '484 Patent

[3] The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module.

[24] The network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.

Claim 28 of the '484 Patent

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

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

[28.2] the request being received through a communication port of an access point,

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

[28.4] the restricted subset including a gatekeeper; applying a security policy to the access device, responsive to the request;

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

[28.6] 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 for communicating between the access device and the less-restricted subset.

Disputed Limitations Claim 28 of the '484 Patent

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

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

[28.2] the request being received through a communication port of an access point,

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

[28.4] the restricted subset including a gatekeeper; applying a security policy to the access device, responsive to the request;

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

[28.6] 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 for communicating between the access device and the less-restricted subset.

Additional Disputed Claims – 38, 41, 42, 43, 53 of the '484 Patent

[38] The method of claim 28, further including updating the access device if requirements of the security policy are not satisfied.

[41.6] . . . updating the access device if requirements of the security policy are not satisfied.

[42] The method of claim 41, wherein the security policy includes an audit of the access device.

[43] The method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy.

[53] The method of claim 41, further including authenticating a user of the access device.

Claim 1 of the '450 Patent

[1.0] A method for applying a security policy to network devices:

[1.1] performing an authentication of a device connected to an access point,

[1.2] scanning the device to collect information regarding the device,

[1.3] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and,

[1.4] configuring the access point in response to a result of applying the security policy;

Disputed Limitations Claim 1 of the '450 Patent

[1.0] A method for applying a security policy to network devices:

[1.1] performing an authentication of a device connected to an access point,

[1.2] scanning the device to collect information regarding the device,

[1.3] applying a security policy, the security policy including one or more requirements pertaining to the authentication and the information, the application of the security policy taking place in response to a gatekeeper, and,

[1.4] configuring the access point in response to a result of applying the security policy;

Additional Disputed Claims – 2, 10, 16, 22, 23, 25, 27 of the '450 Patent

[2] The method claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper.

[10] The method claim 1, wherein one of the requirements pertains to a status of an operating system
exon [sic] the device.

[16.2] / [22.2] . . . applying a security policy to the access device in response to the request, application of the security policy including performing an audit of the access device;

[16.3] / [22.3] . . . providing information to the access device to improve compliance of the access device to the security policy, in response to the audit;

[23] The method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device.

[25] The method of claim 22, wherein performing the audit includes receiving operating system information from the access device.

[27] The method of claim 22, wherein the information includes a software update of software on the access device.

Claim 1 of the '444 Patent

[1.0] A method for auditing a device, the method comprising:

[1.1] performing an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol;

[1.2] sending a request for audit data to an agent running on the device;

[1.3] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;

[1.4] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.

Disputed Limitations - Claim 1 of the '444 Patent

[1.0] A method for auditing a device, the method comprising:

[1.1] performing an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol;

[1.2] sending a request for audit data to an agent running on the device;

[1.3] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;

[1.4] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.

Additional Disputed Claims – 2-7, 12, 17, 22 of the '444 Patent

- [2]** The method of claim 1, wherein applying the security policy includes configuring the access point.
- [5]** The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device after configuring the access point.
- [6]** The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network.
- [7]** The method of claim 2, further comprising continuing to receive at the gatekeeper, from the agent, audit data pertaining to the device after the configuring of the access point.
- [12]** The method of claim 1, wherein the received audit data includes information that concerns operating system of the device.
- [17]** The method of claim 1, wherein the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.
- [22.6]** . . . where applying the security policy includes configuring the access point.
- [22.7]** . . . receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network;
- [22.8]** . . . re-auditing the device in accordance to the security policy using the received updated audit data.

Roadmap

- Challenged Patents Overview
- **Prior Art Overview**
- Motivation to Combine
- Disputed Patentability Issues
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz Overview

[0060] As depicted in network architecture 200 data routing device 214 is connected to network 213, server 215, and access point 209 by corresponding logical communication links 233, 234, and 235 respectively. Network 213 can be virtually any type of network, such as, for example, a corporate or enterprise-wide network or the Internet. Data routing device 214 can be a device capable of grouping computer systems together in a single broadcast domain based on criteria other than physical location (e.g., a physical location on a particular side of a router). Thus, data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.

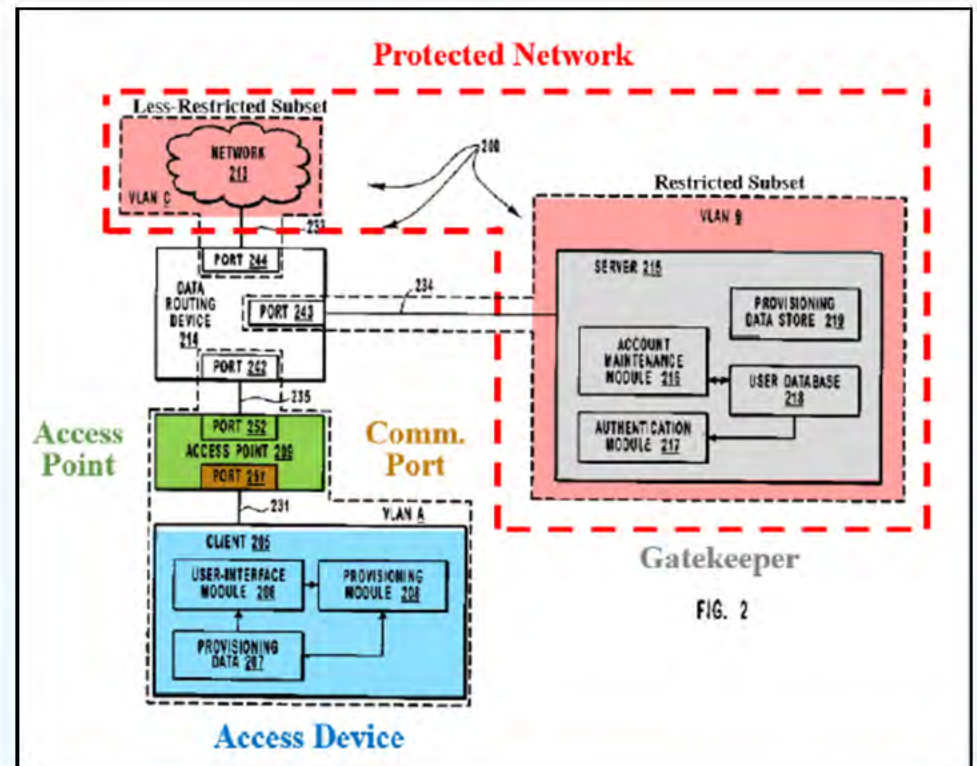


FIG. 2

Ex. 1005, [0060]; 460 Pet., 9; 450 Pet., 9; 444 Pet. 64., 484 (1st) Pet. 51; 484 (2nd) Pet., 53

Ex. 1005, Fig. 1 (annotated); 460 Pet., 8; 450 Pet., 8; 444 Pet. 8., 484 (1st) Pet. 65; 484 (2nd) Pet., 8

Krantz Overview

Security Policy

A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the server may authorize the client for at least partial access to the second network and/or may deny access to the second network and authorize the client for at least partial access to the first network. The server can be a Remote Authent-

type field. When the configuration of EAP is indicated, further numeric values (e.g., the numeric value 13 to indicate EAP-TLS or the numeric value 25 to indicate PEAP) can be included in a LCP packet to indicate the specific EAP type of authentication that is desired.

selected EAP type. For example, when EAP-TLS is selected, client 205 may communicate with server 215 through a series of EAP messages in accordance with EAP-TLS so as to be authenticated and possibly authorized to access resources located on VLAN C.

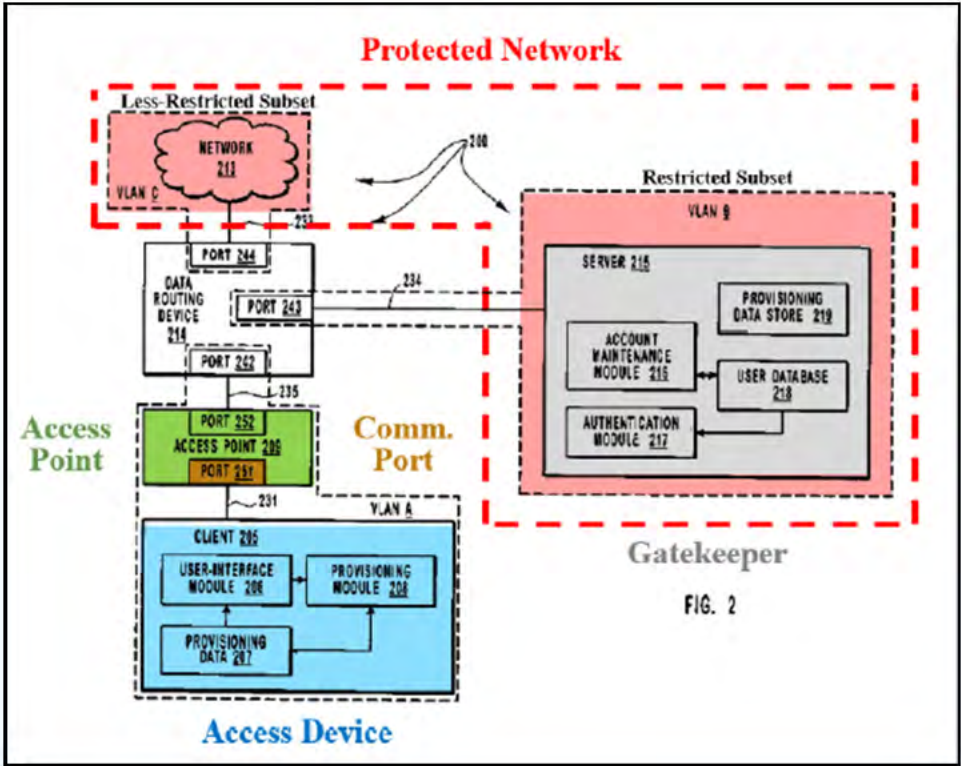
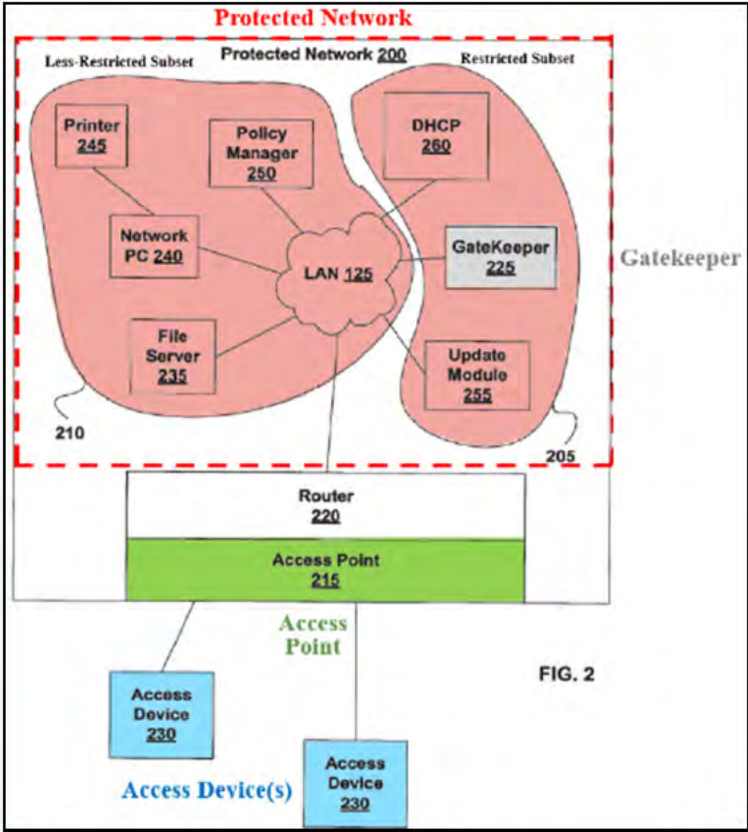
Ex. 1005, [0016], [066-068]; 460 Pet., 9, 38-40; 444 Pet., 10; 484 (1st) Pet., 9, 33-35; 484 (2nd) Pet., 9, 16, 45

Reconfiguring

[0107] When client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.

Ex. 1005, [0107], 460 Pet., 42-44; 450 Pet., 40-42; 444 Pet., 54-56; 484 (1st) Pet. 62-64; 484 (2nd) Pet. 49-51

Krantz Overview

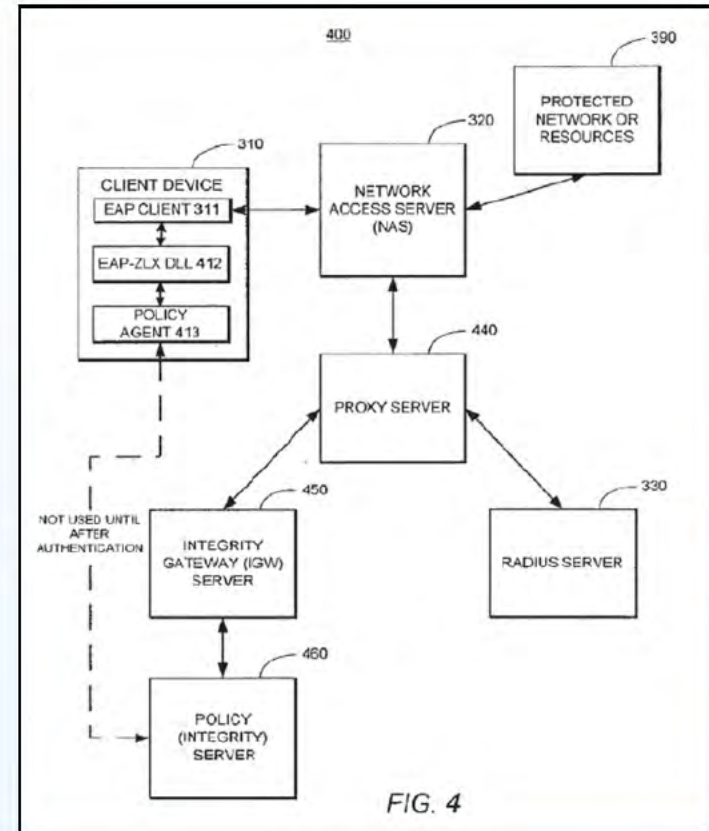


Ex. 1001, Fig. 1 (annotated); Ex. 1005, Fig. 1 (annotated); 460 Pet., 8; 450 Pet., 8; 444 Pet., 8; 484 (1st) Pet., 8; 484 (2nd) Pet., 8

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Herrmann Overview

individuals or groups. In response to a message from the IGW server 450 (or a subsequent message from the policy agent 413 on the client device 310), the policy server 460 evaluates whether or not the client device 310 has a correct, up-to-date version of the applicable security policy. The policy server 460 also serves in an enforcement role. In the event a client device does not have the correct policy loaded or the policy server 460 detects some other problem, it may instruct the NAS 320 to deny network access to a client device.



Ex. 1006, [0067], Fig. 4; 460 Pet., 12-13; 450 Pet., 13-14; 444 Pet., 13-14; 484 (1st) Pet., 12-13; 484 (2nd) Pet., 12-13

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Roadmap

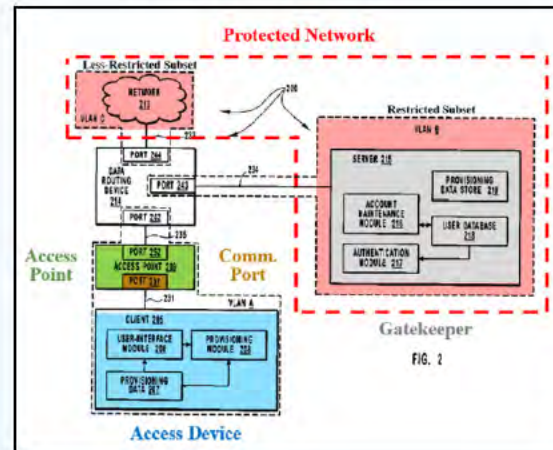
- Challenged Patents Overview
- Prior Art Overview
- **Motivation to Combine**
- Disputed Patentability Issues
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

The Krantz-Herrmann Combination

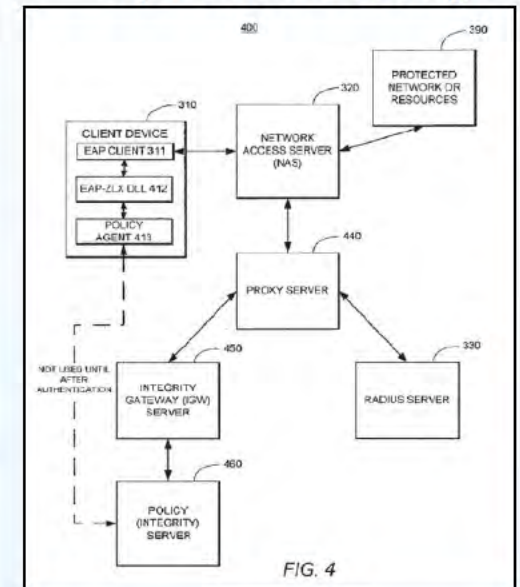
Applies Herrmann's teachings of enforcing security policies to Krantz's system

It would have been obvious to combine Herrmann's techniques related to determining whether an access device is authorized for network access (including checking its antivirus software) with the authentication and authorization system of Krantz. Each performs the same function (authentication and authorization to access network resources) with each yielding not more than what one would expect from such an arrangement (automated network access techniques including a higher level of security by checking antivirus software), as the Krantz/Herrmann system demonstrates. Ex.1003, ¶62.

Krantz's system



Herrmann's security policy enforcement teachings



460 Pet., 64-65; 484 (1st) Pet., 18-19; 484 (2nd) Pet., 18-19; 450 Pet., 14, 17; 444 Pet., 14, 43; Ex.1005, Fig.2; Ex.1006, Fig. 4.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

The Krantz-Herrmann Combination's Obviousness Rationale

Petition

A POSITA would have been motivated to combine Herrmann with Krantz based on the teachings of Krantz. For example, Krantz explains that its system relates to a server that “includes the functionality to authorize clients to access a second network” EX.1005, [0016]. Similarly, Herrmann explains that “[t]he present invention relates [] to .. policy enforcement on computer systems connected to one or more networks...” EX.1006, [0003]. Ex.1003, ¶63.

A POSITA would have also been motivated to apply Herrmann's technique of checking connecting computer systems for antivirus software as it would not only provide added security but increase automation when connecting to a network. Ex.1006, [0068]. These are two stated goals of Krantz. Ex.1005, [0014], [0019]. Thus, a POSITA would have recognized that Herrmann's disclosure of a policy server checking that a computer device complies with, e.g., an antivirus security policy, would be complimentary to the system of Krantz, which seeks an automated process for providing network security. In addition, a POSITA would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as doing would involve minimal changes to the existing Krantz system. Ex.1003, ¶64.

The Krantz-Herrmann Combination's Obviousness Rationale

Patent Owner's arguments misunderstand the references and misapply the law

POR

First, Krantz and Herrmann are directed to different things. While Herrmann relates to network security, Krantz is directed to "automation" and "provisioning"; not network security. EX1005, title, [0002]. Krantz is about reconciling "software incompatibilities" between a user device and network. E.g., Krantz seeks to enable a user device to automatically download ISP software. EX1005, [0020].

Rather, Krantz's RADIUS server 215 analysis is basic. It receives a username and password, it checks a database, and it outputs an acceptance or rejection. EX1005, [0076]. This was well-known, and it required few resources. EX2565, ¶¶46, 111, 120-21.

"Integrity Gateway (IGW) Server 450, Proxy Server 440). Herrmann's new policy infrastructure also adds a "policy agent 413" and custom EAP-ZLX extension. EX1006, (comparing FIG. 3 and FIG. 4). The reason for this new policy infrastructure—as Herrmann suggests—is that you cannot modify the RADIUS server to evaluate a security policy of the access device. See EX2522⁵ (RADIUS

The Krantz-Herrmann Combination's Obviousness Rationale

Patent Owner's arguments misunderstand the references and misapply the law

Petitioner Reply

InfoExpress suggests that Krantz and Herrmann are non-analogous art. POR, 28. But Krantz and Herrmann are both directed toward the same field of endeavor of the 460 Patent—Network Security—Petition, 61-62 (citing Ex.1005, Abstract; Ex.1006, Abstract. Ex.1003, ¶56), and reasonably pertinent to a problem described by the 460 Patent—the reliance “on mere user authentication” and the need to “assure that an access device used by the authenticated user meets network security policies” such as current anti-virus software. Ex.1001, 1:45-60. Both references teach additional aspects to a security policy. Petition, 62 (citing

InfoExpress's argument that Herrmann teaches away¹ from a server-side solution is also incorrect. Herrmann is directed to enforcement at a policy server. Ex.1006, [0067]. Herrmann teaches that its “policy server 460 evaluates whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.” Ex.1006, [0067]-[0068]. Contrary to InfoExpress's assertion, Herrmann teachings are specifically directed to server-side security policy enforcement.

460 Reply, 12-13; 484 (1st) Reply, 12-13; 484 (2nd) Reply, 13-14; 450 Reply, 12-13; 444 Reply, 11-12.

The Krantz-Herrmann Combination's Obviousness Rationale

Patent Owner's arguments misunderstand the references and misapply the law

POR

Krantz and Herrmann would also not be combined together because they disclose two different types of processing arrangements. Krantz describes a centralized server analysis. Herrmann describes a client-side analysis. They would not work together.

For example, Krantz's server 215 (the alleged "gatekeeper") is nothing more than a centralized RADIUS server. EX1005, [0058]. This means that it receives authentication data originating from various client sources. Upon receipt, *the server processes* the authentication data. EX2565, ¶143.

In contrast, Herrmann is a client-side solution. EX1006, [0062]. That means *the client device processes* the information. As incorporated by reference⁷,

Cole Dep.

8 Q. Okay. So you're stating that sort of
9 the -- all the hardware components of Herrmann
10 wouldn't work with Krantz. Is that what you're
11 stating?

12 A. All the software, all the different
13 software components.

14 Q. Okay. So you're stating that you
15 couldn't -- you wouldn't be able to physically
16 combine them?

17 A. Yeah. It wouldn't be obvious to
18 combine those for performance reasons and others.

The Krantz-Herrmann Combination's Obviousness Rationale

Obviousness is not about bodily incorporation

United States Court of Appeals
for the Federal Circuit

ALLIED ERECTING AND DISMANTLING CO., INC.,
Appellant

v.

GENESIS ATTACHMENTS, LLC,
Appellee

2015-1533

Appeal from the United States Patent and Trademark
Office, Patent Trial and Appeal Board in No. 95/001,352.

Decided: June 15, 2016

DANIEL H. BREAN, The Webb Law Firm, Pittsburgh,
PA, argued for appellant. Also represented by RICHARD L.
BYRNE, JAMES G. PORCELLI.

RYAN WAYNE MASSEY, Harness, Dickey & Pierce, PLC,
Troy, MI, argued for appellee.

Before NEWMAN, DYK, and WALLACH, Circuit Judges.
WALLACH, Circuit Judge.

Allied Erecting and Dismantling Co., Inc. ("Allied")
appeals the United States Patent Trial and Appeal

claimed inventions are rendered obvious by the teachings of the prior art as a whole.”). “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference,” *In re Keller*, 642 F.2d 413, 425 (CCPA 1981). *See also In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) (citing *In re Keller*, 642 F.2d at 425), but rather whether “a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention,” *Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1361 (Fed. Cir. 2007).

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- **Disputed Patentability Issues**
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Patent	Disputed Limitation
460 Patent	[1.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied.
484 Patent (1)	[1.3] an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy,
484 Patent (2)	[28.5] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper, if requirements of the security policy are satisfied; and
450 Patent	[1.4] configuring the access point in response to a result of applying the security policy;
444 Patent	[2] The method of claim 1, wherein applying the security policy includes configuring the access point. [22.6] . . . where applying the security policy includes configuring the access point.

Krantz Teaches “configuring” (Mapping #2)

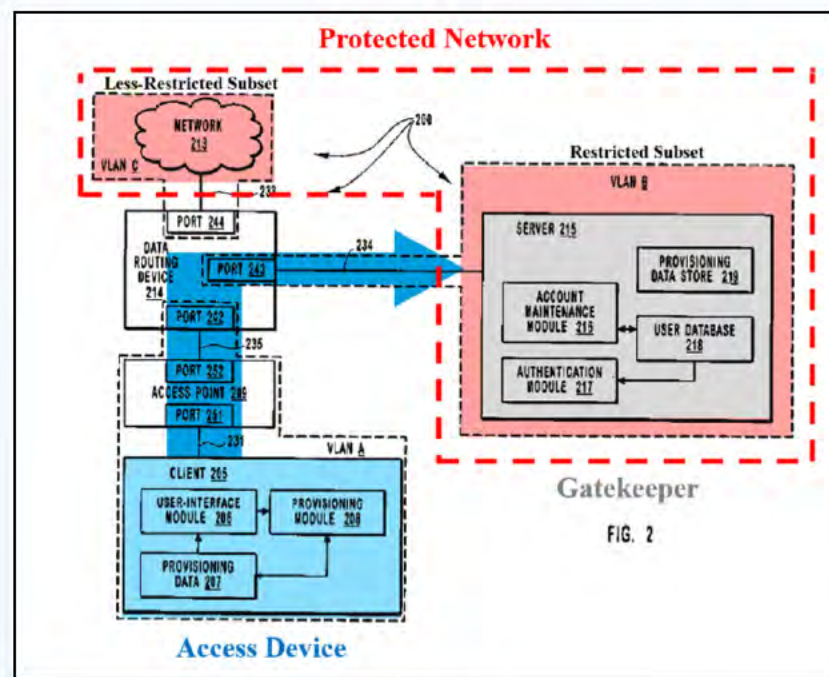
[460 Patent] *the communication port configured for communicating between the access device and a restricted subset of the protected network . . .*

Petition

Mapping #2

Second, Krantz explains that “Access point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 (or any other computer system on VLAN A) that are to be transferred to VLAN B and/or VLAN C. Ex.1005, [0064]. Krantz is therefore explaining that when configured as a “VLAN aware device,” Krantz’s Port 251 (the “communication port”) “is configured for communicating between the access device and a restricted subset of the protected network” because Access Point 209 configures Port 251 to insert VLAN Tag Headers into incoming data frames from a client that may only access VLAN B—the “restricted subset.” Ex.1005, [0064];

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE



460 Pet., 28-30; 484 (1st) Pet., 46; 484 (2nd) Pet., 35-36; 450 Pet., 49-51; 444 Pet., 63-64; Ex.1005, [0064], [0107], Fig.2 (annotated).

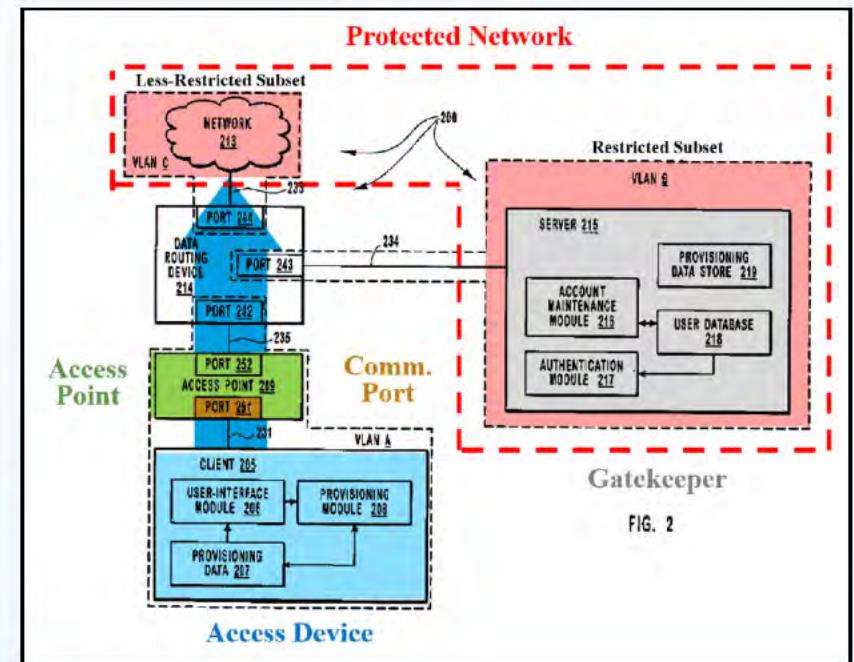
Ex. 1029
IPR2024-00539

Krantz Teaches “reconfiguring” (Mapping #2)

[460 Patent] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper . . .

Petition

Dr. Houh explains that Krantz is describing that when configured as a “VLAN aware device,” Krantz’s “*access point*” is “*reconfiguring the communication port [Port 251 of Krantz] for communicating data between the access device and the less-restricted subset of the protected network*” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client that may now access VLAN C, i.e., the “*less-restricted subset*.” Ex.1005, [0107]; Ex.1003, ¶124. Port 251 is “*reconfigur[ed]*” by Access



460 Pet., 42-45; 484 (1st) Pet., 46-48; 484 (2nd) Pet., 51; 450
Pet., 49-50; 444 Pet., 62-63; Ex.1005, [0064], [0107], Fig.2
(annotated).

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 **37**

Krantz Teaches “reconfiguring” (Mapping #2)

[460 Patent] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper . . .

Krantz

[0107] When client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.

460 Patent

Logic 317 For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. In response, Access Control 320 sends appropriate commands to Switch Logic 317. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310. In alternative

Ex.1005, [0107]; 460 Patent, 9:47-52; 460 Pet., 42-44; 484 (1st) Pet., 42, 44-45; 484 (2nd) Pet., 51-52; 450 Pet., 49-50; 444 Pet., 63.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 **38**

Krantz Teaches “reconfiguring” (Mapping #2)

[460 Patent] reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper . . .

Dr. Houh

Evidence

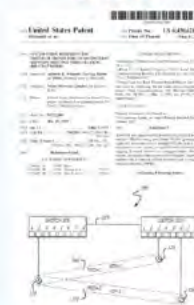
124. Krantz is therefore explaining that when configured as a “VLAN aware device,” Krantz’s “access point” is “reconfiguring the communication port [i.e., Port 251 of Krantz] for communicating data between the access device and the less-restricted subset of the protected network ” because Access Point 209 (via Port 251) will insert VLAN Tag Headers into incoming data frames from a client that may now access VLAN C, i.e., the “less-restricted subset.” Ex.1005, [0107]. Port 251 is “reconfigur[ed]” by Access Point 209 because it was previously tagging incoming data from client 205, as described above, with headers that enabled access to VLAN B, i.e., the “restricted subset” only. Put another way,

As already explained above, configuring input ports in VLAN aware devices to tag incoming data was a well-known technique to POSITAs by 2003. Ex.1007 (IEEE

Ex.1007



Ex.1008



Ex.1009



Ex.1010



Ex.1003 (460 Patent), ¶¶124-125
(citing Exs. 1007, 1008, 1007, 1010).

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 39

Krantz Teaches “reconfiguring” (Mapping #2)

[460 Patent] *reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper . . .*

POR

The Board misapprehends Patent Owner's argument. The issue is not about what component inserts Tag Headers. Rather, inserting Tag Headers into a data frame for data received from an access device is not reconfiguring of the communication ports of the access point. That Krantz's access point may insert the Tag Header does not mean the access point's ports are reconfigured. There is no evidence of any *change* to the access point, which instead, merely performs according to its initial configuration.

POR (460 Patent), 16

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 **40**

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Mapping #2

Petitioner Reply

InfoExpress is incorrect—the opposite is true. Dr. Houh submitted four contemporaneous documents that fully supported his opinion that port 251 of access point 209 of Krantz—when configured as a VLAN aware device—is reconfigured (or changed). Petition, 43-44; Ex.1003, ¶125. By contrast,

460 Reply, 2; 484 (1st) Reply, 2; 484 (2nd) Reply, 1-2; 450 Reply, 2; 444 Reply, 4.

Houh Declaration and Reply Declaration

125. In particular, Krantz discloses “[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C [the “less-restricted subset”]. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.”

14. For the reasons I discussed in my Initial Declaration, the above satisfies the “*reconfiguring the communication port*” limitation under its plain and ordinary meaning. Moreover, the above demonstrates how there is a change in the instructions provided to a communication port so that data is transferred to VLAN C instead of VLAN B. In particular, as I explained in my Initial

Ex.1003 (460 Patent), ¶125, Ex.1028, ¶14.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029

IPR2024-00539 41

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Mapping #2

Petitioner Reply

As Dr. Houh explains, this mapping satisfies the “*reconfiguring the communication port*” limitation under its plain and ordinary meaning because it demonstrates how there is a change in the instructions provided to a communication port of an access point so that data is transferred to VLAN C instead of VLAN B. In particular, Krantz discloses:

When client 205 is authorized to access resources located on VLAN C, access point 209 may enable any protocols that are currently blocked for port 251 and may insert Tag Headers” indicating that data from client 205 is to be transferred to VLAN C [the “less-restricted subset”]. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers.

Ex.1003, ¶125; Ex.1005, [0107]. Krantz is therefore explaining that Server 215 is sending commands to “change the port’s instructions.” which InfoExpress concedes discloses “reconfiguration of the ports themselves.” POR, 18; EX2565, ¶81; Ex.1028, ¶¶13-14.



POR



It was well-understood to POSITA at the time of the invention, that reconfiguration of the ports themselves could be done by changing the port’s instructions. For example, rather than being sent to a RADIUS server for user

460 Reply, 2-3; 484 (1st) Reply, 2-3; 484 (2nd) Reply, 2; 450 Reply, 2-3; 444 Reply, 4-5; POR, 18 (460 Patent).

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 42

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Mapping #2

Petitioner Reply

insert appropriate Tag Headers” Ex.1005, [0107]. Krantz thus expressly teaches “changing how the access point operate[s],” EX2565, ¶81, contrary to Dr. Cole’s opinion. Further, Dr. Cole admits that reconfiguration of a port includes providing instructions to change the operation of a communication port. Ex.1022, 34:7-20, 35:12-16; *see also* POR, 18; EX2565, ¶81 (“[R]econfiguration of the

Cole Declaration

communication ports themselves. It was well understood to POSTA at the time of the invention, that reconfiguration of the communication ports themselves could be done by changing the instructions that correspond to a particular tag header. For

Ex.2565, 181 (460 Patent)

7 Q. Paragraph 81, in the middle of the
8 sentence, you say: (Reading)
9 Reconfiguration of the
10 communication ports themselves could
11 be done by changing the instructions
12 that correspond to a particular tag
13 header.
14 Do you see that?
15 A. Yeah.
16 Q. So you can reconfigure a communication
17 port without physically altering the port itself;
18 is that right?
19 (Witness reviews document.)
20 A. That's what it says.

460 Reply, 3-4; 484 (1st) Reply, 4; 484 (2nd) Reply, 3-4; 450
Reply, 4; 444 Reply, 4; Ex.2565, ¶79-81 (460 Patent), Ex.1022,
34:7-20)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 43

Krantz Teaches “reconfiguring” (Mapping #3)

[460 Patent] *reconfiguring the communication port for communicating data between the access device and the less-restricted subset of the protected network without passing the data through the gatekeeper . . .*

Petition

Mapping #3

To the extent one may assert that Krantz does not disclose “*reconfiguring the communication port*”—Port 251 on Access Point 209—it would have been obvious to do so based on Krantz itself for the reasons already explained above. See §VIII.A.1.iv. For example, as already explained, it would have been obvious to combine the functionality of the Data Routing Device and Access Point of Krantz in the same device. Ex.1003, ¶131.

In such a combined device, as Krantz explains, “when a portion of data, such as, for example, a data frame, is transferred in at a first port . . . based on configuration rules, that the frame is to be transferred out at a second port (e.g., port 243). For example, data routing device 214 can determine that a data frame received from access point 209 is to be sent to server 215. It may also be that a data frame is transferred in and out of data routing device 214 at the same port.” Ex.1005, [0059]. The combined device would be further enabled to “reconfigure” as necessary the “*communication port*” for transfer of data from an authenticated client to VLAN C. Ex.1005, [0060] (“Data routing device 214 can

460 Pet., 46-47; 484 (1st) Pet., 50-52; 484 (2nd) Pet., 37-43, 55; 450 Pet., 52-56; 444 Pet., 66-70.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 **44**

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Mapping #3

POR

Mapping #3 is essentially a repeat of Mapping #2, except that instead of relying on access point 209 to purportedly meet the claimed access point, Petitioner argues it would have been obvious to combine access point 209 and data routing device 214. Nonetheless, the same Tag Header argument is made for this hindsight combination of devices. For the reasons discussed with Mapping #2, the insertion of tag headers is not reconfiguring of the communication ports of an access point.

Sur-Reply

Mapping #3

Petitioner next argues one could combine the functionality of the Data Routing Device 214 and the Access Point 209 from Krantz in a single device. Reply, 5-7. As discussed with Mapping #2, regardless of whether Krantz’s Data Routing Device and Access Point are combined or separate, Petitioner relied on changing the Tag Header in the client data frame, which is not “reconfiguring.”

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

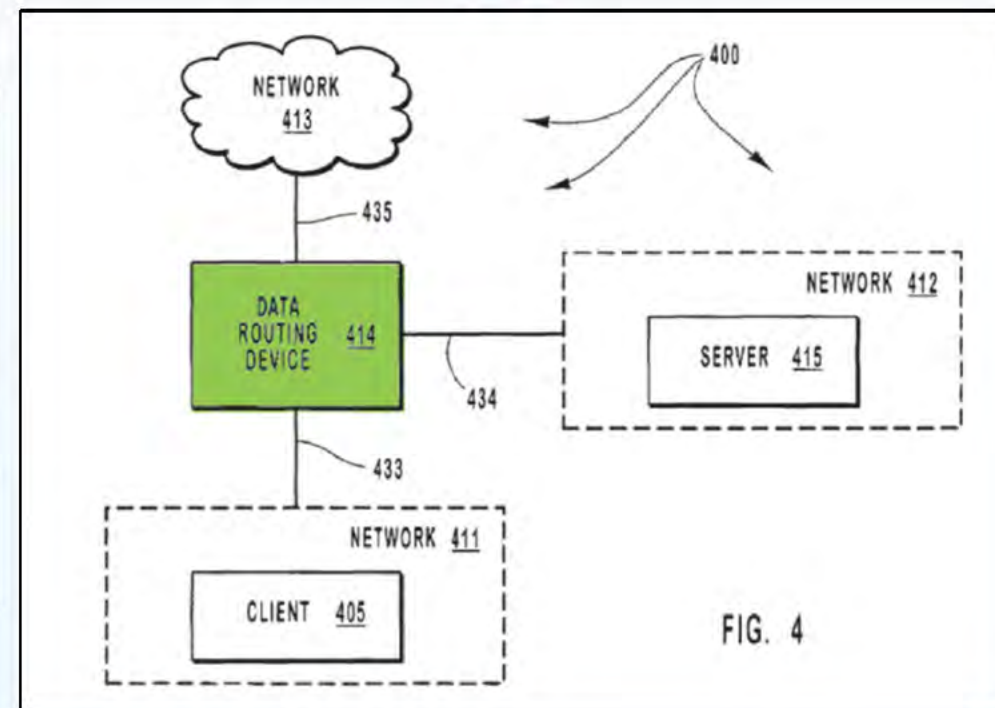
Mapping #3

Petitioner Reply

Dr. Houh explained that a POSITA would have found it obvious that the technique discussed with respect to the “data routing device 214” could simply be implemented at the access point itself as the data routing device is merely a “logical representation” of, e.g., a router and/or switch. Dr. Houh also states that the access point 209 would implement port configuration and data transfer techniques described with respect to “data routing device 214.” Petition, 33 (citing Ex.1005, [0059]; Ex.1003, ¶104). Figure 4 contemplates the combined device:

460 Reply, 5-6; 484 (1st) Reply, 5; 484 (2nd) Reply, 5; 450 Reply, 5; 444 Reply, 7.

Krantz



Ex.1005, Fig. 4 (annotated).

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”

Mapping #3

Petitioner Reply

Mapping #3

Dr. Cole provided no rebuttal testimony on Mapping #3, so Dr. Houh’s testimony is the only evidence of record. Additionally, InfoExpress’s Response simply incorporates its response to Mapping #2—it has therefore waived any argument unrelated to that response.

Dr. Houh’s testimony showed that the “reconfiguring” element would have been obvious based on the combination of the Data Routing Device and Access Point. Petition, 46 (citing §VIII.A.1.iv; Ex.1003, ¶131). Specifically, Krantz explains that the combined Data Routing Device and Access Point “can be configured to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413).” Ex.1005, [0051]. This describes the same “reconfiguring” functionality as the Challenged Patent. Ex.1001, 3:24-26.

Krantz

as, for example, data received from client 405. That is, when data routing device 414 receives data from network 411, data routing device 414 can determine if the data is to be transferred to network 412 or network 413. As such, data routing device 414 can be configured to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413). Data routing device 414 can make this determination using a variety of different techniques.

460 Reply, 5-6; 484 (1st) Reply, 5; 484 (2nd) Reply, 4-5; 450 Reply, 4-5; 444 Reply, 6-7; Ex.1005, [0051]; Ex.1003, ¶104 (460 Patent).

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- **Disputed Patentability Issues**
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz teaches a “restricted subset ... including a gatekeeper” and “a less-restricted subset of the network”

Patent	Disputed Limitation
460 Patent	[1.4] <i>the restricted subset including a gatekeeper</i> ; applying a security policy to the access device in response to the request; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and
484 Patent (1)	[1.4] <i>the restricted subset of the protected network including the gatekeeper.</i>
484 Patent (2)	[28.4] <i>the restricted subset including a gatekeeper</i> ; applying a security policy to the access device, responsive to the request;
444 Patent	[22.7] . . . receiving, from the agent, updated audit data pertaining to the device while the device has access to <i>a less-restricted subset of the network</i> ;

Krantz teaches a “restricted subset ... including a gatekeeper” and “a less-restricted subset of the network”

Patent

FIG. 2 is a block diagram of a Protected Network 200, according to various embodiments of the invention. Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210. Access to Protected Network 200 is possible through an Access Point 215 (a communication device) and an optional Router 220. As is described further herein this access is under the control of a GateKeeper 225. GateKeeper 225 is configured to enforce a security policy against one or more Access Device 230 requesting access to Less-Restricted Subset 210. Typically, Less-Restricted Subset 210 and Restricted Subset 205 are characterized by VLAN settings within Access Point 215. Access Device 230 and Access Point 215 are connected

Cole Dep. Tr.

Q. Okay. So I guess I'll ask my question again. Do you agree that in the context of the challenged patents, that a protected network may either be physically or logically divided into a restricted subset and less-restricted subset?

A. That's exactly what the patent says, so I would agree with that.

Ex.1022, 11:4-10;

460 Patent, 6:55-67; 460 Pet., 36-37; 484 (1st) Pet., 55-56; 484 (2nd) Pet., 43-44.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 50

Krantz teaches a “restricted subset ... including a gatekeeper” and “a less-restricted subset of the network”

[0017] A determination of whether data from the client is to be transferred to the first network or the second network can be implemented using any number of techniques, such as, for example, Virtual Local Area Networks (“VLANs”), Internet Protocol (“IP”) filtering, Virtual Private Networks (“VPNs”), or use of IP Security (“IPSec”) protocols. In some

[0031] The principles of the present invention provide for increasing the level of automation when provisioning and configuring a computer system to access a network. A client attempts to become authorized to access resources located on a second network (e.g., the Internet). The client sends credentials to an access point that is communicatively coupled to a server (located on a first network or located on the second network) that can authorize access to the second network. The server receives the client credentials and determines if the client credentials authorize access to the second network.

Krantz (annotated)

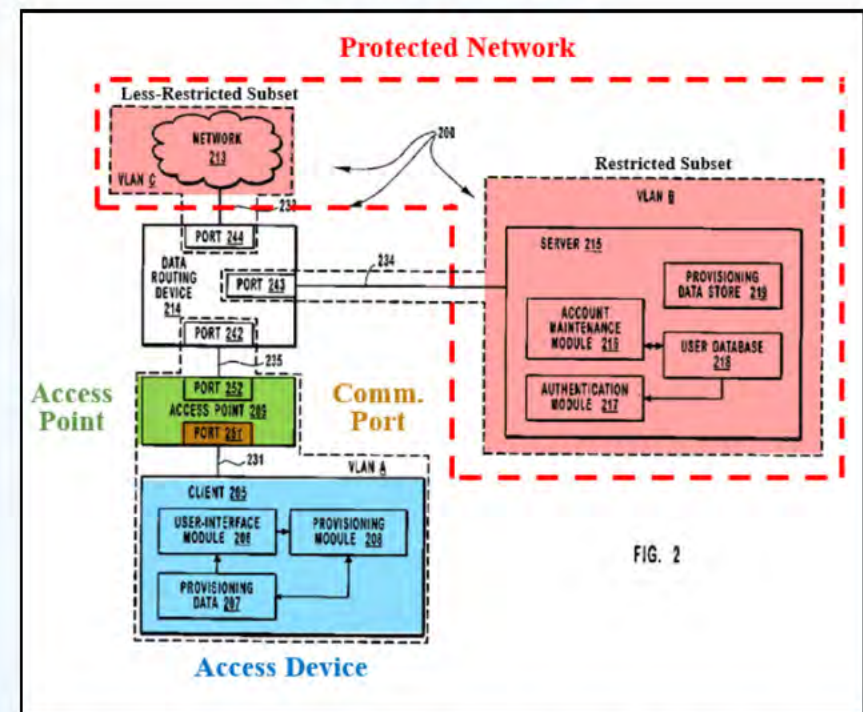


FIG. 2

460 Pet., 13-18, 38-39; 484 (1st) Pet., 19-25, 41; 484 (2nd) Pet., 20-26, 44; 444 Pet., 20-24; Ex.1005, Fig. 2, [0017], [0031]

Ex. 1029
IPR2024-00539 51

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- **Disputed Patentability Issues**
 - Krantz teaches “[configuring / reconfiguring] the [communication port] / [access device]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - **Krantz teaches “applying a security policy” and related elements**
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz teaches “applying a security policy . . .” and related elements

Patent	Disputed Limitation
460 Patent	[1.4] the restricted subset including a gatekeeper; <i>applying a security policy to the access device in response to the request</i> ; using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and
484 Patent (1)	[1.2] <i>a policy auditor configured to audit the access</i> device using the at least one security policy,
484 Patent (2)	[28.4] the restricted subset including a gatekeeper; <i>applying a security policy to the access device, responsive to the request</i> ;
450 Patent	[16.2] / [22.2] . . . <i>applying a security policy to the access device</i> in response to the request, application of the security policy including <i>performing an audit of the access device</i>; [10] The method claim 1, wherein one of the requirements pertains to a status of an operating system exon [sic] the device. [25] The method of claim 22, wherein performing the audit includes receiving operating system information from the access device.

Krantz teaches “applying a security policy . . .” and related elements

Patent	Disputed Limitation
444 Patent	[1.4] <i>applying a security policy</i> that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper [5] The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device after configuring the access point. [6] The method of claim 2, further comprising receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network. [7] The method of claim 2, further comprising continuing to receive at the gatekeeper, from the agent, audit data pertaining to the device after the configuring of the access point. [12] The method of claim 1, wherein the received audit data includes information that concerns operating system of the device. [22.7] . . . receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network; [22.8] . . . re-auditing the device in accordance to the security policy using the received updated audit data.

Krantz teaches “applying a security policy . . .” and related elements

Petition

Furthermore, with respect to the Gatekeeper (depicted above), Krantz discloses “*applying a security policy*.” As an initial matter, the 460 Patent explains that “the security policies may include requirements for user identification⁵ such as usernames and passwords, configuration requirements relating to the configuration of Access Device 230 application requirements relating to applications running on Access Device 230, or the like.” Ex.1001, 6:40-45. Ex.1003, ¶113.

Krantz discloses several specific examples of “*applying a security policy to the access device in response to the request*.” For instance, Krantz explains that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of authentication,” which can include an indication for EAP, which is short for “Extensible Authentication Protocol.” Ex.1005, [0066]-[0067]. Ex.1003, ¶114.

Krantz

wireless network from another. Through the use of beacon and probe frames client 205 can also detect other configuration settings of an access point, such as, for example, data transfer rates, supported types of authentication (e.g., open or shared authentication), supported types of encryption (e.g., Wire Equivalent Protection (“WEP”) or Temporal Key Integrity Protocol (“TKIP”)), etc.

[0067] It should be understood that the listed configuration settings are merely examples of some of the possible configuration settings and that a large number of other configuration settings, in addition to these example configuration settings, can be determined. For example, when establishing

460 Pet., 37-38; 484 (1st) Pet., 32-33; 484 (2nd) Pet., 45; 450 Pet. 80-83; 444 Pet., 36-38; Ex.1005, [0066]-[0067]

Krantz teaches “applying a security policy . . .” and related elements

Petition

Krantz further explains that “[a]fter an EAP type is selected . . . computer systems can attempt to authenticate with one another through the transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, client 205 may communicate with server 215 through a series of EAP messages in accordance with EAP-TLS so as to be authenticated and possibly authorized to access resources located on VLAN C.” Ex.1005, [0068]. The use of EAP-TLS (*e.g.*, Ex.1005, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1016

Krantz similarly discloses that “[w]hen EAP-MSChap V2 is indicated, the “MS Chap V2 Parameters element at line 67 can be included in a configuration sub-file to indicate whether or not operating system credentials should be used for authentication.” Ex.1005, [0099]. Ex.1003, ¶115.

Krantz

selected EAP type. For example, when EAP-TLS is selected, client 205 may communicate with server 215 through a series of EAP messages in accordance with EAP-TLS so as to be authenticated and possibly authorized to access resources located on VLAN C.

Ex.1005, [0068]

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

Ex.1005, [0099]; 460 Pet., 37-39; 484 (1st) Pet., 32-33; 484 (2nd) Pet., 45; 450 Pet. 80-83; 444 Pet., 36-38.

Krantz teaches “applying a security policy . . .” and related elements

Houh Declaration

to access resources located on VLAN C.” Ex.1005, [0068]. The use of EAP-TLS (e.g., Ex.1005, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices. Ex.1016 [RFC2716] at 1; see

...

116. Krantz also explains that both EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization. Ex.1005, [0099]

(“[B]oth of the elements . . . can be included in a configuration sub-file to indicate different EAP types, such as, for example, EAP-TLS and EAP

Microsoft/Challenge/Replay Handshake Protocol Version (“EAP-MSChapV2”).

Accordingly, a POSITA would understand that each of the above techniques in Krantz would be used to authenticate the client 205 (“applying a security policy to the access device in response to the request.”) before authorization is granted.

E.g., Ex.1017, at 2 (“EAP-TLS. TLS (SSL) is the encryption method used to

Ex.1016

The Extensible Authentication Protocol (EAP), described in [5], provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. To date, however, EAP methods such as [6] have focussed on authenticating a client to a server.

Ex.1017

EAP-TLS. TLS (SSL) is the encryption method used to protect the EAP exchange. In Windows, TLS uses certificates for machine logon and for user logon. The computer first authenticates to the network using a machine certificate; this allows for computer policies in Active Directory and SMS packages to be applied before a user logs on. When a user then does log on, he/she authenticates with a user certificate whose subject alternate name contains the user’s Active Directory UPN. At this point, the wireless connection is completely authenticated, and user policies are applied. A public key infrastructure is required for EAP-TLS.

...

exchange mechanism can be used. In Windows, PEAP supports MS-CHAPv2 in addition to TLS. **PEAP-MSCHAPv2** uses machine and user credentials for authentication. MSCHAPv2 uses rotating keys to encrypt both machine and user password hashes. Certificates are still required for the authentication server (IAS) and are used for server-to-client authentication; credentials, carried inside MSCHAPv2, are used for client-to-server authentication. Machine and user certificates are no longer necessary.

Ex.1003, ¶ 114-116 (460 Patent); Ex.1016, 1; Ex.1017, 1

Krantz teaches “applying a security policy . . .” and related elements

POR

data”. Krantz only discloses user authentication, and fails to disclose anything about “applying a security policy to an *access device*” or “system data.” In the Institution Decision, the Board did not disagree with Patent Owner that Krantz lacked this limitation. ID at 19. In fact, this Board provided helpful context in other related institution denials demonstrating the differences when authentication and auditing a security policy on the access device:

• • •

This is not surprising given the clear distinction between user authentication and security compliance of a device as recited in the claims, the specification, and the art. EX2565, ¶95 (citing EX1001, 1:33-39, 11:49-53), ¶99.

Krantz teaches “applying a security policy . . .” and related elements

- The patents describe user authentication and configuration settings as part of a security policy audit

Cole Dep. Tr.

12 Q. Okay. So it's part -- so just to
13 clarify. In the context of the challenged patents,
14 a security policy may include requirements for
15 username and passwords?

16 A. Yes.

5 Q. Okay. And so would you agree that in
6 the context of the challenged patents, that user
7 authentication may be considered part of a security
8 policy audit?

9 A. Yes, I would.

Ex.1022, 8:12-16, 8:20-9:11,10:5-9, 8:20-9:11 (460 Reply, 10-11; 484 (1st) Reply, 10; 484 (2nd) Reply, 10-11; 450 Reply, 10-11.

20 Do you also agree that in the context
21 of the challenged patents, that a security policy
22 may include requirements -- may include
23 configuration requirements related to the
24 configuration of an access device?

25 And I can direct you to line 42 and 43,
1 if that's helpful.

2 A. I was just going there.

3 So: (Reading)

4 The security policies may
5 include requirements for user
6 identification such as username and
7 passwords, configuration requirements
8 relating to the configuration of an
9 access device.

10 So I would agree that it may include
11 configuration requirements.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- **Disputed Patentability Issues**
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - **Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”**
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz in view of Herrmann teaches “. . . monitor[ing] the security status of the access device. . . ”

Patent	Disputed Limitation
460 Patent	[22] . . . wherein the program is further executable to communicate between the gatekeeper and an agent executing on the access device to monitor security status of the access device after reconfiguring the communication port for communicating between the access device and the less-restricted subset.
484 Patent (2)	[28.6] 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 for communicating between the access device and the less-restricted subset.

Krantz in view of Herrmann teaches “. . . monitor[ing] the security status of the access device. . . ”

460 Patent Claim 22

Petition

Herrmann discloses continuous monitoring by an “agent executing on the access device,” including “after reconfigur[ation].” Herrmann explains that “[a]lternatively, if the NAS supports the ability to remove the restrictive filter, then the IGW server can direct the NAS to remove the restrictive filter once the client has established compliance with the required policy. When the client has taken the necessary steps to comply with the policy, the policy server is notified by the client (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status message sent from the client directly to the policy server).” If the policy server verifies that the client is indeed in compliance with the assigned policy, it sends an ‘ISS_AUTH_OK’ message to the IGW server to indicate that the session should be unrestricted. In response to receiving the ‘ISS_AUTH_OK’ message from the policy server, the IGW server directs the NAS to remove the restrictive filter.” Ex.1006, [0080]. Ex.1003, ¶202.

Because of known risks in a networked environment, a POSITA would have looked to some of the well-known security techniques disclosed in Herrmann such as an “agent [that] monitors and controls the interaction of the local machine with other machines and devices that are connected on a LAN or a larger wide area network (WAN), such as the Internet, in order to provide security to the machine.” Ex.1006, [0028]. Because any single connected device on, e.g., a corporate LAN, may jeopardize all local connected devices (including the access device), a POSITA would recognize that the policy server 460 would need to be aware of all devices connected to the access device on the LAN to ensure they each have up to date antivirus software. Ex.1006, [0057], [0067]. Ex.1003, ¶203.

460 Pet., 79-80; 484 (2nd) Pet., 60-61

Krantz in view of Herrmann teaches “. . . monitor[ing] the security status of the access device. . . ”

460 Patent Claim 22

Herrmann

[0080] Alternatively, if the NAS supports the ability to remove the restrictive filter, then the IGW server can direct the NAS to remove the restrictive filter once the client has established compliance with the required policy. When the client has taken the necessary steps to comply with the policy, the policy server is notified by the client (e.g., through an “IA_HEARTBEAT” message, which is a periodic status message sent from the client directly to the policy server). If the policy server verifies that the client is indeed in compliance with the assigned policy, it sends an “ISS_AUTH_OK” message to the IGW server to indicate that the session should be unrestricted. In response to receiving the “ISS_AUTH_OK” message from the policy server, the IGW server directs the NAS to remove the restrictive filter. The

Ex.1006, [0080]; Ex.1003, ¶1202 (460 Patent)

Houh Declaration

202. Similarly, Herrmann discloses continuous monitoring, including after reconfiguration. Herrmann explains that “Alternatively, if the NAS supports the ability to remove the restrictive filter, then the IGW server can direct the NAS to remove the restrictive filter once the client has established compliance with the required policy. When the client has taken the necessary steps to comply with the policy, the policy server is notified by the client (e.g., through an ‘IA_HEARTBEAT’ message, which is a periodic status message sent from the client directly to the policy server). If the policy server verifies that the client is

. . .

Similarly to Krantz, because Herrmann discloses that the security status is continually monitored through an IA_HEARTBEAT, as just discussed, a POSITA would understand that this includes monitoring the security status after reconfiguring the communication port for communicating between the access device and the less-restricted subset.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029
IPR2024-00539 63

Krantz in view of Herrmann teaches “. . . monitor[ing] the security status of the access device. . . ”

460 Patent Claim 22

POR

As backup, the Petition argues Herrmann’s “IA_HEARTBEAT” constitutes an “agent executing on the access device” including “after reconfigur[ation].” Pet. at 79. The Petition stops short of asserting the “heartbeat” is something that would “monitor security status.” The reason, as Herrmann explains, is because a heartbeat is nothing more than a “status message.” EX1006, [0080]. Such a message does not contain substantive policy data about a “security status.” Rather, it only carries minimal information to confirm if an access point is connected and active (i.e., proof of life). EX2565, ¶¶161-63. By contrast, the claimed “security status” relates to whether the device configuration is still compliant with the security policy. CITE. A heartbeat message confers no such information. Moreover, the claim requires that the communication is between the gatekeeper and the agent. In contrast, Herrmann’s heartbeat “status message” is “sent from the client directly to the policy server.”

Petitioner Reply

Claim 22: InfoExpress asserts that neither Krantz nor Herrmann disclose claim 22’s requirement of “*monitor[ing] the security status of the access device,*” but its arguments fail to appreciate that the combination of the art discloses the limitation—InfoExpress instead attacks each individually, which is an improper approach as a matter of law. *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). Moreover, Krantz does “*apply a security policy,*” so requesting “re-authenticat[ion]” (which would include the device) is entirely relevant.

POR, 36-37; 460 Reply, 14-15; 484 (2nd) Reply, 12-13

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- **Disputed Patentability Issues**
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- Secondary Considerations
- Conception & Diligent Reduction to Practice

Krantz teaches “updat[ing] the access device . . .”

Patent	Disputed Limitation
460 Patent	[27] The non-transitory computer readable storage medium of claim 16, wherein the program is further executable to update the access device when requirements of the security policy are not satisfied.
484 Patent (1)	[3] The network gatekeeper of claim 1, wherein the network gatekeeper is further configured to update the access device using an update module. [24] The network gatekeeper of claim 1, wherein the network gatekeeper is configured to update the access device if requirements of the security policy are not satisfied.
484 Patent (2)	[38] The method of claim 28, further including updating the access device if requirements of the security policy are not satisfied. [41.6] . . . updating the access device if requirements of the security policy are not satisfied. [42] The method of claim 41, wherein the security policy includes an audit of the access device. [43] The method of claim 41, further including communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine if the access device satisfies the requirements of the security policy. [53] The method of claim 41, further including authenticating a user of the access device.

Krantz teaches “updat[ing] the access device . . .”

Patent	Disputed Limitation (cont.)
450 Patent	[2] The method claim 1, further comprising facilitating updates to software on the device in response to applying the security policy, using the gatekeeper. [16.3] / [22.3] . . . providing information to the access device to improve compliance of the access device to the security policy, in response to the audit; [23] The method of claim 22, wherein performing the audit includes using an agent on the access device to collect information regarding the access device. [25] The method of claim 22, wherein performing the audit includes receiving operating system information from the access device. [27] The method of claim 22, wherein the information includes a software update of software on the access device.
444 Patent	[17] The method of claim 1, wherein the gatekeeper is configured to take part in bringing a software on the device up to date in response to applying the security policy.

Krantz teaches “updat[ing] the access device . . .”

460 Patent, Claim 27

Petition

Krantz explains that “[w]hen full access to resources located on the second network is not authorized, the server can authorize limited access to the first network or second network such that the client can download provisioning files for gaining full access [to] resources located on the second network.” Ex.1005, [0032]; see also Ex.1005, [0056]; Ex.1005, [0110] (“[T]he method 300 also . . . sub-file, from provisioning data 207.”). For example, Krantz explains that “[i]f credentials do not authorize full access to the second network (e.g., credentials cannot be authenticated, credentials are guest credentials, or an authenticated user is not authorized)” the server can notify the client and send a “configuration sub-file” that “can be executed to configure connection type, communication protocols, authentication type, encryption type, etc.” Ex.1005, [0019]-[0020], [0024].

POR

Notwithstanding, Petitioner’s “provisioning files” argument is equally wrong. The Petition cites Krantz’s disclosure of “provisioning files [] for gaining full access [to] resources located on the second network.” Id. But “provisioning files” are not related to “requirements of the security policy.” Provisioning files merely give devices software necessary to connect to and operate on a network. EX1005, [0013]-[0014]. These files ensure that the device can access network services without requiring manual configuration by the end-user. EX2565, ¶¶166-69; EX1005, [0112] (“[d]uring the registration process with the ISP, the computer system may download provisioning files for the wireless hotspot.”). As discussed above, Krantz

460 Pet., 56-57; 484 (1st) Pet., 59-60; 484 (2nd) Pet., 62-65; 450 Pet., 87-88; 444 Pet., 84-86; POR, 38 (460 Patent)

Krantz teaches “updat[ing] the access device . . .”

460 Patent, Claim 27

Krantz

access to network 413. Client 405 can be authorized to download provisioning files from these computer systems or modules, while being denied access to other resources located on network 413.

. . .

[0110] In parallel with acts 302 through 305, the method 300 also includes an act of executing a schema-based document (act 306). This can include executing a third schema-based document to configure a client for accessing the second network. For example, provisioning module 208 can execute an XML document, defined in accordance with an XML configuration schema, to appropriately configure client 205 for accessing resources located on VLAN C. Provisioning module 208 can retrieve previously downloaded XML documents, such as, for example, a configuration sub-file, from provisioning data 207.

Houh Declaration

206. For example, Krantz explains that “[w]hen full access to resources located on the second network is not authorized, the server can authorize limited access to the first network or second network such that the client can download provisioning files for gaining full access resources located on the second network. Ex.1005, [0032]; see also Ex.1005, [0056] (“Client 405 can be authorized to download provisioning files from these computer systems or modules, while being denied access to other resources located on network 413.”); Ex.1005, [0110] (“In

Ex.1005, [0056], [0110]; Ex.1003, ¶206 (460 Patent)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ex. 1029

IPR2024-00539

69

Roadmap

- Challenged Patents Overview
- Prior Art Overview
- Motivation to Combine
- Disputed Patentability Issues
 - Krantz teaches “[configuring / reconfiguring] the [communication / access] [port / device / point]”
 - Krantz teaches a “restricted subset of ... including a gatekeeper” and “a less-restricted subset of the network”
 - Krantz teaches “applying a security policy” and related elements
 - Krantz in view of Herrmann teaches “monitor[ing] the security status of the access device”
 - Krantz teaches “updat[ing] the access device . . .” and related elements
- **Secondary Considerations**
- Conception & Diligent Reduction to Practice

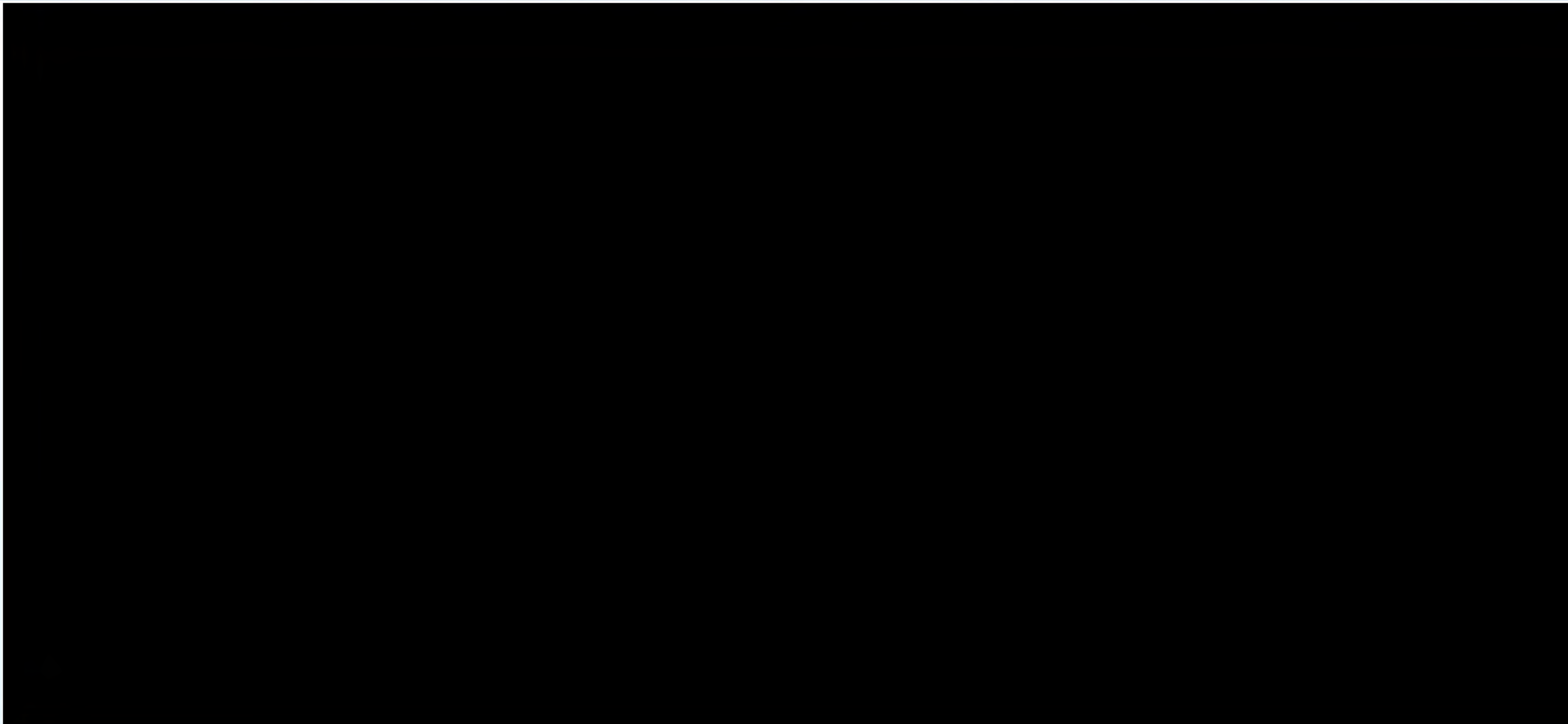
Secondary Considerations

Secondary Considerations

Secondary Considerations

Secondary Considerations

Roadmap



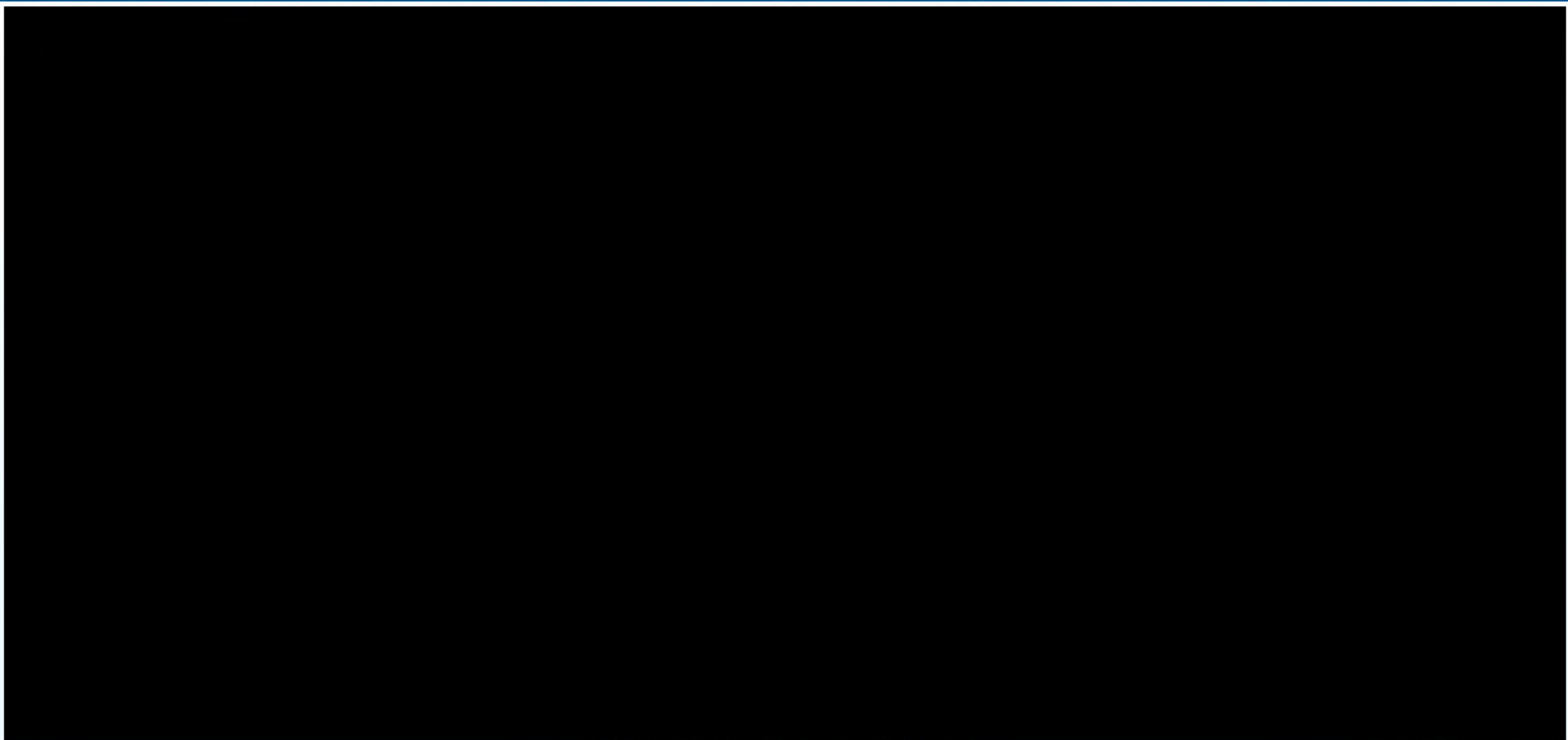
Conception

Conception

Conception

Conception

Conception



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 80

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **81**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **82**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **83**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **84**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **85**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **86**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **87**

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 **88**

Diligence

Diligence

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

IPR2024-00539 90