

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioners,

v.

INFOEXPRESS INC.,
Patent Owner.

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

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. Introduction.....	1
II. The '350 Patent	1
A. Date of Invention.....	1
B. Person of Ordinary Skill in the Art (POSITA)	1
C. Overview of the '350 Patent	2
III. Claim Construction.....	7
A. Reconfiguring an Access Point	7
B. "Audit Data Pertaining to a Device" and "Auditing the Device in Accordance With a Security Policy"	9
IV. Petitioners' Cited References	12
A. Krantz	12
B. Herrmann.....	15
V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims	16
A. Ground 1: Krantz Alone Is Missing Specifically Claimed Limitations.....	17
1. Krantz Fails To Disclose "Reconfiguring An Access Point To Allow Access To The Less Restricted Subset Of The Network In Response To The Security Policy Audit"	17
2. Device Auditing Is Absent From Krantz	23
a) Krantz Fails To Disclose "audit data pertaining to a device"	24
b) Krantz Fails To Disclose "Auditing The Device In Accordance With A Security Policy"	27
c) Krantz Fails To Disclose "Receiving Updated Audit Data Pertaining to the Device Subsequent to Reconfiguring The Access Point"	30

d)	Krantz Fails To Disclose "Monitoring Continued Compliance Of The Device Using The Updated Audit Data"	31
B.	Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious Claims 6-10, 13, 18 or 19.....	31
VI.	All Grounds: Neither Reference Constitutes Prior Art	33
A.	Legal Standards	34
B.	The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....	36
C.	The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.	37
D.	The Filing of U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003 Constitutes Constructive Reduction to Practice.....	45
VII.	Conclusion	45

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed.Cir.2005)	10
---	----

FEDERAL STATUTES

35 U.S.C. § 103	1
-----------------------	---

EXHIBIT LIST

Exhibit Number	Description
2001	Declaration of Dr. Eric Cole
2002	Curriculum Vitae of Dr. Eric Cole
2003	Declaration of Stacey C. Lum
2004	Intentionally Left Blank
2005	U.S. Provisional App. No. 60/505,582
2006	U.S. Provisional App. No. 60/513,080
2007	Declaration of Hugh Smith, Ph.D.
2008	Curriculum Vitae of Hugh Smith, Ph.D.
2009	Conception of the '350 Patent
2010	Constructive Reduction to Practice of the '350 Patent
2011	LAN Based Policy Enforcement Engineering Specification
2012	Metadata for Exhibit 2011
2013	CyberGatekeeper Policy Manager
2014	Metadata for Exhibit 2013
2015	Internal InfoExpress Correspondence
2016	Internal InfoExpress Correspondence
2017	Internal InfoExpress Correspondence
2018	Internal InfoExpress Correspondence
2019	Internal InfoExpress Correspondence
2020	Internal InfoExpress Correspondence
2021	Internal InfoExpress Correspondence
2022	Correspondence with Globe Tech
2023	Email attachment to Exhibit 2022
2024	Internal InfoExpress Correspondence
2025	Correspondence with Meetinghouse
2026	Draft Meetinghouse Agreement
2027	Internal InfoExpress Correspondence
2028	Draft Meetinghouse Agreement
2029	Internal InfoExpress Correspondence
2030	Draft Meetinghouse Agreement
2031	Draft Meetinghouse Agreement
2032	Internal InfoExpress Correspondence
2033	Draft Meetinghouse Agreement
2034	Draft Meetinghouse Agreement

Exhibit Number	Description
2035	Draft Meetinghouse Agreement
2036	Internal InfoExpress Correspondence
2037	Draft Meetinghouse Agreement
2038	Draft Meetinghouse Agreement
2039	Internal InfoExpress Correspondence
2040	Draft Meetinghouse Agreement
2041	Draft Meetinghouse Agreement
2042	Draft Meetinghouse Agreement
2043	Draft Meetinghouse Agreement
2044	Internal InfoExpress Correspondence
2045	Draft Meetinghouse Agreement
2046	Draft Meetinghouse Agreement
2047	Internal InfoExpress Correspondence
2048	Correspondence with Globe Tech
2049	Correspondence with Globe Tech
2050	Internal InfoExpress Correspondence
2051	Correspondence with Globe Tech
2052	Correspondence with Globe Tech
2053	Correspondence with Globe Tech
2054	Correspondence with Globe Tech
2055	Correspondence with Globe Tech
2056	Draft Globe Tech Agreement
2057	Draft Globe Tech Agreement
2058	Draft Globe Tech Agreement
2059	Draft Globe Tech Agreement
2060	Draft Globe Tech Agreement
2061	Draft Globe Tech Agreement
2062	Draft Globe Tech Agreement
2063	Correspondence with Globe Tech
2064	Draft Globe Tech Agreement
2065	Correspondence with Globe Tech
2066	Network Device Configuration API Engineering Specification
2067	Correspondence with Globe Tech
2068	Correspondence with Globe Tech
2069	Network Device Configuration API Engineering Specification
2070	Network Device Configuration API Engineering Specification
2071	Correspondence with Globe Tech

Exhibit Number	Description
2072	Network Device Configuration API Engineering Specification
2073	Network Device Configuration API Engineering Specification
2074	Correspondence with Globe Tech
2075	Correspondence with Globe Tech
2076	Correspondence with Globe Tech
2077	Correspondence with Globe Tech
2078	Correspondence with Globe Tech
2079	Email attachment to Exhibit 2078
2080	Correspondence with Globe Tech
2081	Correspondence with Globe Tech
2082	Correspondence with Globe Tech
2083	Correspondence with Globe Tech
2084	Correspondence with Globe Tech
2085	Correspondence with Globe Tech
2086	Correspondence with Globe Tech
2087	Correspondence with Globe Tech
2088	Correspondence with Globe Tech
2089	Correspondence with Globe Tech
2090	Correspondence with Globe Tech
2091	Correspondence with Globe Tech
2092	Correspondence with Globe Tech
2093	Correspondence with Globe Tech
2094	Correspondence with Globe Tech
2095	Correspondence with Globe Tech
2096	Correspondence with Globe Tech
2097	Correspondence with Globe Tech
2098	Correspondence with Globe Tech
2099	Correspondence with Globe Tech
2100	Correspondence with Globe Tech
2101	Correspondence with Globe Tech
2102	Correspondence with Globe Tech
2103	Correspondence with Globe Tech
2104	Correspondence with Globe Tech
2105	Correspondence with Globe Tech
2106	Correspondence with Globe Tech
2107	Correspondence with Globe Tech
2108	Internal InfoExpress Correspondence

Exhibit Number	Description
2109	Correspondence with Globe Tech
2110	Correspondence with Globe Tech
2111	Correspondence with Globe Tech
2112	Correspondence with Globe Tech
2113	Internal InfoExpress Correspondence
2114	Correspondence with Globe Tech
2115	Email attachment to Exhibit 2114
2116	Correspondence with Globe Tech
2117	Internal InfoExpress Correspondence
2118	Correspondence with Globe Tech
2119	Correspondence with Globe Tech
2120	Correspondence with Globe Tech
2121	Correspondence with Globe Tech
2122	Correspondence with Globe Tech
2123	Correspondence with J. Ong
2124	Correspondence with Globe Tech
2125	Correspondence with Globe Tech
2126	Correspondence with Globe Tech
2127	Correspondence with Globe Tech
2128	Correspondence with Globe Tech
2129	Correspondence with Globe Tech
2130	Correspondence with Globe Tech
2131	Correspondence with Globe Tech
2132	Correspondence with Globe Tech
2133	Correspondence with Globe Tech
2134	Correspondence with Globe Tech
2135	Correspondence with Globe Tech
2136	Correspondence with Globe Tech
2137	Correspondence with Globe Tech
2138	Correspondence with Globe Tech
2139	Correspondence with Globe Tech
2140	Correspondence with Globe Tech
2141	Correspondence with Globe Tech
2142	Correspondence with Globe Tech
2143	Correspondence with Globe Tech
2144	Correspondence with Globe Tech
2145	Correspondence with Globe Tech

Exhibit Number	Description
2146	Correspondence with Globe Tech
2147	Correspondence with Globe Tech
2148	Correspondence with J. Ong
2149	Correspondence with Globe Tech
2150	Correspondence with J. Ong
2151	Correspondence with Globe Tech
2152	Correspondence with J. Ong
2153	Correspondence with Globe Tech
2154	Correspondence with Globe Tech
2155	Correspondence with Globe Tech
2156	Correspondence with Globe Tech
2157	Correspondence with Globe Tech
2158	Correspondence with Globe Tech
2159	Correspondence with Globe Tech
2160	Correspondence with Globe Tech
2161	Correspondence with J. Ong
2162	Correspondence with Globe Tech
2163	Correspondence with C. Tsai
2164	Correspondence with Globe Tech
2165	Correspondence with Globe Tech
2166	Correspondence with Globe Tech
2167	Correspondence with Globe Tech
2168	Correspondence with Globe Tech
2169	Correspondence with Globe Tech
2170	Correspondence with Globe Tech
2171	Correspondence with Globe Tech
2172	Correspondence with Globe Tech
2173	Correspondence with Globe Tech
2174	Correspondence with Globe Tech
2175	Correspondence with Globe Tech
2176	Correspondence with Globe Tech
2177	Correspondence with Globe Tech
2178	Correspondence with Globe Tech
2179	Correspondence with Globe Tech
2180	Correspondence with Globe Tech
2181	Correspondence with Globe Tech
2182	Correspondence with Globe Tech

Exhibit Number	Description
2183	Correspondence with Globe Tech
2184	Correspondence with Globe Tech
2185	Correspondence with Globe Tech
2186	Correspondence with Globe Tech
2187	Correspondence with Globe Tech
2188	Correspondence with Globe Tech
2189	Correspondence with C. Tsai
2190	Correspondence with Globe Tech
2191	Correspondence with Globe Tech
2192	Correspondence with Globe Tech
2193	Correspondence with Globe Tech
2194	Correspondence with Globe Tech
2195	Correspondence with Globe Tech
2196	Correspondence with Globe Tech
2197	Correspondence with Globe Tech
2198	Correspondence with J. Ong
2199	Correspondence with C. Tsai
2200	Correspondence with J. Ong
2201	Cisco Switch Feature Support Matrix
2202	Correspondence with M. Banin
2203	Correspondence with A. Lee
2204	Correspondence with M. Banin
2205	Correspondence with M. Banin
2206	Correspondence with M. Banin
2207	Correspondence with M. Banin
2208	Correspondence with M. Banin
2209	Correspondence with M. Banin
2210	Correspondence with M. Banin
2211	Correspondence with patent counsel
2212	Correspondence with patent counsel
2213	Correspondence with patent counsel
2214	Correspondence with patent counsel
2215	Correspondence with patent counsel
2216	Correspondence with patent counsel
2217	Correspondence with patent counsel
2218	Correspondence with patent counsel
2219	Correspondence with patent counsel

Exhibit Number	Description
2220	Correspondence with patent counsel
2221	Correspondence with patent counsel
2222	Correspondence with patent counsel
2223	Correspondence with patent counsel
2224	Correspondence with patent counsel
2225	Correspondence with patent counsel
2226	Correspondence with patent counsel
2227	Correspondence with patent counsel
2228	Correspondence with patent counsel
2229	Correspondence with patent counsel
2230	Correspondence with patent counsel
2231	Correspondence with patent counsel
2232	Correspondence with patent counsel
2233	Correspondence with patent counsel
2234	Correspondence with patent counsel
2235	Correspondence with patent counsel
2236	Correspondence with patent counsel
2237	Correspondence with patent counsel
2238	Correspondence with patent counsel
2239	Correspondence with patent counsel
2240	Correspondence with patent counsel
2241	Correspondence with patent counsel
2242	Correspondence with patent counsel
2243	Correspondence with patent counsel
2244	Correspondence with patent counsel
2245	Correspondence with patent counsel
2246	Correspondence with patent counsel
2247	Correspondence with patent counsel
2248	Correspondence with patent counsel
2249	Correspondence with patent counsel
2250	Correspondence with patent counsel
2251	Correspondence with patent counsel
2252	Correspondence with patent counsel
2253	Correspondence with patent counsel
2254	Correspondence with patent counsel
2255	Correspondence with patent counsel
2256	Correspondence with patent counsel

Exhibit Number	Description
2257	Correspondence with patent counsel
2258	Correspondence with patent counsel
2259	Correspondence with patent counsel
2260	Correspondence between S. Lum and A. Lee
2261	Correspondence between S. Lum and A. Lee
2262	Correspondence with patent counsel
2263	Correspondence with patent counsel
2264	Correspondence with patent counsel
2265	Correspondence with patent counsel
2266	Correspondence with patent counsel
2267	Correspondence with patent counsel
2268	Correspondence with patent counsel
2269	Correspondence with patent counsel
2270	Correspondence with patent counsel
2271	Correspondence with patent counsel

I. Introduction

Patent Owner InfoExpress Inc. submits this Patent Owner Preliminary Response to the Petition for *Inter Partes* Review by Petitioners related to claims 1, 2, 4-10, 13, 16, and 18-19 (the "Challenged Claims") of U.S. Patent 8,347,350 (the '350 Patent'). Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims. Patent Owner submits that the Grounds presented and the prior art relied on by Petitioners fail to render any of the Challenged Claims unpatentable under 35 U.S.C. § 103 because the prior art fails to disclose or render obvious all of the limitations of the Challenged Claims. Moreover, the art relied on by Petitioners does not qualify as prior art.

II. The '350 Patent

A. Date of Invention

Patent Owner submits that for the reasons discussed in section VII.B below, that the date of invention for each of the Challenged Claims is no later than December 2, 2002.

B. Person of Ordinary Skill in the Art (POSITA)

A POSITA in at the time of the invention would have had a working knowledge of computer network security art. A POSITA would have had 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.

C. Overview of the '350 Patent

The '350 Patent is directed to a novel and seminal approach to a security solution for controlling access to a protected network not previously done or contemplated at the time of the invention. Before these claimed inventions, network security required multiple "gatekeepers" placed directly between clients, i.e., users, and the network. EX1101, Fig. 1, 2:43-45; EX2001, ¶¶ 44-46. Like a security guard at a front gate, each user would present credentials so the guard could determine whether he or she was authorized to pass through the gate, and the guard would also need to direct them where to go. For computer networks, preexisting solutions required the individual checking of each device attempting network access to make sure they had appropriate hardware and software, *e.g.*, virus protection and operating systems. This consumed substantial network bandwidth and computer processing resources, resulting in a bottleneck. EX1101, 2:38-45.

An example of the prior art architecture is shown in annotated FIG. 1 of the '350 Patent.

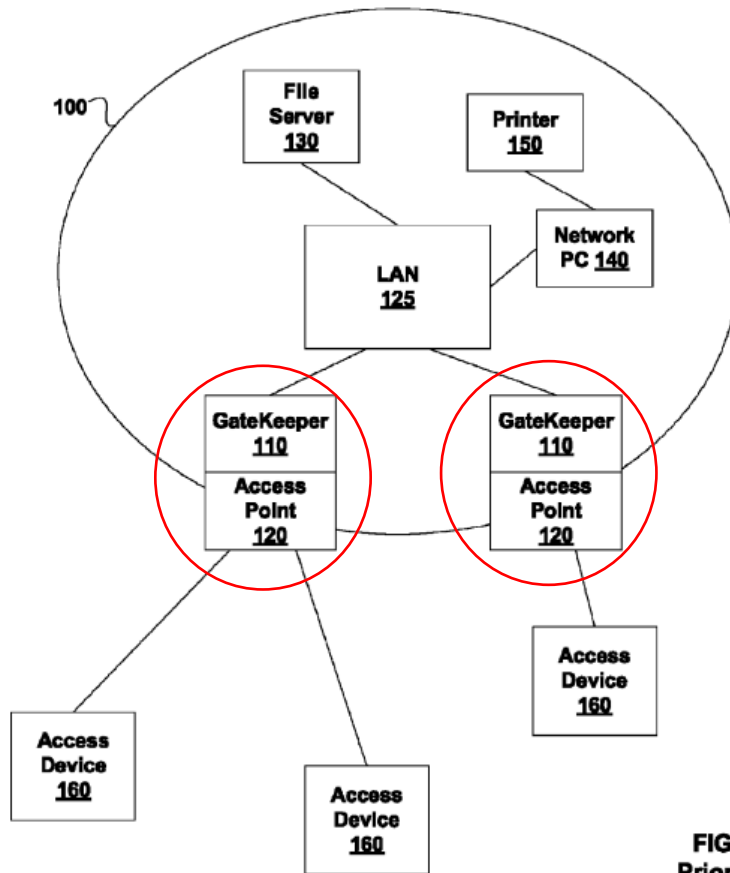


FIG. 1
Prior Art

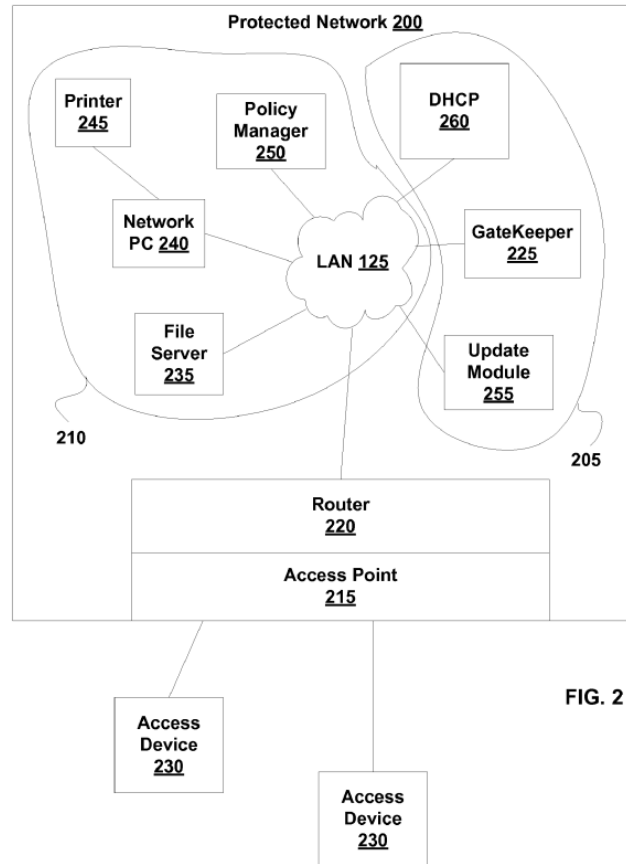
The protected network 100 included two Gatekeepers 110, each associated with a different instance of an Access Point 120. Each Access Point 120 could include numerous individual communication ports that are used to connect an access device through GateKeeper 110 to other elements within the protected network such as File Server 130. The specification explains that a "disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110." EX1101, 2:30-32. With large networks, such as corporate networks where access points may include many communication ports, 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." EX1101, 2:35-38. The gatekeeper then becomes a limiting factor or bottleneck on the bandwidth of communication between access devices and the protected network. EX1101, 2:38-41.

The '350 Patent addressed this particular problem with a new, novel, and non-obvious approach that relieves computer resources by reconfiguring an access point for previously authorized devices to access a protected network. Initial communications from the devices are passed to a restricted subset of the protected network wherein the restricted subset includes a gatekeeper. EX1101, Abstract. This gatekeeper can enforce security policy requirements pertaining to device requirements against the device's data before granting access to a less-restricted subset of the protected network.¹ If device requirements of the security policy are satisfied, the access point itself is reconfigured such that further communication from the device is enabled to access the less-restricted subset without having to go through the gatekeeper. EX2001, ¶¶ 44-46. In so doing, the number of devices and users requiring checking by the gatekeeper are greatly reduced, and the bottleneck problems are ameliorated.

¹ In some embodiments, the gatekeeper may also check user credentials to determine if the user is authorized. EX1101, 6:38-45.

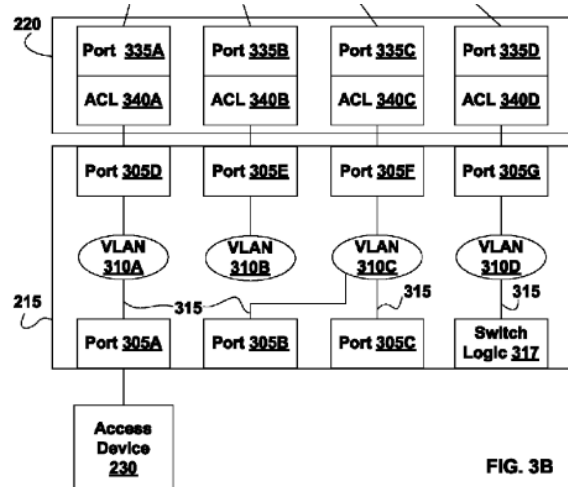
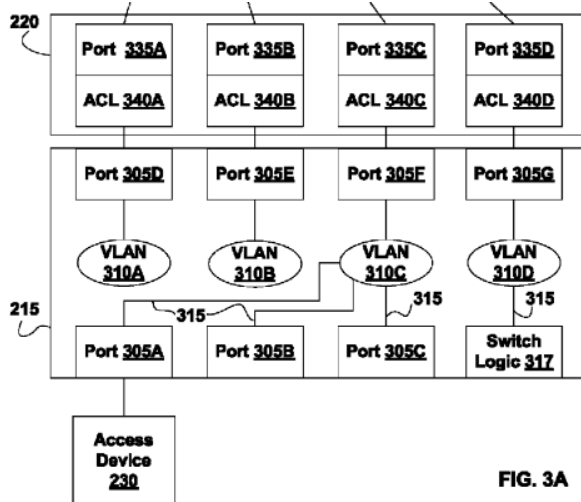
By way of example, the '350 Patent discloses a protected network that includes a restricted subset with a gatekeeper and one or more less-restricted subsets.



EX1101, Fig. 2. 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). EX1101, 2:54-56, 5:33-37. A gatekeeper in the restricted subset 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. EX1101, 2:56-60.

A key feature of the '350 Patent is that rather than requiring all device access requests to pass through the gatekeeper, the access point itself is reconfigured. In so

doing, after access is granted to a device, further communication between the access device and the protected network can include access to the less restricted subset without having to go through the gatekeeper. EX1101, Figs. 3A & 3B, 8:57–9:6. To grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected. EX1101, 3:24-29. The Detailed Description give the following example of reconfiguring the access point.



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. EX1101, 8:20-27.

In this embodiment, the assignments for the ports of the access point 215 are changed.

By reconfiguring 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. Thus, after access has been granted, most network traffic does not need to pass through the gatekeeper.

III. Claim Construction

Petitioners assert claims should be given their ordinary and customary meaning as understood by a POSITA, and contends the Board need not expressly construe the claim terms. Petition at 7. Petitioners, however, avoid providing any explanation as to what the ordinary and customary meaning for any claim term is. Indeed, Petitioners' application of the prior art references demonstrates a claim construction that specifically is neither plain nor customary, and actually contradicts the '350 intrinsic evidence.

Patent Owner contends the claims should be given their ordinary and customary meaning as understood by a POSITA in the context of the intrinsic evidence. Given Petitioners' deviation from its purported plain and ordinary meaning, Patent Owner provides the following context for certain claim terms to properly frame the appropriate ordinary and customary meaning.

A. Reconfiguring an Access Point

The Challenged Claims require "reconfiguring an access point to allow access to the less-restricted subset of the network in response to the security policy audit."

In the context of the claim language and the specification, the plain and ordinary meaning of this limitation requires that the configuration **of an access point is changed**. Not a change to the end user device (*i.e.*, "access device").

With regard to "reconfiguring," one must first look to the words of the claim. "Reconfiguring" means to rearrange something into an altered form or to configure something in a new way.² An access point is generally any computer or device through which users can gain access to a network.³ The '350 Patent gives "a network switch" as an example of an access point. EX1101, 7:57-60.

The '350 Patent specification is consistent with this plain meaning. For example, the '350 Patent specification teaches "[t]o grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected. The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1101, 3:24-29. As discussed above, the Detailed Description provides an example of reconfiguring the "access point" 215 involving reassigning ports.

² See <https://www.merriam-webster.com/dictionary/reconfigure>.

³ See, *e.g.*, <https://www.pcmag.com/encyclopedia/term/access-point>.

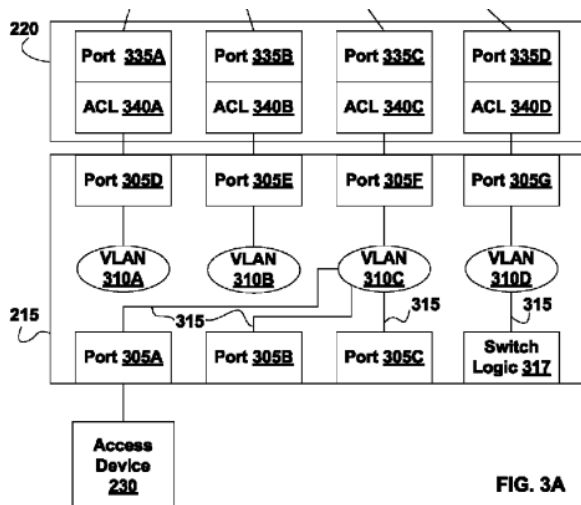


FIG. 3A

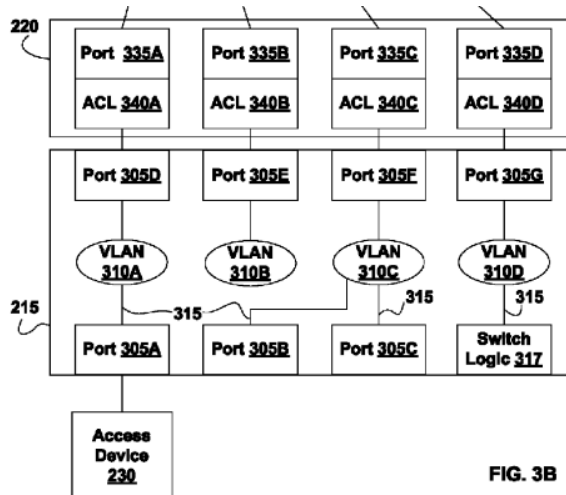


FIG. 3B

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.

Thus, the plain and ordinary meaning of reconfiguring an access point is to change the access point itself in a way that the checked device is able to access the less-restricted portion of the protected network.

B. "Audit Data Pertaining to a Device" and "Auditing the Device in Accordance With a Security Policy"

The claim terms "audit data pertaining to a device" and "auditing the device in accordance with a security policy" are specifically directed to ensuring that the **device** that is attempting to access the protected network meet certain software and/or hardware criteria as required to comply with the security policy.

The claims themselves support this plain and ordinary construction. *E.g.*, *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed.Cir.2005). Claim 1, the only independent claim, requires: "receiving *audit data pertaining to a device* that does not have access to a less-restricted subset of a network;" and "*auditing the device* in accordance with a security policy based at least in part on the audit data." EX1101, 15:56-60, 16:1-2.

Here, the claim language itself is clear. First, the claims specifically recite the "audit data" pertains to the "device" (as opposed to the user). Similarly, the claim specifies it is the "device" that is audited ("auditing the device") (not the user) in accordance with a security policy. The specification also explains "security policy" in the context of the device:

In 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. For example, GateKeeper 110 may make certain that Access Device 160 has up-to-date virus software and encryption protocols as proscribed by the security policy.

EX1101, 2:19-26. As such, the plain language of the claim requires that the "audit data" and "auditing" to be expressly about the device. Not the user.

The '350 Specification makes this express distinction between the claimed device "audit data" / "auditing" and user authentication:

In addition to authenticating users ... GateKeeper 110 is configured to ensure that Access Device 160 conforms to a predetermined security policy....

EX1101, 2:19-22. FIG. 4 shows that “authenticate user 440,” “obtain audit data 450,” and “apply security policy 460” are all separate and distinct steps.

FIG. 4 is a flowchart illustrating a method of granting access to Less-Restricted Subset 210 (FIG. 2), according to various embodiments of the invention. ... This request is received from Access Device 230 in a Receive Access Request Step 430. In response, GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively. If the security policy is satisfied, then in a Reconfigure Port Step 470, GateKeeper 225 reconfigures the communication port of Access Point 215 to which Access Device 230 has connected.

EX1101, 10:30-44.

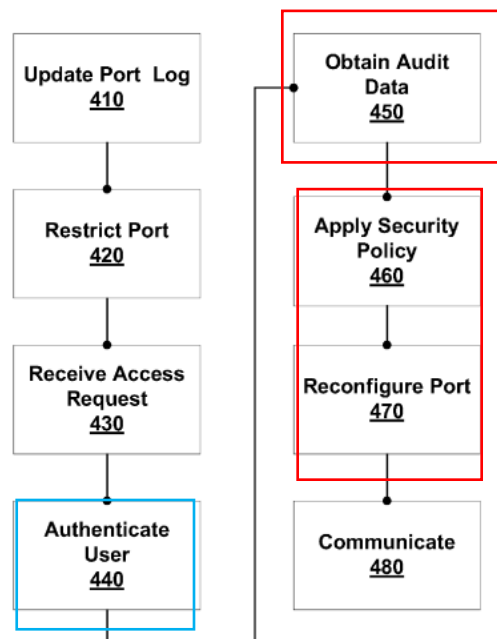


FIG. 4

Accordingly, the claim terms "audit data pertaining to a device" and "auditing the device in accordance with a security policy" should be given their plain meaning consistent with the intrinsic evidence and not conflated with a user authentication construction.

IV. Petitioners' Cited References

Petitioners' cited references, Krantz and Herrmann, are not prior art to the Challenged Claims as discussed herein. In addition, Krantz and Herrmann are readily distinguished from the Challenged Claims, and merely illustrate examples of the earlier network security approached improved upon by the '350 Patent.

A. Krantz

Petitioners' primary reference is U.S. Patent No. 2004/0111520 ("Krantz"), which was filed on December 6, 2002, and published on June 10, 2004. Krantz is described as follows:

A computer system attempts to authenticate with a server to gain authorization to access a first network. It is determined by the server that the computer system is not authorized to access the first network. The computer system is given authorization to access a second network for at least the purpose of downloading files (e.g., signup and configuration files) needed to access the first network. A user-interface for receiving user-entered signup information is automatically presented at the computer system. A first schema-based document including user-entered information is transferred to the server. If the server determines that the user-entered information is appropriate, a second-schema document, which includes an indication of authorization to access the first network (e.g., a user-identifier and password), is received. A third schema-based document is executed at

the computer system to compatible configure the computer system for accessing the first network.

EX1105, Abstract. Krantz discloses the concept wherein upon the failure of a computer system to **authenticate a user** to one network, the user is permitted to access a second network for the limited purpose of downloading files by a server.

EX2001, ¶¶ 47-49.

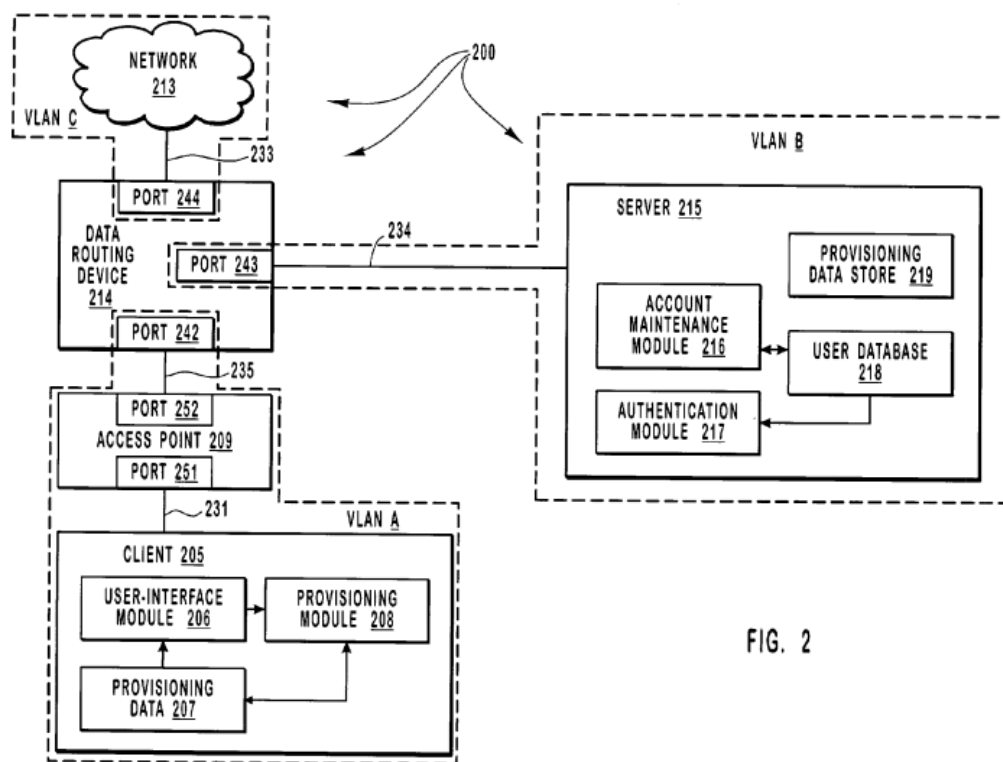


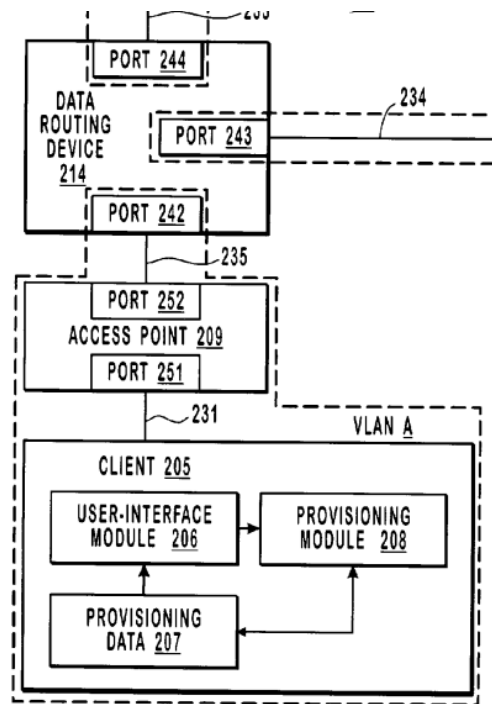
FIG. 2

Krantz discloses:

A server includes the functionality to authorize clients to access a second network (e.g., the Internet). The server can be located on a first network that is separate from the second network or can be located on the second network. A client sends credentials to the server to attempt to authenticate with the server. Based on the credentials, the server may authorize the client for at least partial access to the second network and/or may deny access to the second network and authorize the client for at least partial to access to the first network. The server can be a

Remote Authentication Dial-In User Service ("RADIUS") server that is located on the first network. Clients can be provided partial access to the first or second network at least for the purposes of authenticating with the server and downloading provisioning files used to gain full access to the second network. Thus, computer systems that are not currently able to access resources located on the second network may be able to electronically download provisioning files for gaining access to those resources.

EX1105, [0016]. As shown, in the excerpted portion of Fig. 2 from Krantz below, the client communicates via access point 209 through port 251. The access point 209 then sends the request to data routing device 214. This data routing device acts as the gatekeeper to direct data through either port 244 or port 243.



See EX1105, [0060].

Krantz also only teaches user authentication. *E.g.*, EX1105, [0016]; EX2001, ¶ 49. Not auditing a device. EX2001, ¶ 49. Further, Krantz also fails to teach or

suggest the reconfiguration of any port (or "access point"). Moreover, in all instances, data must pass through the data routing device, which acts as a gatekeeper. *Id.*

B. Herrmann

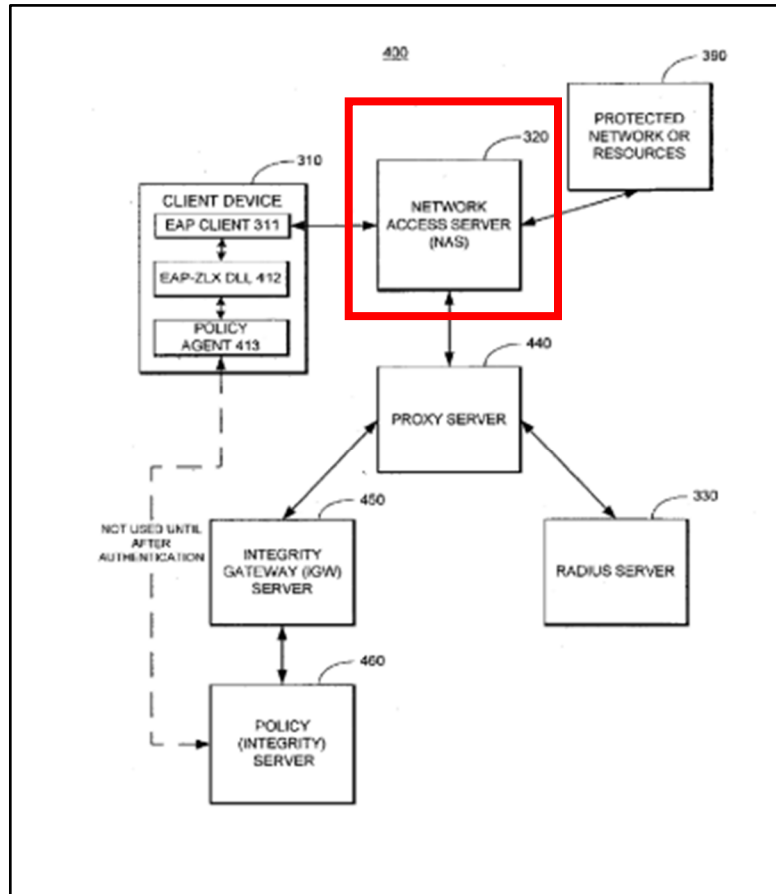
Petitioner's secondary reference for Ground 2 is U.S. Patent App. No. 2004/0107360 ("Herrmann") which is to be combined with Krantz. Herrmann was filed on March 3, 2003, and published on June 3, 2004.

Herrmann describes a system 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.

EX1106, Abstract; EX2001, ¶¶ 50-53. Herrmann describes a system and methodology for policy enforcement of a client device for access to a network. *Id.* This generally requires the device attempting to connect to pass a generic security protocol. Similar to the prior art discussed in the '350 Patent, as shown in the figure below, Herrmann places its network access servers (e.g. gatekeeper) directly between the client device and the protected network. Thus, any attempts to access

the protected network must first be checked for security policy compliance by the NAS (shown in red below).



EX1106, Fig. 1. There is no teaching of reconfiguring any access point to permit the client to access the protected network, and instead the client device must go through the NAS. EX2001, ¶ 53.

V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims

Ground 1 based on only Krantz is directed to all of the Challenged Claims. Ground 2 based on the combination of Krantz with Herrmann is directed to a subset of the Challenged Claims, namely, claims 6-10, 13, 18 and 19.

A. Ground 1: Krantz Alone Is Missing Specifically Claimed Limitations

Petitioners' Ground 1 relies solely on Krantz for obviousness. Krantz, however, fails to teach multiple required limitations, including: (1) "reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit"; and (2) several claim requirements pertaining to device auditing, including (a) "audit data pertaining to a device;" (b) "auditing the device in accordance with a security policy"; (c) "receiving updated audit data pertaining to the device subsequent to reconfiguring the access point"; and (d) "monitoring continued compliance of the device using the updated audit data." Accordingly, the petition for institution of an IPR based on Ground 1 should be denied.

1. Krantz Fails To Disclose "Reconfiguring An Access Point To Allow Access To The Less Restricted Subset Of The Network In Response To The Security Policy Audit"

The '350 Patent claims require "reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit." The specification explains that: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1101, 3:26-29. Thus, there are changing pathway assignments for the ports of *the "access point."*

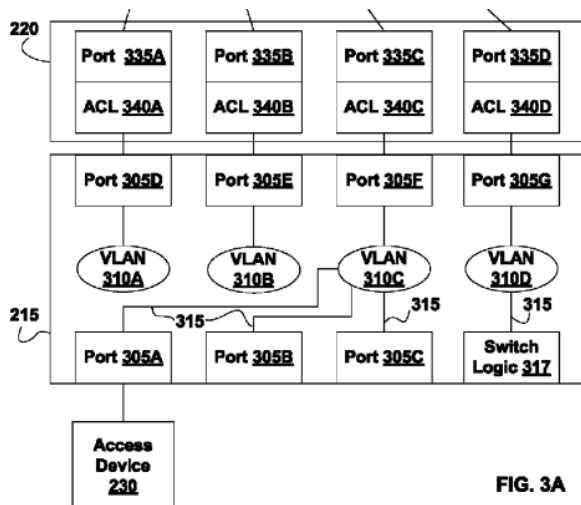


FIG. 3A

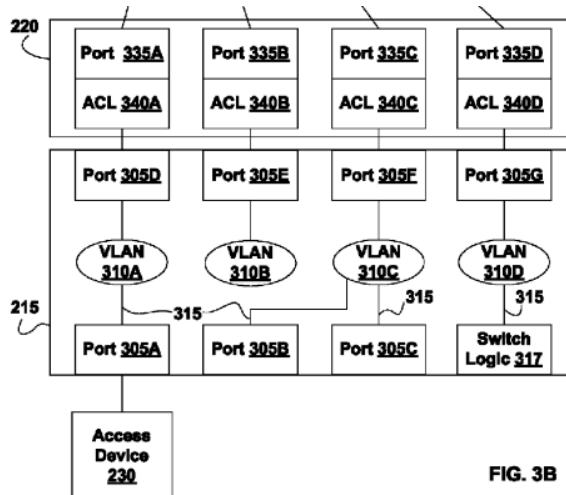


FIG. 3B

Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. VLANs 310A-310D are logical associations between members of Ports 305A-305G. Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other. These associations are illustrated in FIGS. 3A and 3B by Lines 315. EX1101, 7:66-67, 8:1-7.

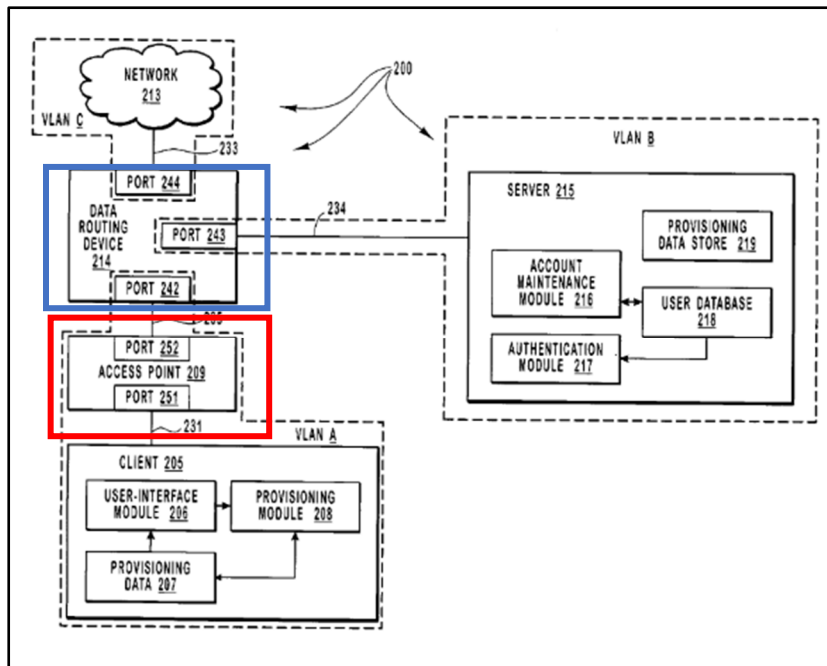
...

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. EX1101, 8:20-27.

Petitioners make three different arguments for how Krantz supposedly "reconfiguring the access point." None work.

Petitioners' Mapping #1:

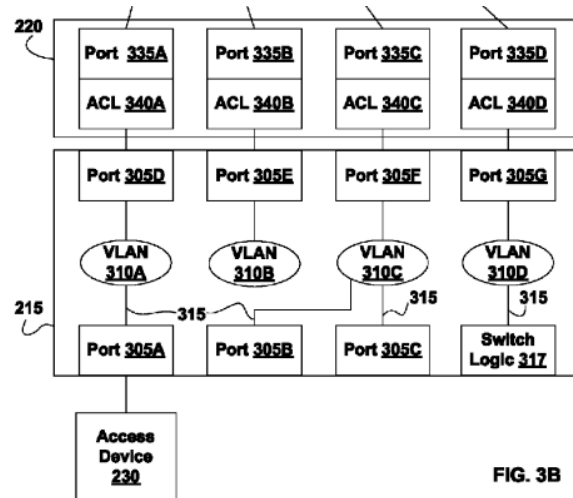
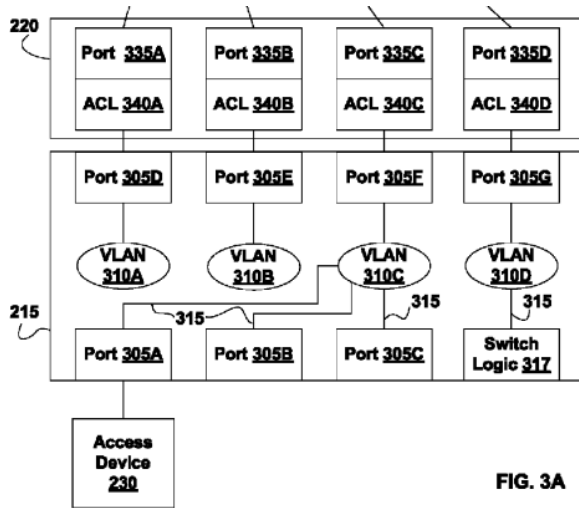
Petitioners' first argument for how Krantz supposedly discloses "reconfiguring of an access point" ignores the "access point" entirely.



Instead, it simply summarizes data flow through static ports 251, 252, 242, 243, 244. Not only are those ports not "reconfigured." Some of them are not even for the "access point."

Petitioners argue that "access point 209" (red annotation) is configured to transfer data from client 205 via port 251 to data routing device 214 via port 252. Pet. at 36. Petitioners then argue that communication ports of a different element (not the access point)—the data routing device 214 (blue annotation)— permit data to first communicates with VLAN B. Petitioners argue that after authentication of the user, "access point 209 can be 'reconfigur[ed]' in order 'to allow access to the less restricted subset of the network' because it facilitates the transfer of data between client 205 ('the device') and ultimately VLAN C (the 'less restricted subset of the network')" Pet. at 37.

This, however, is not supported. The '350 Patent is clear: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1101, 3:26-29.



This means that depending on the "reconfiguration" the same port may send data to different locations. For example, as shown in FIG. 3A of the '350 Patent above, port 305A of access point 215 sends data via 315 to VLAN 310C. In FIG. 3B, however, that same port 305A has been "reconfigured" to send data to VLAN 310A.

Krantz has no "reconfiguration." Instead, Krantz's ports send data to the same location (e.g. port 243 to VLAN B and port 244 to VLAN C). Further, Krantz explains that it is not the access point, but rather, the data routing device 214 which directs the traffic and acts as the gatekeeper to direct users either to VLAN B or VLAN C. EX1105, [0060]; EX2001, ¶59.

Accordingly, the Krantz Mapping #1 fails.

Petitioners' Mapping #2: Reconfiguring Client Data (Not Access Points)

Petitioners' second argument avoids any action on the "access point" altogether. Rather, it asserts that "[a]ccess point 209" is a "VLAN aware device and can insert Tag Headers into data frames received from client 205 ... that are then transferred to VLAN B or VLAN C." Pet. at 38-39. Put differently, the access point is not being reconfigured at all. Rather, Krantz is merely adding tag headers to something else—client data:

A tagged data frame is a data frame that includes an indication, such as, for example, a Tag Header, that identifies a VLAN and/or frame classification associated with the tagged data frame. A Tag Header can be inserted into a data frame by a VLAN aware device to indicate to data routing device 214 a VLAN ID of the VLAN from which a tagged data frame was received. For example, access point 209 can insert a Tag Header into data from client 205 to indicate to data routing device 214 that the data was received from VLAN A. A Tag Header can also include other control information that can be used by data routing device 214 to classify a corresponding data frame. An untagged data frame is a frame that does not include a Tag Header. A port VLAN ID ("PVID") may be used to indicate a VLAN from which an untagged data frame was received. For example, untagged data frames received at port 243 may be classified as being received from VLAN B.

EX1105, [0061].

As is clearly stated, it is the access point that is acting (not being acted upon) to add the Tag Header to client data, which enables a message from a client with the Tag Header data to be directed by the data routing device 214 (the gatekeeper) to VLAN C, instead of VLAN B. What is missing, however, is **any** reconfiguration of the access point 209. EX2001, ¶59. Indeed, Krantz says nothing about changing access

point 209. Instead, traffic continues to pass from access point 209 through routing device 214 (the gatekeeper).

Petitioners' Mapping #3:

Petitioners' third argument concedes "reconfiguring the access point" is missing, but incorrectly suggests it would have been obvious for one to combine access point 209 and data routing device 214 such that the Tag Headers can be configured to either be directed to VLAN C or VLAN B. Pet. at 42-44.

As discussed, not only is the access point 209 not "reconfigured," but neither is the data routing device 214. That is because configuring client data with tag headers is not reconfiguring of the access point or its ports. At best, it is client data manipulation.

Even if "tag headers" could be reconfiguration, Krantz expressly recites access point 209 and data routing device 214 as separate devices. Arbitrarily combining these separate and distinct component finds no support in Krantz. To the contrary, Petitioners' own cited portions of Krantz expressly teaches the access point 209 and the data routing device 214 are separate and distinct components. EX1105, [0073] ("[A]ccess point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity messages within an EAP-RADIUS message that is transferred onto VLAN B."). This teaching from Krantz also confirms that any alleged reconfiguration would be of user identification

data, not an access point as claimed, because "EAP-Response/Identity messages" expressly relate to user authentication.⁴ Lastly, even it were possible to combine access point 209 and data routing device 214, this would not resolve the bottleneck problem with the prior art, such as Krantz. Instead, all traffic would still go through access point 209 and data routing device 214, which acts as a gatekeeper. See EX1105, [0060].

2. Device Auditing Is Absent From Krantz

Krantz only discloses *user* authentication data. Not *device* "audit data" and *device* "auditing." Yet, the Challenged Claims specifically require several steps pertaining to *device* auditing, including (a) "audit data pertaining to a device;" (b) "auditing the device in accordance with a security policy;" (c) "receiving updated audit data pertaining to the device subsequent to reconfiguring the access point, and (d) "monitoring continued compliance of the device using the updated audit data." Despite Petitioners' attempts to conflate authentication with audit data, Krantz lacks any device auditing.

⁴ This understanding is consistent with how a POSITA understands EAP-Response/Identity. *See*, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm.

a) Krantz Fails To Disclose "audit data pertaining to a device"

The '350 Patent draws a clear distinction between user "authentication" and device "audit data." The '350 Patent explains that "audit data pertaining to a device" is data about the device's software and/or hardware that is necessary to comply with the security policy. EX1101, 11:39-50. The '350 Patent further provides examples of types of device "audit data" include: "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." *See id.*

User authentication is something different. The '350 Patent describes "authentication of a user" as information about a user; not a device, *i.e.*, "requiring the user to enter a username and password..." EX1101, 1:32-33. Authentication is a different technical concept, process, and implementation from the claimed "audit data pertaining to a device."

Yet, Krantz only discloses user authentication:

- "Krantz explains that . . . '**authentication module 217** can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in the user database 218.'" Pet. at 27.
- "If an **authenticated user** of the client 205 is authorized to access resources..." *Id.*

- "Krantz explains that the 'method 300 includes act of [client 205] sending credentials to a server to attempt to **authenticate** with the server..." *Id.* at 28-29.
- "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." *Id.* at 29.
- "If 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**) . . ." EX1105, [0019]

Despite this concession, Petitioners use several tactics to try and transform Krantz's authentication into the claimed "audit data pertaining to a device." None of them work.

Petitioners claim that Krantz discloses "receiving audit data" because it "sends credentials to the server":

Krantz "can include sending an Extensible Authentication Protocol ("EAP") Response/Identity message from the client to the server... Other credentials provided from Krantz's access 'device' may include for example, 'user-identifier[s] and password[s]." Pet. at 26.

This "credentials" argument fails immediately. First, the '350 Patent explains user authentication and "audit data pertaining to a device" are different. *Compare* EX1101, 1:32-33 (authentication) *to* 11:39-50 (audit data). Second, the Krantz "credentials" are the "user-identifier[s] and password[s]" which the '350 Patent expressly explains is authentication; not audit data. *See* Pet. at 26; EX1101, 1:32-33. Indeed, a user may access different devices using the same username and password. Third, Petitioners claim credentials also "can include sending an Extensible

Authentication Protocol ('EAP') Response/Identity message..." Pet. at 26. EAP is for authentication. In fact, it is an acronym that stands for Extensible **Authentication** Protocol. EX1101, 8:34-35, 14:31-44. Cole Decl., ¶56 (citing EX1105, [0018]-[0019]). Fourth, Petitioners assert "authentication module 217 can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in user database 218... If credential information matches an entry in user database 218, the identity of the user is authenticated." Pet. at 27. Again, on its face, this is user data unrelated to audit data for the device. EX2001, ¶¶ 56-59.

Krantz's *user* authentication disclosures do not pass muster. Indeed, the '350 Patent explains that there are disadvantages to "reliance on mere user authentication" including the lack of any assurance that the device meets network security policies. *See* EX1101, 1:45-48.

Additionally, Petitioners baldly claim that "Krantz's disclosure is consistent with the '350 Patent's description that audit data can be used to authenticate a user." Pet. at 27. This is wrong for several reasons. First, the claim requires "audit data pertaining to a device." Not to "authenticate a *user*." Second, the '350 Patent distinguishes between authenticating a user and the separate security evaluation for the device based on "audit data":

[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.**

EX1101, 13:54-67 (ALL CAPS emphasis of "AND" in original).

Lastly, this is not what the '350 Patent says. Rather, it explains that **in addition to** conducting a security policy audit for a device, the authentication of the user can be conducted within the same process. *See* EX1101, Fig. 4, 10:32-37. These are not the same things.

Accordingly, Krantz fails to disclose or suggest the claim limitation of "audit data pertaining to a device."

b) Krantz Fails To Disclose "Auditing The Device In Accordance With A Security Policy"

As set forth above, Krantz only describes user authentication, not device "audit data." For those same reasons, Krantz also does not disclose "auditing the device in accordance with a security policy." Indeed, the '350 Patent expressly distinguishes the steps of user authentication for the steps for security audits for the device:

"GateKeeper 225 authenticates a user, obtains audit data...", EX1101, 10:34-35.

"Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B." See *id.*, 11:39-42.

Notwithstanding, Petitioners again try to transform Krantz's authentication into something it is not.

Petitioners argue that "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.' Pet. at 32-33. Again, this does not suggest the "auditing the device." Petitioners' configuration settings argument is again based on user authentication. Nowhere in Petitioners' cited portions of Krantz is any comparison of a security policy for a device discussed. Instead, in Petitioners' cited portion of Krantz (EX1105, [0066]-[0067]), the authentication only relates to user identification. EX2001, ¶¶ 56-59.

Similarly, Petitioners reference to an EAP-Response/Identity message or and EAP-MSChapV2 does not change this. Each of the EAP-Response/Identity message or and EAP-MSChapV2 message relates to user authentication.⁵ But, the Challenged Claims require "auditing the device in accordance with a security policy"—

⁵ See <https://www.portnox.com/cybersecurity-101/mschapv2/> (EAP-MSChapV2); https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm (EAP-Response/Identity).

something different from Krantz's user identification. The '350 Patent makes this clear distinction:

According to embodiments like that disclosed in U.S. Provisional Patent Application No. 60/513,080, the disclosure of which has been incorporated herein by reference, an 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 endpoints 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."**

EX1101, 13:53-67.

Indeed, the known EAP or 802.1x user authentication mechanisms and associated credentials and specifics are distinct from "auditing the device." In fact, "MSCHAPv2" is an acronym for "Microsoft Challenge Handshake Authentication Protocol version 2," and is an authentication protocol used for securing remote access connections in Virtual Private Networks (VPNs). As the portnox article referenced in footnote 5 explains, " MSCHAPv2 is used to verify the identity of a

user or device trying to establish a connection to a network or a remote server." It has nothing to do with whether a device meets a security policy for a device.⁶

c) Krantz Fails To Disclose "Receiving Updated Audit Data Pertaining to the Device Subsequent to Reconfiguring The Access Point"

Just like Krantz failed to disclose device "audit data," it also fails to disclose "receiving updated audit data pertaining to the device." Once again, however, Petitioners' arguments trying to transform user authentication into "updated audit data pertaining to the device" only demonstrate why such contortion does not work. Petitioners claims that a subscription paid for by a user can expire, and Krantz provides for checking of the user's subscription. But the validity of a user's subscription has nothing to do with the device or device compliance with a security policy.

Petitioners' references to an EAP-Response/Identity message or and EAP-MSChapV2 do not change this. Each of the EAP-Response/Identity message or and EAP-MSChapV2 message relates to user authentication.⁷ But, the claim requires

⁶ Notably, Petitioners' secondary reference, Herrmann, confirms that authentication technology, e.g., NAS and RADIUS, are distinct from security policy compliance. "One problem that is not addressed by current NAS and RADIUS [authentication] technology is ensuring that all devices that connect to a network comply with and enforce applicable security policies." EX1106, [0011]

⁷ See <https://www.portnox.com/cybersecurity-101/mschapv2/> (EAP-MSChapV2); https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm (EAP-Response/Identity).

that the audit data relates to the device and a security policy – something different from Krantz. EX2001, ¶¶ 56-59

d) Krantz Fails To Disclose "Monitoring Continued Compliance Of The Device Using The Updated Audit Data"

The Challenged Claims also require "monitoring continued compliance of the device using the updated audit data." This limitation is also missing from Krantz. EX2001, ¶¶ 56-59.

Petitioners rely on Krantz's disclosure that after a period of time, the Krantz system may re-authenticate the user based on whether the user's subscription is still valid. Pet. at 46-47. Re-authentication does not involve any updated audit data because it is not audit data about a device and also because it is not updated data. As with the flaw to all of Petitioners' related to audit data, so too does Krantz fails to disclose the subject claim limitation because user authentication is different from security policy compliance of a device.

B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious Claims 6-10, 13, 18 or 19

Petitioners only argue that claims 6-10, 13, 18 and 19 are obvious in view of Krantz in combination with Herrmann.⁸

⁸ Petitioners concede that the Ground 2 combination with Herrmann does not render independent claim 1 obvious. Thus, if the Board determines not to institute on Ground 1, there would also be no independent reason to institute on Ground 2.

Claims 6-10, 13, 18 and 19 are each dependent claims from independent claim 1. Petitioners rely on Herrmann for the additional requirements of claims 6-10, 13, 18 and 19. For at least the reasons discussed with respect to Ground 1 and the failure of Krantz to disclose several claimed limitations, Ground 2 must fail. EX2001, ¶60.

Claim 6 depends from claim 1. Each of the remaining claims in Ground 2 depend on claim 6. Petitioners argue that the requirement of claim 6, namely an agent running on the device to collect audit data, would have been obvious to include with Krantz because Herrmann discloses an agent on the client. As discussed, Krantz says nothing about audit data related to a device. Rather, Krantz is directed only to user authentication. For this reason alone, it makes no sense to include an agent to collect audit data for the device with Krantz.

For the reasons discussed, the combination of Krantz and Herrmann fail to disclose all of the claimed limitations. As such, even if one would have been motivated Krantz with Herrmann, Ground 2 still fails.

Nonetheless, a POSITA would not have been motivated to combine Krantz and Herrmann. The '350 Patent expressly teaches that prior art methods for determining user authentication and security policy compliance face the problem that a gatekeeper creates a bottleneck. Krantz simply relates to providing a means for a person to pay to access the internet, such as at a hotel or airport. Herrmann concerns itself with security policy compliance, and places multiple servers between

the client and the protected network. Essentially, Krantz and Herrmann are references that the '350 Patent sought to improve upon. Neither Krantz nor Herrmann, however, even recognize the bottleneck problem identified by the '350 Patent. Petitioners' argument boils down to an improper use of the '350 Patent as the impetus for combining Krantz and Herrmann, a decidedly improper argument. *See* Pet. at 13-20.

Moreover, Krantz's lack of any teaching of audit data for a device means that Herrmann's teaching of an agent for collecting audit data would be meaningless to Krantz. For this reason as well, there would be no motivation to combine.

VI. All Grounds: Neither Reference Constitutes Prior Art

The Board has previously found antedating prior art references is sufficient grounds for denying *inter partes* review institution. *LG Elecs., Inc. v. Wi-LAN Inc.*, No. IPR2018-00704, Paper No. 14 at 20 (P.T.A.B. Sept. 5, 2018) (“[W]e determine that Patent Owner has provided sufficient evidence to antedate ZTE . . . [and therefore] Petitioner has not demonstrated a reasonable likelihood of prevailing[.]”).

Neither Krantz nor Herrmann are prior art because the InfoExpress inventors conceived of the invention before the effective dates and exercised reasonably continuous diligence in reducing to the claimed inventions to practice.

A. Legal Standards

A reference is prior art only if filed before the date of “the invention by the [patent owner].” 35 U.S.C. § 102(e) (pre-AIA). *See, e.g., Sequenom v. Leland Stanford Junior Univ.*, No. IPR2013-00390, at 5 (P.T.A.B. Nov. 25, 2014); *Dynamic Drinkware LLC v. Nat’l Graphics, Inc.*, No. IPR2013-00131, at 7 (P.T.A.B. Sept. 12, 2014) *aff’d*, 800 F.3d 1375 (Fed. Cir. 2015).

To antedate a reference, a Patent Owner must show that there was conception prior to the critical date and “reasonably continuous diligence” throughout the critical period from just before the effective date of the prior art until reduction to practice. *E.g., ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019); *Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc.*, 774 F.3d 968, 975 (Fed. Cir. 2014).

Under the reasonably continuous diligence standard, an inventor is not required to work on reducing the invention to practice every day during the critical period, and periods of inactivity within the critical period do not automatically vanquish a claim of reasonable diligence. *ATI*, 920 F.3d at 1369; *Monsanto Co. v. Mycogen Plant Sci., Inc.*, 261 F.3d 1356, 1369 (Fed. Cir. 2001); *Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.*, 841 F.3d 1004, 1009 (Fed. Cir. 2016).

Additionally, an attorney’s work preparing a patent application can demonstrate diligence. *Perfect Surgical*, 841 F.3d at 1009-1012; *Bey v. Kollonitsch*, 806 F.2d 1024, 1030 (Fed. Cir. 1986).

Inventor declarations submitted to establish conception and diligence must be corroborated.⁹ *Perfect Surgical*, 841 F.3d at 1007. The “rule of reason” analysis governs whether corroboration is sufficient to establish diligence. *Id.* at 1009. “A variety of activities may corroborate an inventor’s testimony of reasonable diligence, and such corroborating evidence is considered ‘as a whole.’” *Id.* at 1007-08 (quoting *Brown v. Barbacid*, 436 F.3d 1376, 1380 (Fed. Cir. 2006)). The patent owner need not corroborate every contested factual issue, but instead merely needs to produce sufficient independent circumstantial evidence to support the testimony. *Perfect Surgical*, 841 F.3d at 1009.

The purpose of diligence is to show that the invention was not abandoned, set aside, or unreasonably delayed, not to “scour the patent owner’s corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity.” *Id.* Indeed, “[a] patent owner need not prove the inventor continuously exercised reasonable diligence throughout the critical period; it must show there was reasonably continuous diligence.” *See ATI*, 920 F.3d at 1369.

⁹ No corroboration of the technical content in documentary evidence is required. *See Price v. Symsek*, 988 F.2d 1187, 1195 (Fed. Cir. 1993) (“‘[C]orroboration’ is not necessary to establish what a physical exhibit before the board includes. Only the inventor’s testimony requires corroboration before it can be considered.”); *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1169 (Fed. Cir. 2006).

B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.

Petitioners assert that Krantz has an effective date of December 6, 2002 and Herrmann has an effective date of March 13, 2003.¹⁰ Pet. at 7, 9. InfoExpress conceived of the claimed invention before that.

On November 14, 2002, the InfoExpress inventors had the “CyberGatekeeper LAN Based Policy Enforcement Engineering Specification” (EX2011: “LAN Engineering Specification”) prepared demonstrating that the claimed inventions were conceived of at least as of that date. EX2003 (Lum Declaration), ¶12; EX2012. This conception is demonstrated in the claim chart mapping by Dr. Smith showing the LAN Engineering Specification mapped to the challenged claims as set forth in EX2009. EX2007.

Indeed, leading up to the November 14, 2002, LAN Engineering Specification, InfoExpress had started diligently working.

[REDACTED]

[REDACTED]

¹⁰ Herrmann’s provisional date is listed as December 2, 2002. Petitioners waived any right to establish this provisional date as the §102(e) date because they failed to submit, mention, or analyze its provisional filing in the Petition. *SAS Institute Inc. v. Iancu*, 138 S.Ct. 1348, 1355 (2018) (the petition must define the boundaries of the IPR); *Globus Med., Inc. v. Depuy Synthes Prods., LLC*, No. IPR2015-00107, at *3 (P.T.A.B. May 1, 2015). Notwithstanding, the Herrmann provisional date is still later in time than the November 14, 2002, conception of the claimed inventions and thus would not be prior art regardless.

[REDACTED]

This was groundbreaking because preexisting security technologies did not include the implementation of auditing support functionality over authentication protocols such as 802.1x. Mr. Lum and the InfoExpress team diligently worked in October 2002 and November 2002 to produce the LAN Engineering Specification of November 14, 2002. EX2056; EX2061; EX2021.

C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.

Before and after the November 14, 2002 LAN Engineering Specification, InfoExpress exercised reasonably continuous diligence up and through at least the filing of U.S. Patent Application No. 60/513,080 on October 21, 2003. The filing of this application constitutes constructive reduction to practice of the claimed inventions. EX2007, EX2010.

The InfoExpress inventors, employees, and team members diligently pursued reducing the claimed invention to practice from conception until constructive reduction to practice on at least October 21, 2003. This diligence is shown by substantial InfoExpress evidence including emails, technical specifications and analyses, iii) source code, and iv) the Declaration of Inventor and InfoExpress CEO Stacey Lum. EX2003.

As further detailed in the diligence calendar submitted herewith, InfoExpress worked consistently to reduce the claimed invention to practice. This evidence leaves no doubt that the InfoExpress inventors conceived of and diligently pursued reduction to practice during the critical period. *See ATI*, 920 F.3d at 1373 (Court finding that Patent Owner’s evidence did “not point to the remotest suggestion of abandonment or setting aside” where the Patent Owner provided a calendar demonstrating that designated activity on the majority of days in the diligence period, and a declaration summarizing various documents in support of diligence); *Monsanto*, 261 F.3d at 1369 (Court finding substantial diligence evidence where the Patent Owner identified record evidence showing activity multiple times per month during the critical period, and there was no reason to doubt that the activity was relevant in reducing the invention to practice).

December 2002

• [REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

- See EX2003, ¶¶ 6-7, 30, 33, 37, 49 (Lum Declaration).

January 2003

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]
- Mr. Lum spoke with eventual patent counsel to clear conflicts.
EX2212.
- See EX2003, ¶¶6-7, 30, 33, 37, 49) (Lum Declaration)

February 2003:

- [REDACTED]
- [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- See EX2003, ¶¶ 32-33, 38, 40-43, 50-51, 56-57 (Lum Declaration).

March 2003:

- [REDACTED]
- [REDACTED]

[REDACTED]

- See EX2003, ¶¶44, 52, 58) (Lum Declaration)

April 2003:

- [REDACTED]

[REDACTED]

[REDACTED]

May 2003:

- [REDACTED]

[REDACTED]

[REDACTED]

- See EX2003, ¶¶44-45, 52 (Lum Declaration).

June 2003:

- [REDACTED]

- See EX2003, ¶53 (Lum Declaration).

July 2003:

[REDACTED]

[REDACTED]

August 2003

- [REDACTED]

[REDACTED]

- See EX2003, ¶¶52 (Lum Declaration).

September 2003

- [REDACTED]

- U.S. Provisional Patent Application Serial No. 60/505,582 was filed on September 24, 2003.

- [REDACTED]

- [REDACTED]

- See EX2003, ¶¶53, 62-63 (Lum Declaration).

October 2003

- [REDACTED]

- [REDACTED]

- U.S. Provisional Patent Application Serial No. 60/513,080 was filed on October 21, 2003.
- *See* EX2003, ¶¶14, 23, 25, 64-66 (Lum Declaration).

D. The Filing of U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003 Constitutes Constructive Reduction to Practice.

As set forth in EX2010 and discussed by Prof. Smith (EX2007), the ‘080 Provisional provides written description support for the Challenged Claims in accordance with pre-A.I.A. 35 U.S.C. §§ 119(e) & 112, ¶ 1.

The evidence discussed above demonstrates diligence on the part of the inventors towards reducing the claimed invention to practice. *ATI*, 920 F.3d at 1374.

VII. Conclusion

For these reasons, Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims.

Respectfully submitted,

Dated: June 26, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	<i>/s/ Brian R. Michalek</i> Brian R. Michalek (Reg. No. 65,816) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 brian.michalek@saulewing.com Joseph M. Kuo (Reg. No. 38,943) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 joseph.kuo@saulewing.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saulewing.com Counsel for Patent Owner
---	---

Certification of Word Count Under 37 C.F.R. § 42.6(d)

The undersigned hereby certifies that the foregoing complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the document contains 13,365 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: June 26, 2024

/Brian R. Landry/
Reg. No. 62,074

Certification of Service Under 37 C.F.R. § 42.6(e)(4)

The undersigned hereby certifies that the foregoing was served in its entirety by filing through the Patent Trial and Appeal Board P-TACTS, as well as providing a courtesy copy via e-mail to the attorneys of record.

Date: June 26, 2024

/Brian R. Landry/
Reg. No. 62,074