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.

IPR2024-00676
U.S. Patent No. 8,677,450

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

PAGE

I. Introduction....1

II. The '450 Patent....1

A. Date of Invention....1
B. Person of Ordinary Skill in the Art (POSITA)....1
C. Overview of the '450 Patent....2

III. Claim Construction....5

A. "Information Regarding the Device" and "Providing Information to the Access Device"....6
B. "Configuring The Access Point"....9

IV. Petitioners' Cited References....10

A. Krantz....10
B. Herrmann....13

V. Krantz in Combination with Herrmann Fails to Render the Challenged Claims Obvious....15

A. The Use of Device "Information" and Device "Auditing" Distinct From Authentication Is Absent From Krantz and Herrmann....15

1. Krantz and Herrmann Fail To Disclose "Information" Regarding the Device As Claimed....15
2. Krantz And Herrmann Fail To Disclose "Performing An Audit Of The Access Device" Distinct from Authentication....21

B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Applying A Security Policy" Limitation (All Challenged Claims)....24
C. Krantz and Herrmann Fail To Disclose "Configuring The Access Point" Limitation....27

VI. All Grounds: Neither Reference Constitutes Prior Art....33

A. Legal Standard.....33
B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....35
C. The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice. 36
D. The Inventors Achieved a Constructive Reduction to Practice by the Filing of U.S. Provisional Patent Application Serial No. 60/513,080, Which Was Filed on October 21, 2003.....45

VII. Conclusion 45

TABLE OF AUTHORITIES

ATI Techs. v. Iancu, 920 F.3d 1362 (Fed. Cir. 2019) 34

Bey v. Kollonitsch, 806 F.2d 1024 (Fed. Cir. 1986) 34

Globus Med., Inc. v. Depuy Synthes Prods., LLC, No. IPR2015-00107 (P.T.A.B. May 1, 2015) 35

LG Elecs., Inc. v. Wi-LAN Inc., No. IPR2018-00704 (P.T.A.B. Sept. 5, 2018) 33

Monsanto Co. v. Mycogen Plant Sci., Inc., 261 F.3d 1356 (Fed. Cir. 2001) 34, 37

Perfect Surgical Techs., Inc. v. Olympus Am., Inc., 841 F.3d 1004 (Fed. Cir. 2016).....34, 35

Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005) 6

Polaris Indus., Inc. v. Arctic Cat, Inc., 882 F.3d 1056 (Fed. Cir. 2018).....25, 26

SAS Institute Inc. v. Iancu, 584 U.S. 357, 138 S. Ct. 1348 (2018).....35

Sequenom v. Leland Stanford Junior Univ., No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014).....33

Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc., 774 F.3d 968 (Fed. Cir. 2014).....34

Willis Elec. Co. v. Polygroup Macau Ltd. (BVI), 777 F. App'x 495, 498 (Fed. Cir. 2019) 8-9, 17

FEDERAL STATUTES

35 U.S.C. § 102(e) 41, 42

35 U.S.C. § 103 1

35 U.S.C. § 112, ¶ 1 53

35 U.S.C. § 119(e) 53

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	Diligence Calendar
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 '450 Patent
2010	Constructive Reduction to Practice of the '450 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
2035	Draft Meetinghouse Agreement

Exhibit Number	Description
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
2072	Network Device Configuration API Engineering Specification

Exhibit Number	Description
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
2109	Correspondence with Globe Tech

Exhibit Number	Description
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
2146	Correspondence with Globe Tech

Exhibit Number	Description
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
2183	Correspondence with Globe Tech

Exhibit Number	Description
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
2220	Correspondence with patent counsel

Exhibit Number	Description
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
2257	Correspondence with patent counsel

Exhibit Number	Description
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
2272	Intentionally Left Blank
2273	Correspondence between S. Lum, J. Ong, C. Tsai and A. Lee
2274	Correspondence between S. Lum, C. Tsai and A. Lee
2275	Internal Notes
2276	Correspondence between C. Tsai, J. Ong and S. Lum
2277	Correspondence between C. Tsai, J. Ong and S. Lum
2278	Correspondence between C. Tsai, J. Ong and S. Lum
2279	Correspondence between C. Tsai, J. Ong and S. Lum
2280	Correspondence between C. Tsai and S. Lum
2281	Correspondence between T. Nakano and S. Lum
2282	Draft Meetinghouse Agreement
2283	Correspondence with Globe Tech
2284	Intentionally Left Blank
2285	Correspondence between S. Lum and corporate counsel
2286	Intentionally Left Blank
2287	Correspondence with Globe Tech
2288	Correspondence with Globe Tech
2289	Correspondence with Globe Tech
2290	Correspondence with Globe Tech
2291	Correspondence with Globe Tech
2292	Correspondence with Globe Tech
2293	Correspondence with Globe Tech
2294	Correspondence with Globe Tech

Exhibit Number	Description
2295	Correspondence with Globe Tech
2296	Correspondence with Globe Tech
2297	Correspondence with Globe Tech
2298	Correspondence between S. Lum and J. Ong
2299	Correspondence between S. Lum and J. Ong
2300	Correspondence with Globe Tech
2301	Correspondence with Globe Tech
2302	Correspondence between M. Banin and S. Lum
2303	Correspondence with Globe Tech
2304	Correspondence with Globe Tech
2305	Correspondence with Globe Tech
2306	Correspondence with Globe Tech
2307	Correspondence with Globe Tech
2308	Correspondence with Globe Tech
2309	Correspondence with Globe Tech
2310	Correspondence with Globe Tech
2311	Correspondence with Globe Tech
2312	Correspondence with Globe Tech
2313	Correspondence with Globe Tech
2314	Correspondence with Globe Tech
2315	Correspondence with Globe Tech
2316	Correspondence with Globe Tech
2317	Correspondence with Globe Tech
2318	Correspondence with Globe Tech
2319	Correspondence with Globe Tech
2320	Correspondence with Globe Tech
2321	Correspondence with Globe Tech
2322	Correspondence with Globe Tech
2323	Correspondence with Globe Tech
2324	Correspondence with Globe Tech
2325	Correspondence with Globe Tech
2326	Correspondence with Globe Tech
2327	Draft Patent Application
2328	Draft Patent Application
2329	CyberGatekeeper Enforcement Modes
2330	CyberGatekeeper Enforcement Modes
2331	Correspondence with Globe Tech

Exhibit Number	Description
2332	Correspondence with Globe Tech
2333	Correspondence with Globe Tech
2334	Correspondence with Globe Tech
2335	Correspondence with Globe Tech
2336	Correspondence with Globe Tech
2337	Correspondence with Globe Tech
2338	Correspondence with Globe Tech
2339	Correspondence with Globe Tech
2340	Internal InfoExpress Correspondence
2341	Intentionally left blank
2342	Internal InfoExpress Correspondence
2343	Correspondence with Globe Tech
2344	Correspondence with Globe Tech
2345	Correspondence with Globe Tech
2346	Correspondence with Globe Tech
2347	Correspondence with Globe Tech
2348	Correspondence with Globe Tech
2349	Correspondence with Globe Tech
2350	Correspondence with Globe Tech
2351	Correspondence with Globe Tech
2352	Correspondence with Globe Tech
2353	Correspondence with Globe Tech
2354	Correspondence with Globe Tech
2355	Correspondence with Globe Tech
2356	Correspondence with Globe Tech
2357	Correspondence with Globe Tech
2358	Correspondence with Globe Tech
2359	Correspondence with Globe Tech
2360	Correspondence with Globe Tech
2361	Correspondence with Globe Tech
2362	Correspondence with Globe Tech
2363	Correspondence with Globe Tech
2364	Correspondence with Globe Tech
2365	Correspondence with Globe Tech
2366	Correspondence with Globe Tech
2367	Correspondence with Globe Tech
2368	Correspondence with Globe Tech

Exhibit Number	Description
2369	Correspondence with Globe Tech
2370	Correspondence with Globe Tech
2371	Correspondence with Globe Tech
2372	Correspondence with Globe Tech
2373	Correspondence with Globe Tech
2374	Correspondence with Globe Tech
2375	Correspondence with Globe Tech
2376	Correspondence with Globe Tech
2377	Correspondence with Globe Tech
2378	Correspondence with Globe Tech
2379	Correspondence with Globe Tech
2380	Correspondence with Globe Tech
2381	Correspondence with Globe Tech
2382	Correspondence with Globe Tech
2383	Intentionally left blank
2384	Correspondence with Globe Tech
2385	Correspondence with Globe Tech
2386	Internal InfoExpress Correspondence
2387	Correspondence with Globe Tech
2388	Correspondence with Globe Tech
2389	Internal InfoExpress Correspondence
2390	Correspondence with Globe Tech
2391	Intentionally left blank
2392	Intentionally left blank
2393	Intentionally left blank
2394	Intentionally left blank
2395	Correspondence with Globe Tech
2396	Internal InfoExpress Correspondence
2397	Correspondence with Globe Tech
2398	Intentionally left blank
2399	Correspondence with Globe Tech
2400	Correspondence with Globe Tech
2401	Correspondence with Globe Tech
2402	Correspondence with Globe Tech
2403	Correspondence with Globe Tech
2404	Correspondence with Globe Tech
2405	Correspondence with Globe Tech

Exhibit Number	Description
2406	Correspondence with Globe Tech
2407	Correspondence with Globe Tech
2408	Correspondence with Globe Tech
2409	Correspondence with Globe Tech
2410	Correspondence with Globe Tech

I. Introduction

Patent Owner InfoExpress Inc. submits this Patent Owner Preliminary Response to the Petition for *Inter Partes* Review by Petitioners related to claims 1-4, 7-10, 14, 16, 22-23, 25 and 27 (the "Challenged Claims") of U.S. Patent 8,677,450 (the '450 Patent"). Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims. Patent Owner submits 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 '450 Patent

A. Date of Invention

Patent Owner submits that for the reasons discussed in section VI 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 '450 Patent

The '450 Patent is directed to a novel and seminal approach to a security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required a "gatekeeper" placed directly between each client, i.e., user, and the network. EX1401, Fig. 1, 2:34-42; EX2001, ¶¶ 44-46. But as the '450 Patent further explains, access control further required evaluation of each accessing device's hardware and software, *e.g.*, virus protection and operating systems, before the gatekeeper granted such access—thus consuming substantial network resources and creating bottlenecks. EX1401, 2:27-30, 2:39-45. An example of the prior art architecture is shown in annotated FIG. 1 of the '450 Patent.

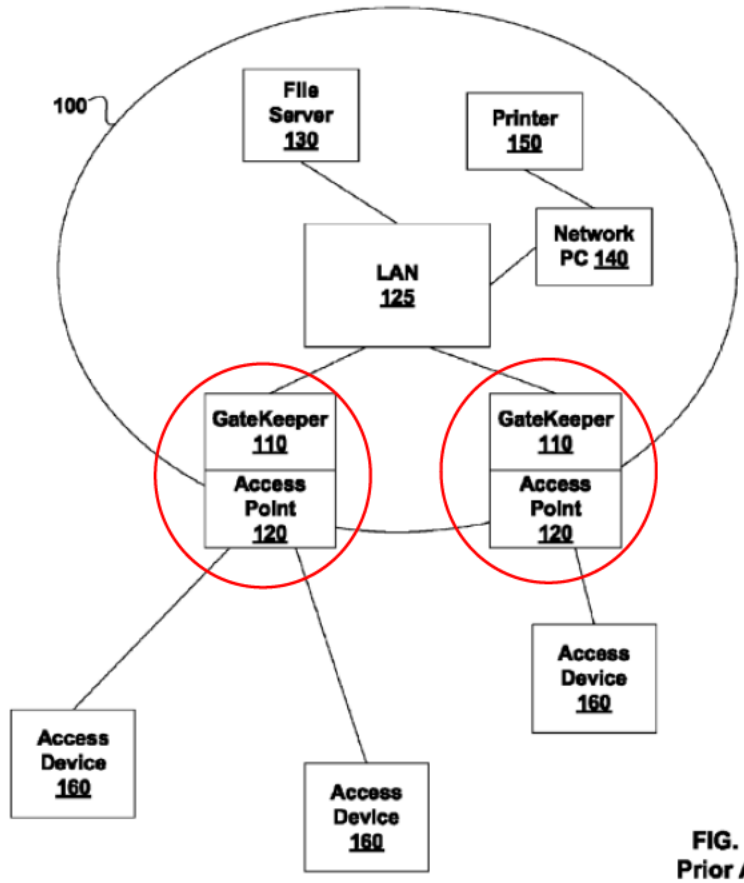


FIG. 1
Prior Art

The protected network 100 included two Gatekeepers 110, each associated with a different instance of an Access Point 120. With large corporate networks including many access points, 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." EX1401, 2:39-42. The gatekeeper then becomes a limiting bottleneck on the bandwidth of the system. EX1401, 2:42-45.

The '450 Patent addressed this particular problem with a new, novel, and non-obvious approach that relieves computer resources by configuring an access point for previously authorized devices to access a protected network.

By way of example, the '450 Patent discloses a protected network that includes a restricted subset with a gatekeeper and one or more less-restricted subsets.

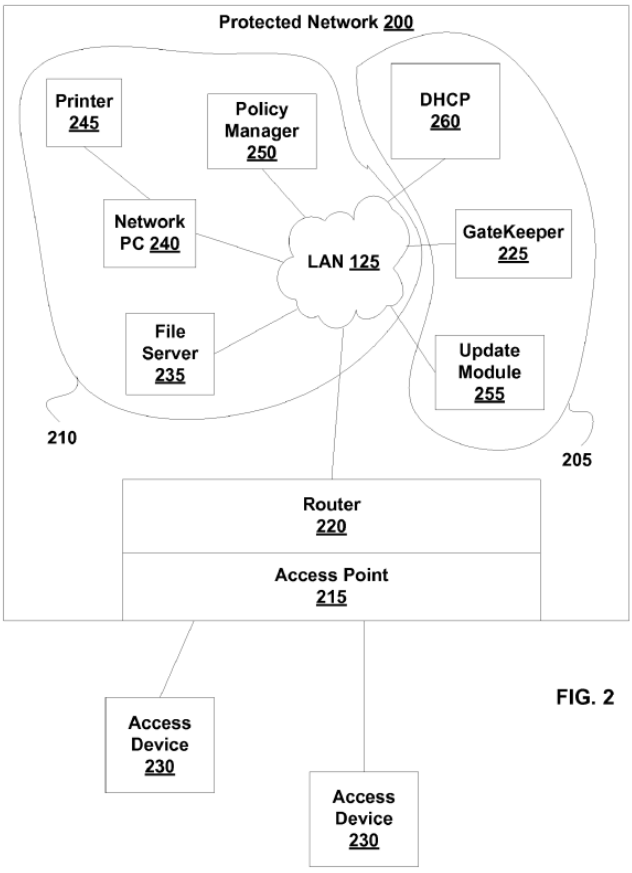


FIG. 2

EX1401, 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). EX1401, 2:58-60, 5:38-40. 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. EX1401, 2:60-64.

A key feature of the '450 Patent is that rather than require all device access requests to pass through the gatekeeper, the access point itself is configured.

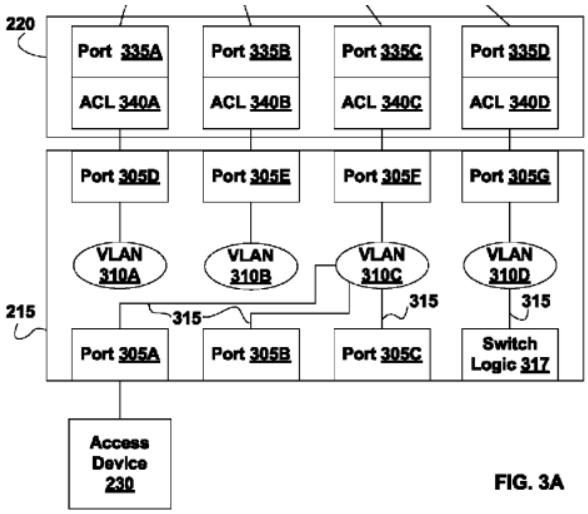


FIG. 3A

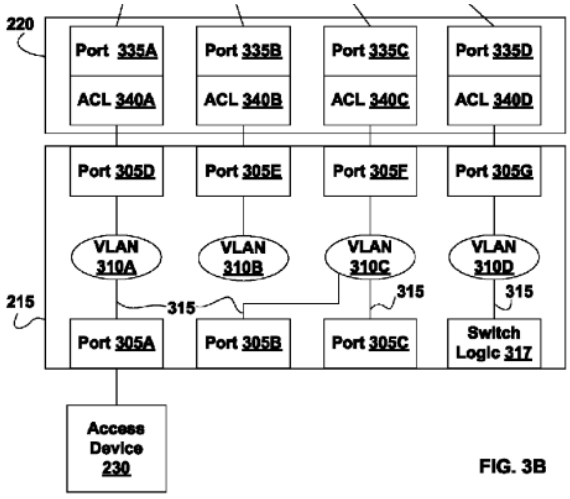


FIG. 3B

> 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.

EX1401, 8:25-32.

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.

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. Pet. at 7. Petitioners, however, avoid providing any explanation and deviate from the plain 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 ‘450 intrinsic evidence. Patent Owner contends the claims should be given their plain meaning in the context of the intrinsic evidence.

A. "Information Regarding the Device" and “Providing Information to the Access Device”

The claim terms "information regarding the device" and "providing information to the access device" are specifically directed to ensuring that the **device** that is attempting to access the network meet (or maintain) 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). Here, the claim language itself is clear. First, independent claim 1 specifically recites "information regarding the device" (as opposed to the user). Similarly, independent claims 16 and 22 recite "providing information to the access device." As such, the plain language of the claim requires the "information" to be expressly about the device. Not user authentication. The ‘450 claims expressly distinguishes the claimed "information" regarding the device and authentication:

1. A method for applying a security policy to network devices, the method comprising:

performing an authentication of a device connected to an access point;

scanning the device to collect information regarding the device;

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

configuring the access point in response to a result of applying the security policy.

EX1401, 16:10-21 (annotations added); *see also* 16:54-67 & 17:1-2 (claim 16 reciting "providing information to the access device to improve compliance" and "authenticating a user of the access device.").

The specification further establishes that "information regarding the device" and "authentication" are two different evaluations. "Reliance on mere user authentication includes several disadvantages. For example, there are no provisions to assure that an access device used by the authenticated user meets network security policies." EX1401, 2:48-51. The '450 Specification makes this express distinction between the claimed device "information" and user "authentication":

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

EX1401, 2:23-25. 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.

EX1401, 10:35-49.

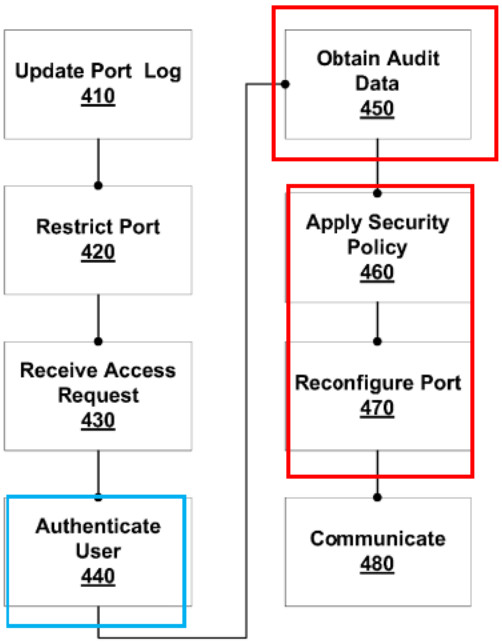


FIG. 4

Accordingly, the claim terms "information regarding the device" and "providing information to the access device" should be given their plain meaning consistent with the intrinsic evidence and not conflated with user authentication. *See Willis Elec. Co., Ltd. v. Polygroup Macau Ltd. (BVI)*, 777 F. App'x 495, 498 (Fed.

Cir. 2019) (finding Petitioner's construction "flawed" when it "d[id] not delineate between two separately recited elements").

B. "Configuring The Access Point"

Independent claims 1 and 22 require "configuring the access point" in response to an audit and to allow access. EX1401, 16:20-21 (claim 1), 17:27-28 (claim 22). In the intrinsic context, the plain and ordinary meaning of this limitation requires configuration of an ***access point***—not a change to the end user device (i.e., "access device") or to user identification data.

The '450 Patent specification is consistent with this plain meaning. For example, it explains: "The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1401, 3:30-33.

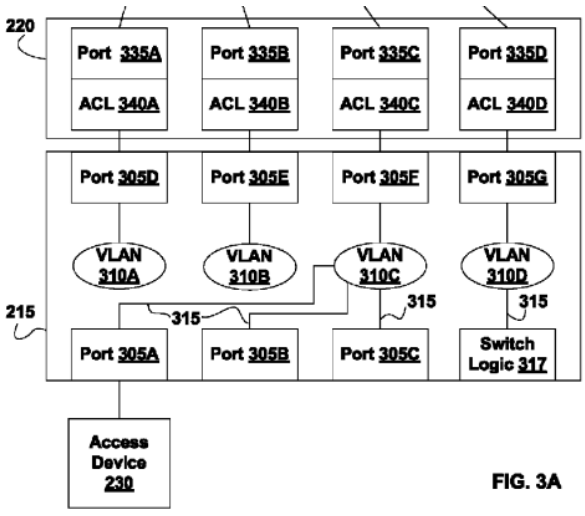


FIG. 3A

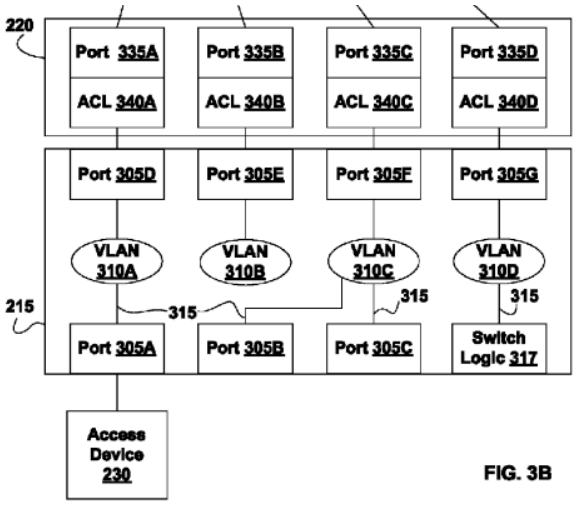


FIG. 3B

This "reconfiguring" is shown above and explained by the '450 Patent:

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.

EX1401, 8:4-12.

As shown in FIGS. 3A-3B, the "configuring" of the access point 215 shows the reassigning of Lines 315 from a port to a different VLAN. Thus, plain meaning for "configuring the access point" requires there to be a change to the access point itself; not a change to something else.

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 approaches improved upon by the '450 Patent.

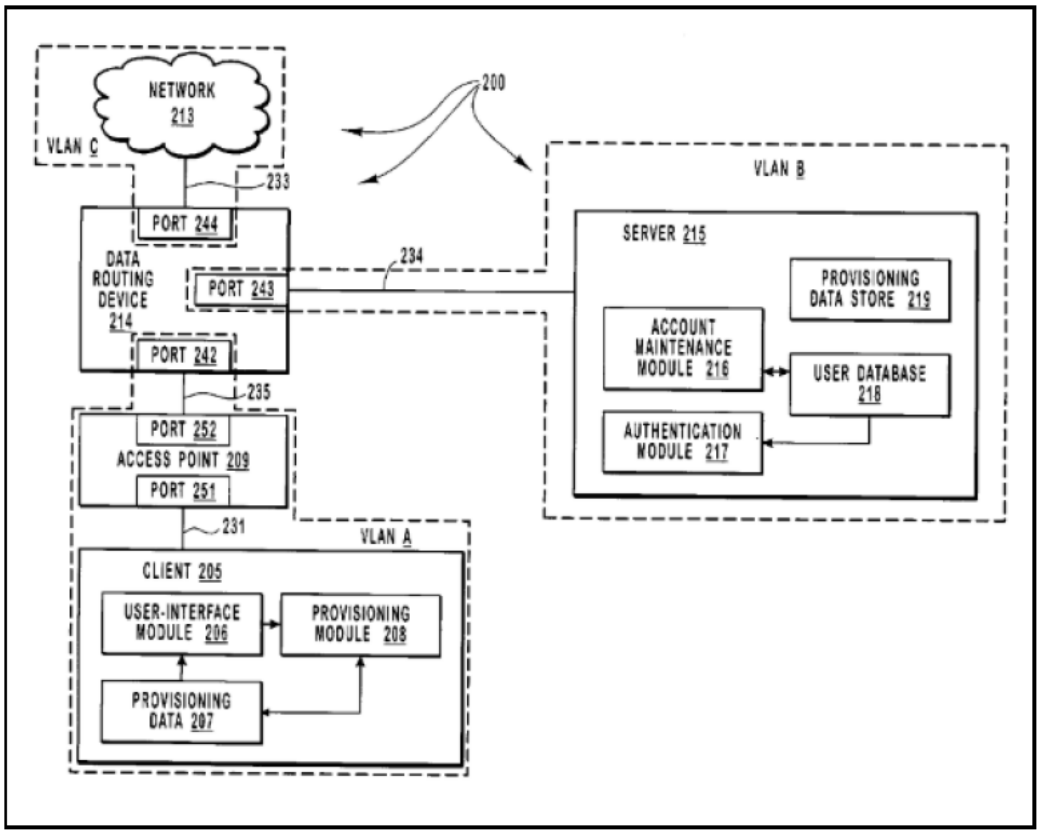
A. Krantz

Petitioners' primary reference is U.S. Patent No. 2004/0111520 ("Krantz"), which was filed on December 6, 2002. 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.

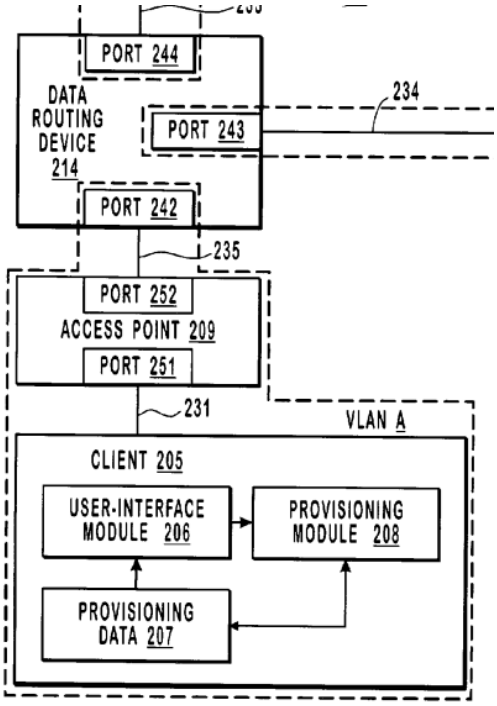
EX1405, Abstract. Krantz discloses the concept wherein upon the failure of a computer system to authenticate to one network, the computer system is permitted to access a second network for the limited purpose of downloading files by a server. EX2001, ¶¶47-49.



EX1405, cover page. 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.

EX1405, [0016]. As shown, in the excerpted portion of Fig. 2 from Krantz, an access point 209 is identified and the client communicates via access point 209 through port 251. The access point 209 then sends data to data routing device 214 via port 252. This data routing device directs data through either port 244 or port 243.



There is no teaching in Krantz of changing any configuration for any port, and more specifically, Krantz does not teach changing the configuration of any port of the access point 209. EX2001, ¶¶63-66. Instead, all data pass ports 251 and 252 and then pass to the data routing device.

B. Herrmann

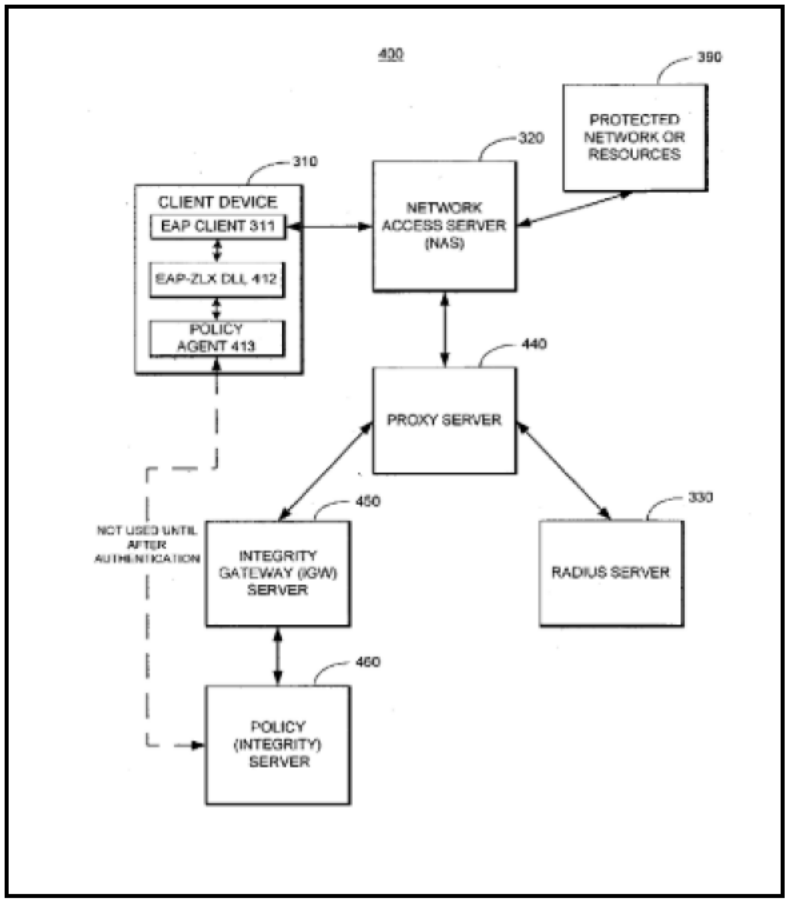
Petitioners cite to U.S. Patent App. No. 2004/0107360 ("Herrmann") to be used in combination with Krantz. Herrmann was filed on March 13, 2003, and published on June 3, 2004.

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.

EX1406, Abstract; EX2001, ¶¶50-53. Like the prior art discussed in the '450 Patent, Herrmann utilizes servers between the client device and the protected network, and any attempts to access the protected network must first be checked for security policy compliance by at least a Network Access Server (NAS), which would create the bottleneck problems. EX2001, ¶53



EX1006, Fig. 1, *compare id. to* EX1401, Fig. 1.

V. Krantz in Combination with Herrmann Fails to Render the Challenged Claims Obvious

Petitioners' Ground 1 relies on Krantz alone as its base reference for several of the claimed limitations. The Petition, however, fails to account for key claim limitations that are expressly missing. Neither Krantz nor Herrmann teach "information" regarding an access device as distinct from authentication, nor do they teach "configuring the access point. " Further, the arguments for the motivation to combine isolated teachings from Herrmann with Krantz do not pass muster. Accordingly, institution must be denied.

A. The Use of Device "Information" and Device "Auditing" Distinct From Authentication Is Absent From Krantz and Herrmann

Krantz only discloses ***user*** authentication. Not ***device*** "information" and ***device*** "auditing." Yet, all Challenged Claims specifically each require at least one step pertaining to ***device*** auditing and using device "information," including (a) "collect[ing] information regarding the device," (b) "providing information to the access device," or (c) "performing an audit of the access device." Despite Petitioners' attempts to conflate authentication with device "information" and device "auditing," neither reference makes such a disclosure..

1. Krantz and Herrmann Fail To Disclose "Information" Regarding the Device As Claimed

The '450 Patent draws a clear distinction between user "authentication" and "information" regarding a device. Krantz fails to disclose any evaluation of the

device "information." Tellingly, Petitioners conflate the claimed "authentication" and device "information." For example, Petitioners rely on Krantz's "EAP-messages to pass certificates, keys, and supported cipher suites" for both the claimed "authentication" and device "information":

> Moreover, Krantz discloses that performing an "*authentication*" of the network device can include exchanging… **EAP-messages**…" Ex.1405, [0073], [0074] ("It may also be that **client 205 and server 215 exchange EAP-messages** to pass certificates, keys, and supported cipher suites…"); *see also*, Ex.1405, [0018],

Pet. at 65

> The Krantz gatekeeper may enforce/"*apply*" *security policies*, which can include "*one or more requirements pertaining to the authentication and the information*." For instance, "[i]t may also be that **client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites** ['*information*']. Depending on the EAP type, **other credential information may also be exchanged** between client 205 and server 215." Ex.1405, [0074]; Ex.1403, ¶109.

Pet. at 38

Authentication and device information are not the same thing. This is particularly the case, considering "authentication" and device "information" are

separate claim limitations. For example, independent claim 1 recites: "applying a security policy… including one or more requirements pertaining to the ***authentication and*** the ***information***." Petitioners' conflation would be render the claim meaningless. *See Willis*, 777 F. App'x at 498 ("Nothing in the claims suggests that 'inner void' and the 'channel void' can coexist as the same element.").

The '450 Patent explains that "information" regarding a device is data about the device's software and/or hardware that is necessary to comply with the security policy. EX1401, 11:48-59. The '450 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 '450 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…" EX1401, 1:38-40. Authentication is a different technical concept, process, and implementation—wholly distinct from the claimed "audit data pertaining to a device."

Yet, Krantz only discloses user authentication:

- "Krantz discloses . . . '**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 41 (quoting EX1405, [0076]) (certain alterations omitted).

- "If an **authenticated user** of client 205 is authorized to access resources…" EX1504, [0076] (cited in Pet. at 41).
- "Krantz discloses [that a] client [205] sends credentials to the server to attempt to **authenticate** with the server…" (Pet. at 28.)
- "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." EX1405, [0104] (cited in Pet. at 26).
- "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**) . . ." EX1405, [0019] (cited in Pet. at 18, 37, 59.)

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

Petitioners claim that Krantz discloses "scanning the device to collect information regarding the device" because "information is gathered, such as the operating system ***credentials of the device***." Pet. at 35.

This "credentials" argument fails immediately. First, the '450 Patent explains user authentication and "information" regarding the device are different. *Compare* EX1401, 1:38-42 (authentication) *to* 11:48-59 (audit data). Second, the Krantz "credentials" are the "user-identifier[s] and password[s]" which the '450 Patent expressly explains are for authentication; they are not device "information." *See* Pet. at 26; EX1401, 1:38-42. Indeed, a user may access different devices using the same username and password. Third, 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 a user is authenticated." Pet. at 90-91. Again, on its face, this is user data unrelated to the device information. EX2001, ¶¶ 56-59. Fourth, Petitioners claim "[c]redentials can include sending an Extensible Authentication Protocol ('EAP') Response/Identity message…" Pet. at 24 (cleaned up). EAP is for authentication. In fact, it is an acronym that stands for Extensible **Authentication** Protocol. EX1401, 8:38-39, 14:38-45. EX2001, ¶56 (citing EX1405, [0017]-[0019]).

Krantz's *user* authentication disclosures do not pass muster. Indeed, the '450 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* EX1401, 1:48-51.

Lastly, Petitioners try to justify their authentication and device information mix-and-match because "[a]uthenticating a user can be part of the audit[.]" Pet. at 25, n.4. This, however, is misdirection. First, the '450 Patent merely explains that **in addition to** conducting a security policy audit for a device, the authentication of the user can be conducted along with the same process. *See* EX1401, Fig. 4, 11:40-47. Nowhere does it say that device "information" can be used to replace authentication information. Second, the claim delineates "information" and

"authentication" as two separate elements. Lastly, the '450 Patent distinguishes between authenticating a user and the separate security evaluation for the device based on device "information":

> [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.**

EX1401, 13:66-67, 14:1-13 (ALL CAPS emphasis of "AND" in original).

Accordingly, Krantz fails to disclose or suggest this claim limitation.

The Petition relies on Herrmann only for an agent on a device. See Pet. at 35-37. Thus, Herrmann is not relevant to the device "information" limitation. Even if it were, Petitioners' application of Herrmann continues to conflate authentication with device "information" just as with Krantz. Petitioners argue:

- "A POSITA would recognize that checking for **anti-virus software** would simply be an additional item for **authentication module 217** (of server 215 to check in the already disclosed Krantz **authentication process**." Pet. at 14.
- "Krantz's **authentication module**, which compares credentials of a user against a database (e.g., user-identifier and password), as modified by Herrmann, would also check for **approved antivirus programs**." Pet. at 15.

- "Thus, Herrmann proposes **collecting information** from a client device to be used during the **authentication process** to enforce network security policies." Pet. at 10.

Authentication and device "information," however, are separate. *See, e.g.* '450, cl. 1 ("the security policy including one or more requirements pertaining to the authentication and the information."); cl. 16 ("providing information to the access device to improve compliance" and "authenticating a user of the access device").

Accordingly—even with Herrmann—Petitioners continue to conflate two different evaluations required in the Challenged Claims for two different features of the claimed system and fail to disclose this limitation.

2. Krantz And Herrmann Fail To Disclose "Performing An Audit Of The Access Device" Distinct from Authentication

As set forth above, Krantz only describes user authentication, not device "information." For those same reasons, Krantz also does not disclose "performing an audit of the access device." Indeed, the '450 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...", EX1401, 10:43-44.
>
> "Policy Auditor 325 collects further data to perform a security audit of Access Device 230 responsive to Security Policy 330A or Security Policy 330B." *Id.*, 11:49-51.

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

Petitioners argue that "Krantz explains network access may be controlled by 'configuration settings,' e.g. 'supported types of encryption' or 'supported types of authentication' including EAP." Pet. at 82 (quoting EX1405, [0066]-[0067]). This, however, does not suggest the "performing an audit of the access 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 (EX1405, [0066]-[0067]), the authentication only relates to user identification. EX2001, ¶¶ 56-59.

Similarly, Petitioners' reference to an EAP-Response/Identity message (Pet. at 83) or and EAP-MSChapV2 does not change this. Pet. at 82. Each of the EAP-Response/Identity message or and EAP-MSChapV2 message relates to user authentication.[1] Pet. at 81-82. But, the Challenged Claims require "performing an audit of the access device"– something different from Krantz's user identification. The '450 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

[1] *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).

> 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."**

EX1401, 13:64-67, 14:1-12.

Indeed, the known EAP or 802.1X user authentication mechanisms and associated credentials and specifies are distinct from "performing an audit of the access 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.

As for Herrmann, the Petition argues that "a network administrator may require all users access the network to implement a virus definition update…." (Pet. at 84). But even so, Herrmann conflates anti-virus software with the authentication module and process of Krantz which is not "auditing." *See* Pet. at 10 and 14-15.

B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Applying A Security Policy" Limitation (All Challenged Claims)

All Challenged Claims require "applying a security policy" which in turn includes: (i) "one or more requirements pertaining to the authentication and the information" or (ii) "performing an audit of the access device." But, Krantz only discloses authentication; not device "information." EX2001, ¶59.

Petitioners claim "A POSITA would recognize that checking for anti-virus software would ***simply*** be an additional item for authentication module 217 (of server 215 to check in the . . . Krantz['s] authentication process…" Pet. at 14. This is unsupported. Indeed, intrinsic evidence says there would be nothing "simple" about it:

> 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.

EX1401, 14:10-12.

The patent then explains the technical infrastructure and how to do this complicated process of both auditing and authentication. *See, e.g.*, EX1401, 14:53-65 ("The ECL calls the corresponding CF to perform authentication… If the SF receives a success response from the server EAPM… the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specifically formatted audit requests to the ESL…"). None of this is

suggested by Krantz or Herrmann, and this is clearly not simply a matter of "merely be an additional item" to add to the authentication process.

Notwithstanding the patent's explanation that such a combination "is complicated and not an obvious variation," Petitioners argue a POSITA would have modified Krantz because it is "focus[ed] on network authentication/security." Pet. at 40 (citing to EX1405 (Abstract) and EX1403, ¶114 (Houh Decl.). Krantz's Abstract, like the rest of Krantz, is limited to authentication, and includes nothing about device auditing. EX2001, ¶¶49, 56-59. And the Houh testimony is merely conclusion. The lack of any recognition in Krantz of security policy compliance by a device further demonstrates the argument to merely be impermissible hindsight. *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068 (Fed. Cir. 2018) (cautioning that hindsight "often overlooks that the genius of invention is often a combination of known elements which in hindsight seem preordained" and disparages looking to "what a skilled artisan would have been ***able*** to do, rather than what a skilled artisan would have been ***motivated*** to at the time of the invention.") (emphasis in original, internal quotations and citations omitted).

Petitioners' other motivation argument is that the "two stated goals of Krantz involve automation and security." Pet. at 37 (citing EX1405, [0014] and [0019]). Paragraph [0014] merely states it would be advantageous to increase "the level of automation when provisioning and configuring a computer system to access a

network." Automation has no bearing on whether a POSITA would incorporate an agent on a device for function related to audit data pertaining to the device. *See* EX2001, ¶49. The lack of any recognition in Krantz of security policy compliance by a device demonstrates the argument to merely be impermissible hindsight. See *Polaris*, 882 F.3d at 1068.

Krantz lacks any recognition of a "security policy" that includes device "information" or "auditing." Such a conspicuous absence highlights the smoke and mirrors of the Petition's reliance on Krantz's paragraph [0019] and purported goal of "security." Krantz's goal of "security" only relates to user authentication and does not provide a reason to incorporate the agent for retrieving audit data pertaining to a device for security policy compliance evaluation of the device software and hardware. EX2001, ¶¶49, 57-59.

With regard to the claimed "applying a security policy" step, Petitioners argue it would have been obvious to combine Herrmann and Krantz because "Herrmann's server components are like Krantz's gatekeeper…" Pet. at 44. Even if this were true (it is not), Petitioners cite to no authority for the proposition that motivation to combine is present because two references have similar computer components. In fact, the intrinsic evidence demonstrates otherwise in that the combination of auditing and authentication is "complicated" (EX1401, 14:11-13) and sets forth a detailed description of the components and process used address this "complicated"

(EX1401, 14:11-13) combination of auditing and authentication. EX1401, 14:14-67.

C. Krantz and Herrmann Fail to Disclose "Configuring The Access Point" Limitation

The '450 Patent claims require "configuring the access point." The specification explains that: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1401, 3:30-33. Thus, there are changing pathway assignments for the ports of *the "access point*."

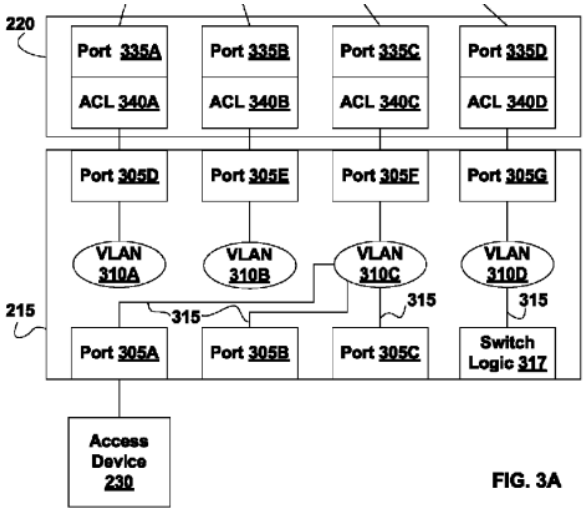


FIG. 3A

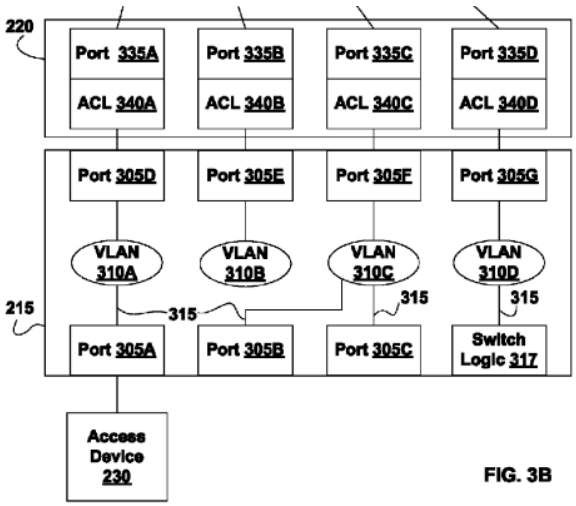


FIG. 3B

> 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.

EX1401, 8:4-12.

> 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.

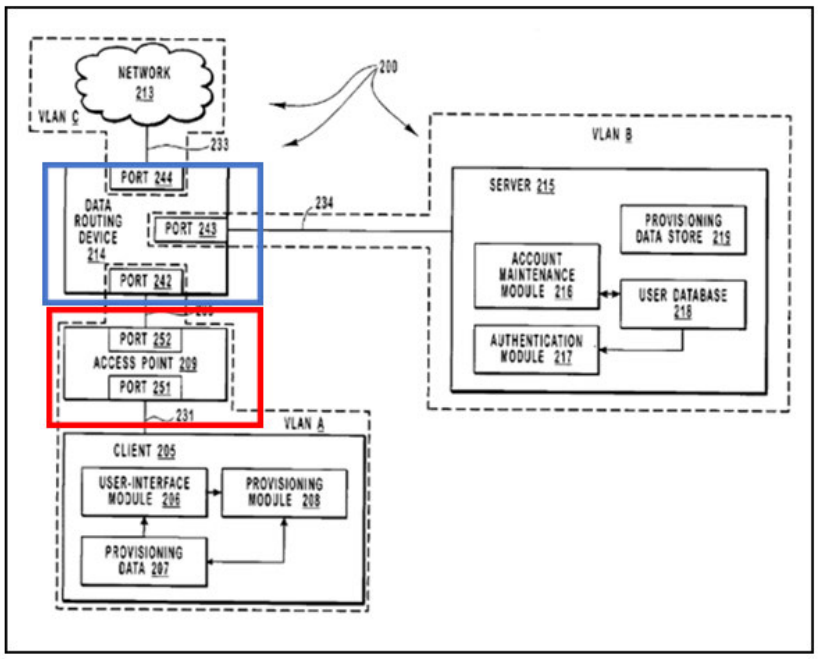
EX1401, 8:25–32.

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

Petitioners' Mapping #1:

Petitioners' first argument for how Krantz supposedly discloses “configuring the access point” requires one to ignore what Krantz actually discloses. Petitioners argue that the access point is configured because it was previously configured to only transfer data to VLAN B but then transfers data to VLAN C. Pet. at 47-48. This, however, does not support making any changes to the Krantz access point 209.

In fact, as shown below, the Krantz access point 209 is only part of VLAN A and not even part of, or in direct communication, with VLAN B or VLAN C.



The ‘450 Patent is clear: “[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1401, 3:30-33.

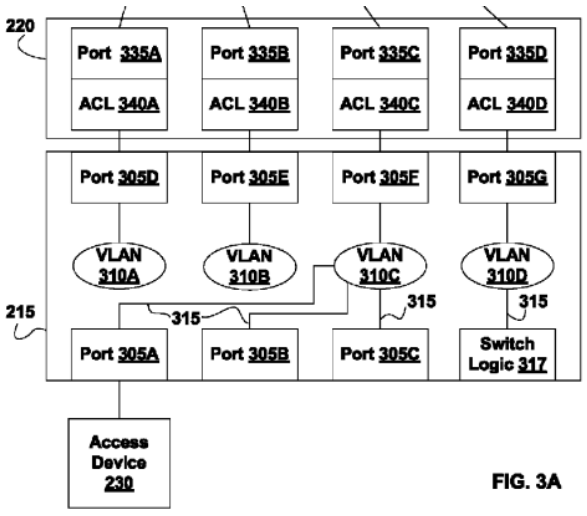


FIG. 3A

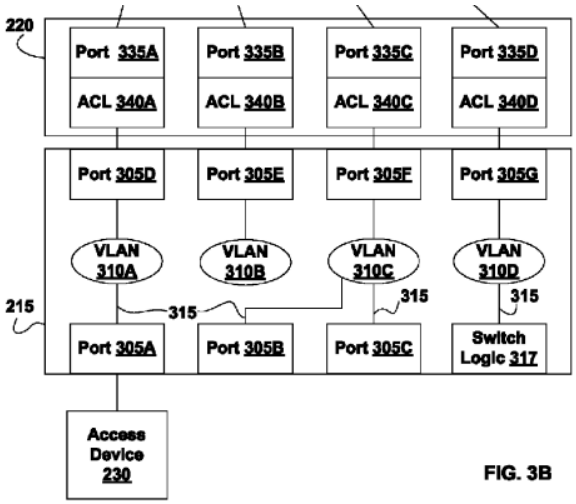


FIG. 3B

This means that depending on the “configuring” the same port may send data to different locations. For example, as shown in FIG. 3A of the '450 Patent above,

port 305A of access point 215 sends data to VLAN 310C (as denoted by line 315). In FIG. 3B, however, that same port 305A has been "reconfigured" to send data to VLAN 310A.

Krantz has no "configuring." Instead, the Krantz 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 to direct users either to VLAN B or VLAN C. EX1405, [0060]; EX2001, ¶¶49, 63. And even then there is no configuring of the data routing device 214. Rather, the data routing device 214 reads "tag headers" that are inserted into client data (EX2001, ¶63) or uses "IP filtering" (*id.*) to direct traffic. Neither of these demonstrate a change or "configuring" of the access point 209 (or data routing device) disclosed in Krantz. EX2001, ¶53. As such, Mapping #1 fails.

Petitioners' Mapping #2:

Petitioners' second argument avoids any action on the "access point" altogether. Rather, they assert that "[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 … that are [then] transferred to VLAN B or VLAN C." EX1405, [0064]) (cited in Pet. at 49). The Krantz "tag headers" are different from the claimed "configuring the access point."

Recognizing this deficiency, Petitioners try to combine Krantz with three additional references in an attempt to transform "tag headers" into "configuring the access point." *See* Pet. at 28-29 (§ VIII.A.1.iv) (citing Exs. 1407, 1408, 1409, and 1410). None of these references, however, save Krantz from the fact that its clear disclosure is that the tag header is inserted into "data from client 205:"

> 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.

EX1405, [0061].

Indeed, nothing in the access point 209 is being configured. Rather, it is the *access point* causing the action itself to insert the Tag Header to client data. It is this, not any configuring of the access point, which enables a message from a client to be directed by the data routing device 214 (the gatekeeper) to VLAN C, instead of VLAN B. What is missing, however, is **any** change to the access point 209.

Accordingly, Mapping #2 fails.

Petitioners' Mapping #3:

Petitioner's third argument appears to be that it would have been obvious for one to take the access point 209 and the data routing device 214 and combine these so that the Tag Headers can be configured to either be directed to VLAN C or VLAN B. There are numerous flaws with such an argument.

As discussed, inserting tag headers into client data – whether by the access point 209 or data routing service 214—is not “configuring the access point.” Rather, it is only manipulating "data from client 205." As such, the different data paths of Krantz still require the data routing device to check user identification information, namely, the tag header.

Even if "tag headers" could be configuring, Krantz expressly recites separate access point 209 and data routing device 214. Arbitrarily combining these separate and distinct component finds no support in Krantz. To the contrary, Petitioners' own cited portions of Krantz expressly teaches access point 209 and a different component data routing device 214. EX1405, [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 further confirms that any change is to user identification data, not to an access point as claimed, because

"EAP-Response/Identity messages" expressly relate to user authentication.[2] 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. *See* EX1405, [0060].

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 Standard

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).

---

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

To antedate a reference, one must show 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. *See, 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).

For reasonable continuous diligence, an inventor need not work on reducing the invention to practice every day, and periods of inactivity 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. *Perfect Surgical*, 841 F.3d at 1007. The "rule of reason" analysis governs whether corroboration is sufficient. *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 (quotation omitted). 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.*

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

Petitioner asserts Krantz has an effective date of December 6, 2002 (Pet. at 7) and Herrmann has an effective date of March 13, 2003.[3] *Id*. at 10. InfoExpress conceived of the claimed invention before that.

On November 14, 2002, 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. EX2012; EX2003 (Lum Declaration), ¶ 12. This conception is demonstrated in the claim chart mapping by Dr. Smith

[3] 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*, 584 U.S. 357, 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.

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 was diligently working.



This was groundbreaking because preexisting security technologies did not include the implementation of auditing support functionality over authentication protocols such as 802.1x. The InfoExpress team diligently worked in October 2002 and November 2002 to produce the LAN Engineering Specification of November 14, 2002. EX2021; EX2056; EX2061; EX2273; EX2274; EX2275; EX2342.

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 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:

i. emails (e.g., EX2015-EX2065; EX2067; EX2068; EX2071; EX2074-EX2200; EX2202-EX2271; EX2273; EX2274; EX2276-EX2283; EX2285; EX2287-EX2326; EX2331-EX2340; EX2342-EX2382; EX2384-EX2390; EX2395-EX2397; EX2399-EX2410);

ii. technical specifications and analyses (e.g., EX2011-EX2014; EX2066; EX2069; EX2070; EX2072; EX2073; EX2201; EX2275; EX2329; EX2330);

iii. source code (e.g., EX2113; EX2114; EX2121; EX2129; EX2138; EX2178; EX2191; EX2197; EX2206; EX2298; EX2303; EX2314; EX2339; EX2348; EX2352; EX2359; EX2364; EX2384; EX2399; EX2404; EX2405); and

iv. the inventor declaration of InfoExpress CEO Stacey Lum (EX2003). .

As further detailed in the diligence calendar submitted herewith (EX2004), 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 (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]
- See EX2003, ¶¶6-7, 30, 33, 37, 49 (Lum Declaration).

January 2003:

- [redacted]
- [redacted]
- [redacted]

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

May 2003:

- [redacted]

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

June 2003:

- See EX2003, ¶53 (Lum Declaration).

July 2003:

- *See* EX2003, ¶¶52, 59-61 (Lum Declaration).

August 2003:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- *See* EX2003, ¶52 (Lum Declaration).

<u>September 2003</u>:

- [redacted]
- [redacted]
- [redacted]

- [redacted]

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

October 2003:

- [redacted]

- *See* EX2003, ¶¶14, 23, 25, 64-66 (Lum Declaration).

D. The Inventors Achieved a Constructive Reduction to Practice by the Filing of U.S. Provisional Patent Application Serial No. 60/513,080, Which Was Filed on October 21, 2003

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: July 25, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	*/s/ Brian R. Michalek* 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@saul.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@saul.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saul.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 13,494 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: July 25, 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: July 25, 2024

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