

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.

IPR2024-00677
U.S. Patent No. 8,578,444

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. Introduction.....	1
II. The '444 Patent	1
A. Date of Invention.....	1
B. Person of Ordinary Skill in the Art (POSITA)	1
C. Overview of the '444 Patent	2
III. Claim Construction.....	6
IV. Petitioners' References.....	6
A. Krantz	6
B. Herrmann.....	9
V. Krantz In Combination with Herrmann Fails to Render Obvious the Challenged Claims.....	11
A. Neither Krantz Nor Herrmann Disclose "Applying A Security Policy That Includes At Least One Requirements Pertaining To The Audit Data And At Least One Requirement Pertaining To Authentication" (All Challenged Claims).....	12
1. Krantz.....	12
2. Herrmann	17
B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Security Policy ... Pertaining to Audit Data" Limitation (All Challenged Claims).....	18
C. Neither Krantz Nor Herrmann Disclose "Applying The Security Policy Includes Configuring The Access Point (Claims 2-7 and 22).....	21
D. Claims 5-7 Are Not Obvious In View of Krantz With Herrmann.....	28
E. Claim 22 Is Not Obvious In View of Krantz In Combination With Herrmann.....	29
VI. All Grounds: Neither Reference Constitutes Prior Art	29
A. Legal Standard.....	30
B. The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....	31

C.	The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.	33
D.	The inventors exercised achieved a constructive reduction to practice by the filing of U.S. Provisional Patent Application Serial No. 60/513,080 was filed on October 21, 2003.....	42
VII.	Conclusion	42

TABLE OF AUTHORITIES

FEDERAL CASES

<i>ATI Techs. v. Iancu</i> , 920 F.3d 1362 (Fed. Cir. 2019)	30, 34, 42
<i>Bey v. Kollonitsch</i> , 806 F.2d 1024 (Fed. Cir. 1986)	30
<i>Monsanto Co. v. Mycogen Plant Sci., Inc.</i> , 261 F.3d 1356 (Fed. Cir. 2001)	30, 34
<i>Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.</i> , 841 F.3d 1004 (Fed. Cir. 2016)	30, 31
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	19, 20, 27
<i>SAS Institute Inc. v. Iancu</i> , 138 S.Ct. 1348 (2018)	31

FEDERAL STATUTES

37 C.F.R. § 42.6(d)	44
37 C.F.R. § 42.6(e)(4)	45
37 C.F.R. § 42.24(b)	44
37 C.F.R. § 42.24(b)(1)	44
35 U.S.C. § 102(e)	30, 31
35 U.S.C. §§ 119(e) & 112, ¶ 1	42

STATE STATUTES

ECL	18
-----------	----

OTHER AUTHORITIES

<i>Globus Med., Inc. v. Depuy Synthes Prods., LLC</i> , No. IPR2015-00107 (P.T.A.B. May 1, 2015)	31
, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm	27, 28

https://www.portnox.com/cybersecurity-101/mschapv2/	28
<i>LG Elecs., Inc. v. Wi-LAN Inc.</i> , No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018)	29
Petitioners' “Tag Headers”	25
report on February 10, 2003. EX2075	36
<i>Sequenom v. Leland Stanford Junior Univ.</i> , No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014)	30
U.S. Patent 8,578,444	passim

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 '444 Patent
2010	Constructive Reduction to Practice of the '444 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 related to claims 1-7, 10, 12, 17, and 22 (the "Challenged Claims") of U.S. Patent 8,578,444 (the '444 Patent'). The Board should reject the Petition and not institute an IPR because the Grounds and the art relied upon fail to render any of the Challenged Claims unpatentable. The art fails to render obvious all of the limitations of the Challenged Claims, and a POSITA would not have been motivated to combine the references as argued by Petitioners. Moreover, the art relied on does not qualify as prior art.

II. The '444 Patent

A. Date of Invention

For the reasons discussed in Section VII below, 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 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 '444 Patent

The '444 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. EX1201, Fig. 1, 2:39-47; EX2001, ¶¶ 44-46. But as the '444 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. EX1201, 2:34-45.

Exemplary prior art architecture is shown in annotated FIG. 1.

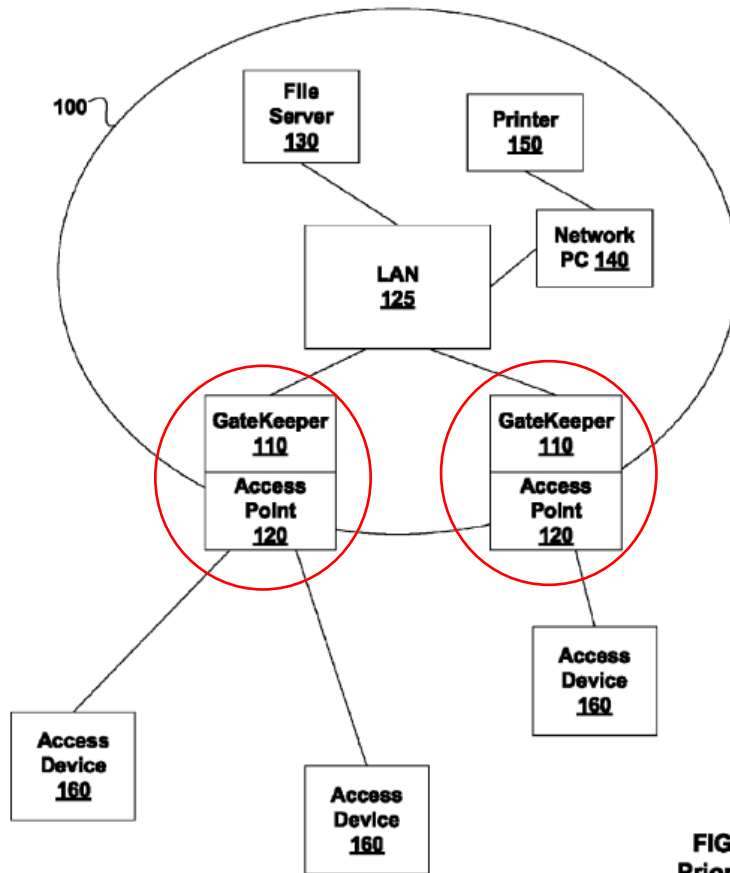


FIG. 1
Prior Art

The network 100 included two Gatekeepers 110, each associated with a different Access Point 120. With 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." EX1201, 2:39-42. The gatekeeper then becomes a limiting bottleneck on the system's bandwidth. *Id.*, 2:42-45.

The '444 Patent addressed this previously unidentified problem with a new approach, relieving computer resources through configuring an access point after clearing a device as authorized and satisfying security policies to access the

computer network. A disclosed example shows a protected network including a restricted subset with a gatekeeper and one or more less-restricted subsets.

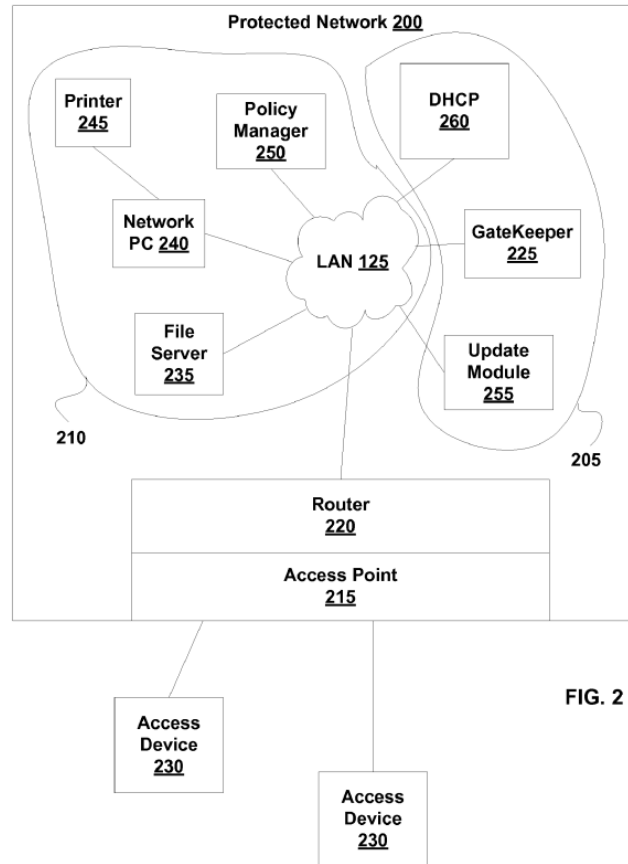
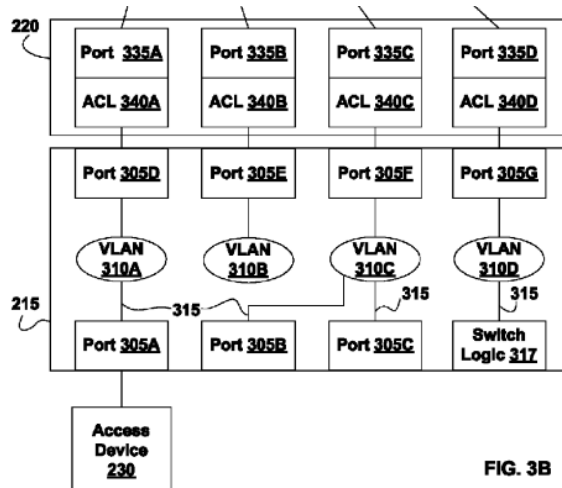
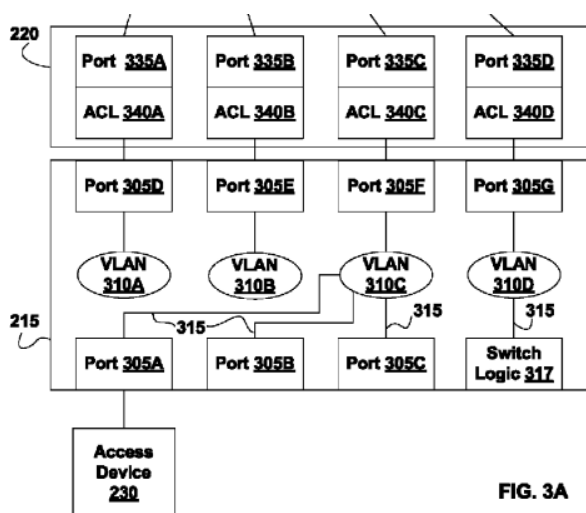


FIG. 2

EX1201, Fig. 2. Before a device can access a less-restricted subset 210, its request is first passed to the restricted subset (205). EX1201, 2:58-60, 5:38-40. A gatekeeper in the restricted subset checks whether the device is authentic (it is what it purports to be) and satisfies security policies. If so, the device is granted access to a less-restricted subset of the protected network. EX1201, 2:60-64. Regarding security policies, the patent teaches an agent on the device to receive requests for and to send audit data pertaining to the device so the gatekeeper can apply the security policy to

the device. See, EX1201, 11:60-61 ("Obtain Audit Data Step 450 is facilitated by an agent running on Access Device 230.")

Another feature of the patent is that rather than require all device access requests to pass through the gatekeeper (a previously unidentified shortcoming), the access point itself is configured based on user authentication and device compliance with security policies. The Detailed Description explains this.



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.

EX1201, 8:25-32.

By configuring the access point after qualifying the access device for authentication and device security policy compliance, the device access the less-restricted subset

without going through the gatekeeper. Thus, substantial network traffic does not need to pass through the gatekeeper.

III. Claim Construction

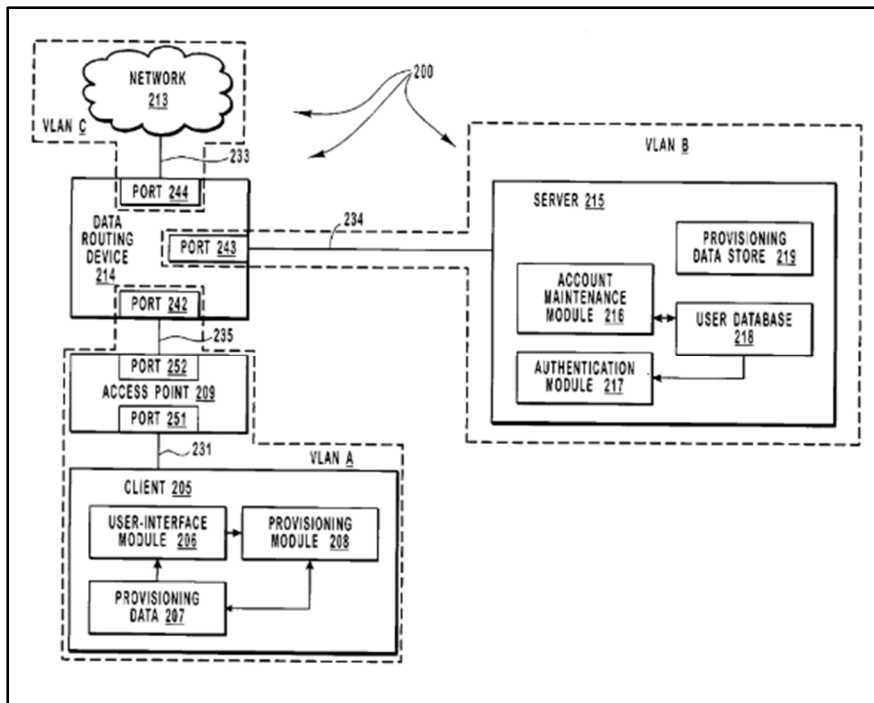
Petitioners assert claims should be given their ordinary and customary meaning as understood by a POSITA, and contends the Board need not expressly construe the claim terms. Pet. at 7. Patent Owner contends the claims should be given their plain meaning in the context of the intrinsic evidence, which is explained below in the context of the purported prior art.

IV. Petitioners' References

Petitioners' references, Krantz and Herrmann, are not prior art (discussed herein). Krantz and Herrmann are also different from the Challenged Claims, and merely illustrate network security approaches improved upon by the patent.

A. Krantz

Petitioners' primary reference is Krantz which details “[a] computer system attempts to authenticate with a server to gain authorization to access a first network.” EX1205, Abstract.



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.

EX1205, [0016].

Regarding authentication of clients so as to access a network, Krantz teaches:

In these embodiments, the server (based at least in part on received credentials) may authorize the client for at least partial access to the single network, such as, for example, by authorizing client access to selected computer systems or modules on the single network.

Sending credentials can include sending an Extensible Authentication Protocol ("EAP") Response/Identity message from the client to the server. If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point. In VLAN embodiments, the access point can insert a Tag Header into the encapsulating message to indicate to a data routing device that the encapsulating message is to be transferred to the first network. The access point may also be configured to block communications from the client that use protocols other than EAP and 802.1X.

When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.

EX1205, [0017]-[0018], [0076]. As Krantz explains, authentication merely checks whether the identification credentials match those in a database. Absent from Krantz is any discussion of auditing the device for compliance with security policy for the device. EX2001, ¶¶49, 58. Also absent is an agent on the device to receive requests for device information to be provided to a gatekeeper.

Figure 1 is a network architecture diagram. At the top, a **DATA ROUTING DEVICE 214** is shown with three ports: **PORT 244**, **PORT 243**, and **PORT 242**. **PORT 244** is connected to a network labeled **200**. **PORT 243** is connected to a network labeled **234**. **PORT 242** is connected to **PORT 252** of the **ACCESS POINT 209** via a link labeled **235**. The **ACCESS POINT 209** also has **PORT 251**, which is connected to the **CLIENT 205** via a link labeled **231**. The **CLIENT 205** is enclosed in a dashed box labeled **VLAN A**. Inside the client, there are three modules: **USER-INTERFACE MODULE 206**, **PROVISIONING MODULE 208**, and **PROVISIONING DATA 207**. Arrows indicate data flow: from **PROVISIONING DATA 207** to **USER-INTERFACE MODULE 206**, from **USER-INTERFACE MODULE 206** to **PROVISIONING MODULE 208**, and from **PROVISIONING MODULE 208** back to **PROVISIONING DATA 207**.

Krantz does not teach configuring any port of the access point 209 after applying a security policy to a device's audit data. EX2001, ¶¶57-58. Instead, all data pass ports 251 and 252 and then pass to the data routing device.

Petitioners cite to Herrmann in Ground 2 in combination with Krantz.

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.

EX1206, Abstract; EX2001, ¶¶51-53. Petitioners rely on Herrmann for an agent on a device to determine compliance of the device's software, e.g., virus software. Like the prior art discussed in the '444 Patent, Herrmann utilizes servers between the client and the protected network such that all attempts to access the network are first checked for device-based security policy compliance by at least a Network Access Server (NAS), and face bottleneck problems. EX2001, ¶¶53, 60.

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

The Petition fails to show how either reference—alone or in combination—meets several "security policy" limitations requiring both "audit data" and "authentication."

Further, the arguments for the motivation to combine isolated teachings from Herrmann with Krantz do not pass muster. Accordingly, institution should be denied

A. Neither Krantz Nor Herrmann Disclose "Applying A Security Policy That Includes At Least One Requirements Pertaining To The Audit Data And At Least One Requirement Pertaining To Authentication" (All Challenged Claims)

The Challenged Claims recite "applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to authentication...." This limitation clearly distinguishes between "audit data" and "authentication." Yet, the Petition fails to show any single reference where a "security policy" includes both "audit data" and "authentication."

1. Krantz

Krantz teaches authentication, but not "audit data." Petitioners improperly conflate "audit data" and "authentication" to mean the same thing. Here, Petitioners assert Krantz's "user-identifier[s] and password[s]" are both "audit data" and "authentication."

message that can be transferred through the access point.” Ex.1205, [0018]. Other “audit data” provided by Krantz’s “device” may include, for example, “user-identifier[s] and password[s].” Ex.1205, [0076]. Krantz further explains that

Pet. at 21

Krantz discloses:

When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials [*“apply[ing] a security policy”*] to entries in **user database** 218. If credential information matches ... **the identity of a user is authenticated** (server 215 believes that the user represented by the user-identifier is the user who entered the credential information) [*“that includes at least on requirement pertaining to authentication”*]. If an

Pet. at 59

But this would render the claim meaningless.¹

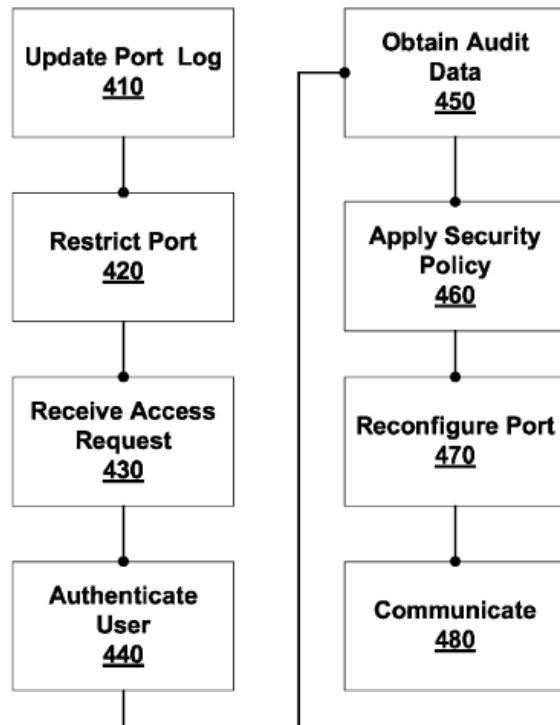
The patent explains that "audit data pertaining to a device" is data about the device's software and/or hardware necessary to comply with the security policy.

¹ Despite the distinction between authentication and audit data, Petitioners mix and match authentication and audit data throughout their Petition. In particular, for the limitation "sending a request for audit data to an agent running on the device," the Petition incorporates the discussion related to element [1.1] directed to "performing an authentication." Pet. at 31 ("As discussed for claim [1.1], Krantz discloses a method for 'auditing a device.'")

EX1201, 11:48-59. The '444 Patent further provides examples of types of "audit data pertaining to a device" 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.*

Authentication is different. The patent describes "authentication" as identifying or authorization information, e.g., "requiring the user to enter a username and password..." *Id.*, 1:39-40. Authentication is different from the claimed "audit data pertaining to a device." Indeed, the claims recite authentication and auditing separately. *See e.g.* Claim 1 ("... performing an authentication using an EAP protocol" and "receiving the audit data... the audit data pertaining to the device...").

Fig. 4 further establishes authentication ("Authenticate User 440") and audit data ("Obtain Audit Data 450") are distinct elements.



EX1201, Fig. 4

Yet, Krantz only discloses user authentication:

- "Krantz discloses 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 55 (citing EX1205, [0076]).
- "If an **authenticated user** of client 205 is authorized to access resources..." EX1205, [0076] (cited in Pet. at 55).
- "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." Pet. at 40-41 (citing EX1205, [0104]).
- "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**) . . ." EX1205, [0019].

Further, the Petition relies on purported disclosures from Krantz that pertain only to authentication. EX2001, ¶49; *see also* Pet. § VIII.A.1.ii. For example, Petitioners argue:

[S]ending credentials can include sending an Extensible Authentication Protocol ("EAP") Response/Identity message from the client to the servers ['performing an authentication using an EAP protocol from the device'].

Pet. at 24-25 (quoting EX1205, [0018]) (quotation marks and emphasis omitted).

The Petition further references Krantz's disclosures of "EAP-messages," "EAP-Response/Identity message within an EAP-RADIUS message," "EAP-MSChap V2," and "EAP-TLS and EAP-MSCHAP V2." Pet. at 26-28. Again, these disclosures are only for authentication. *See* EX2001, ¶¶55-56.

Krantz's authentication disclosures do not pass muster. Indeed, the patent explains there are disadvantages to "reliance on mere user authentication" including the lack of any assurance that the device meets network security policies. *See* EX1201, 1:48-51.

Because Krantz does not disclose "audit data pertaining to a device," it also fails to disclose many of the other limitations of the Challenged Claims including: "A method of auditing a device" (all claims); "sending a request for audit data to an agent...." (all claims), "receiving the audit data..." (all claims).

2. Herrmann

The Petition relies on Herrmann only for an agent on a device. See Pet. at 50. Thus, it is not relevant to the "applying a security policy" limitation. Even if it was, Petitioners application of Herrmann continues to conflate authentication and auditing just like in 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 authentication process..." Pet. at 14.
- A POSITA would have understood that checking for anti-virus software would merely be an additional item for server 215 ("*gatekeeper*") to check in the authentication process..." Pet. at 43.
- "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, Petitioners claim Herrmann's supposed "audit data" would be evaluated through Krantz "authentication process"; not the audit process which is a separate claim element.

The claims, however, require "applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to authentication." Thus—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.

B. There Is No Motivation To Combine Krantz With Herrmann To Meet The "Security Policy ... Pertaining to Audit Data" Limitation (All Challenged Claims)

The claims require: "a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication... " But, Krantz only discloses authentication; not audit data. EX2001, ¶59. Further, the Petition only relies on Herrmann for a combination reference that runs an agent on a device. Pet. at 50.

Petitioners claim "[a] POSITA would have understood that checking for anti-virus software would merely be an additional item for server 215 (*"gatekeeper"*) to check in the authentication process..." Pet. at 43. The intrinsic evidence says otherwise:

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.

EX1201, 14:11-13.

This is aligned with the claims which recite "performing an authentication using an EAP protocol... to an access point configured to use an 802.1x protocol." The patent then explains how to do this complicated process. *See, e.g.*, EX1201, 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 "focused on network authentication and security." Pet. at 82 (citing to EX1205 (Abstract)). Krantz's Abstract, like the rest of Krantz, is limited to authentication, and includes nothing about device auditing. EX2001, ¶¶49, 57-59. 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).

Further, the Petition argues motivation to combine on the claim that the "two stated goals of Krantz involve automation and security." Pet. at 35 (citing Krantz paragraphs [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.

This lack of any recognition in Krantz to a "security policy" that includes "audit data" 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.

In addition, the Petition incorrectly asserts a "POSITA would have understood checking for anti-virus software would merely be an additional item for server 215 ('gatekeeper') to check in the authentication process disclosed by Krantz." Pet at 43. The Petition argues that a POSITA would have arrived at this supposed understanding because "Krantz is focused on network authentication/security." Pet. at 43. Again, Krantz is unrelated to device compliance with a security policies like virus protection. EX2001, ¶¶49, 57-59. Instead, Krantz's authentication relates only to determining whether the user or user's device has the necessary credentials, *i.e.*, whether the user is authorized to access the network such as through being a

subscriber. EX1205, [0016] ("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."); EX2001, ¶¶49, 57-59. Without any recognition of any evaluation of an access device other than authorization a POSITA would have not been motivated to combine Herrmann's checking for a virus-protection program with Krantz. EX2001, ¶¶49, 57-59.

With regard to the "applying step," Petitioners argue it would have been obvious to "implement 'applying of the security policy taking place under control of the gatekeeper' as described *supra* with respect to Herrmann, in the gatekeeper of Krantz" because the "server components in Herrmann are similar to the gatekeeper of Krantz." Pet. at 57. Even if this was 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. All computers have similar components, and mere commonality is not sufficient to establish motivation.

C. Neither Krantz Nor Herrmann Disclose "Applying The Security Policy Includes Configuring The Access Point (Claims 2-7 and 22)

Independent claim 22 and claims 2-7 of recite: "applying the security policy includes configuring the access point." As discussed with claim 1, these claims are

also not obvious in view of Krantz and Herrmann since neither teach "applying the security policy includes configuring the access point."

The patent explains: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less restricted VLAN." EX1201, 3:30-33. Thus, there are changing pathway assignments for the ports of *the access point*. The specification explains: "[t]he passing of access requests to the restricted subset and granting of access are accomplished by configuring and reconfiguring a communication port of an access point." EX1201, 2:64-67.

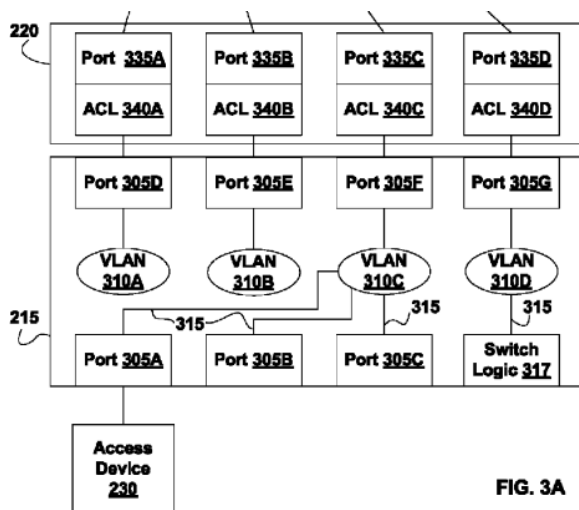


FIG. 3A

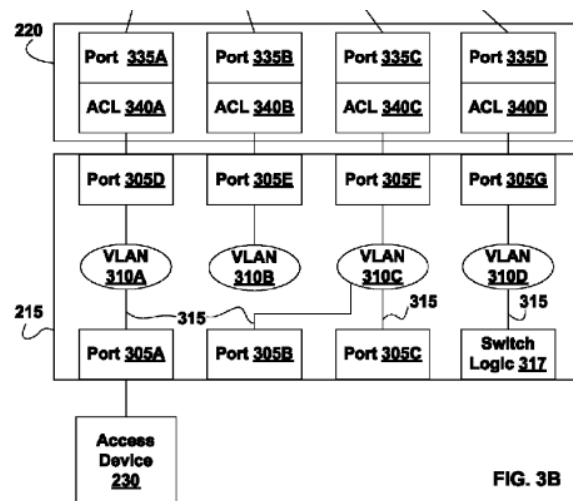


FIG. 3B

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.

EX1201, 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.

Id., 8:28-32.

As shown, an access point's port is configured to change connections. Petitioners make several arguments for how Krantz discloses "configuring the access point."

None work.

Petitioners broadly suggest Krantz configures an access point because a user device originally directed to VLAN B is directed to VLAN C. Pet. at 62-63. But according to the annotated figure at page 62 of the Petition, the "access point 209" is never configured as part of applying a security policy. Instead, the access point 209 always transfers data from "client 205" via "port 251" to "data routing device 214" via "port 252," including before and after authentication.

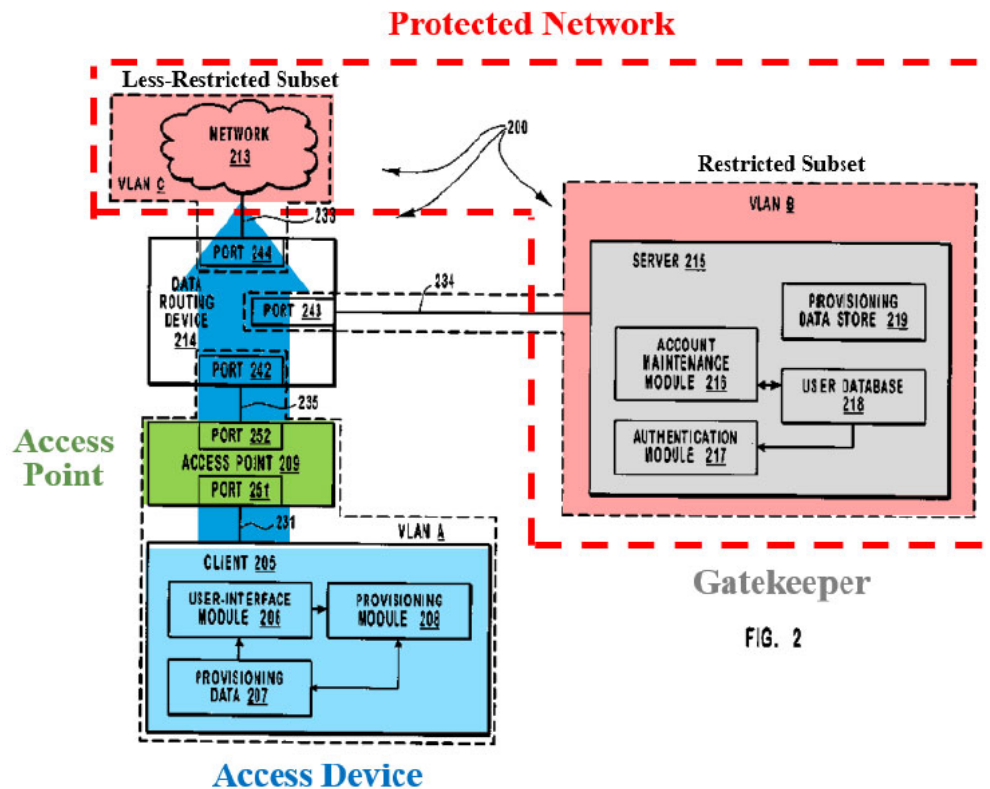


FIG. 2

Pet. at 62.

There is no configuration of access point 209 at all.

The patent is clear: "management of Access Point 215 is accomplished by configuring and reconfiguring one or more communication ports within Access Point 215...." EX1201, 7:6-7.

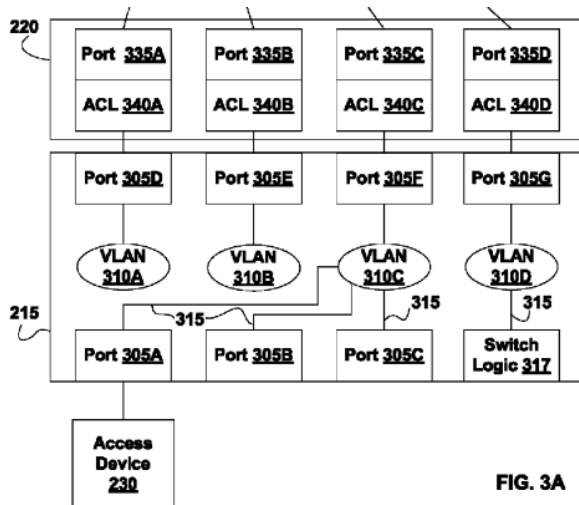


FIG. 3A

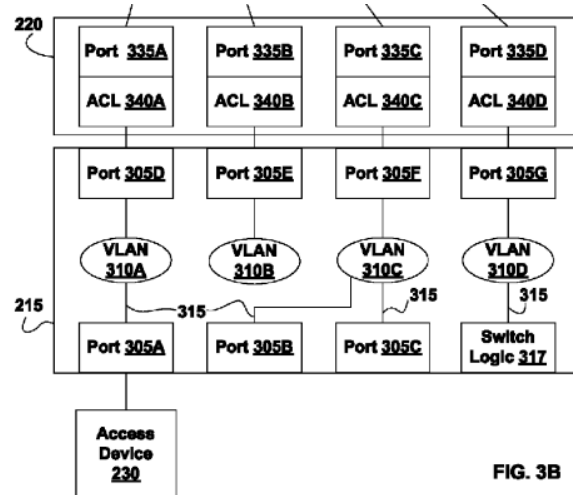


FIG. 3B

This means the access device's port is configured to send data to a particular network depending on the security policy application. As shown in FIG. 3A, port 305A of the access point 215 sends data to VLAN 310C (as shown by line 315). In FIG. 3B, however, that same port 305A has been "configured" to send data to VLAN 310A due to application of the security policy. By contrast, as shown above, Krantz discloses no configuring of access point 209 at all, let alone as part of applying a security policy.

Petitioners argue "Krantz explains that '[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 that are to be transferred to VLAN B and/or VLAN C.'" Pet. at 62 (citing EX1205, [0023], [0061] and [0064]). Petitioners' "Tag Headers" argument fails.

The claim requires configuring the access point, not the client data. Yet, the Petition contends Tag Headers are inserted "*into data frames received from client 205 that are to be transferred to VLAN B and/or VLAN C.*" *Id.* (emphasis supplied).

Data frames in client data are like the address an envelope. *See* EX1201, ¶61. Adding a header to an envelope, such as "Attn: John Doe," is simply different from configuring the access point. Krantz's "data routing device 214" directs the traffic to either the VLAN B or VLAN C based on consideration of the user's identification information.

Data routing device 214 can process the inserted Tag Header and transfer the EAPOL packet onto VLAN B. Server 215 can receive the EAPOL packet, which is transferred to authentication module 217 for authentication. ... When credentials are sent to server 215, authentication module 217 can receive the credentials (e.g., user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of a user is authenticated (i.e., server 215 believes that the user represented by the user-identifier is the user who entered the credential information). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.

EX1205, [0073]-[0076]. There is no configuring of the access point 209. EX2001, ¶59.

Alternatively Petitioners argue if Krantz does not expressly disclose "wherein applying the security policy includes configuring the access point," it would have been obvious to implement the Data Routing Device disclosure of Krantz within the Access Point 209 itself." Pet. at 66. As discussed, configuring client data with tag headers is not configuring of the access point. Rather, it is only manipulating "data from client 205."

Even if "tag headers" could be considered to be configuring of access point, Krantz separately describes access point 209 and data routing device 214. Arbitrarily combining these distinct components 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. EX1205, [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.")²

Lastly, Petitioners argue Krantz's data routing device and access point have the same functionality, and therefore, a POSITA would have combined them. Such speculation is without logic. Krantz's data routing device determines where data goes based on fields in the client data. EX1205, [0059]. An access point is, as the name suggests, a device through which data passes. As such, Krantz itself explains the components have different functions. Petitioners' reliance on its expert to make this leap amounts to nothing more than impermissible hindsight. *Polaris*, 882 F.3d at 1068.

² Notably, EAP-Response/Identity relates only to authentication. See, https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048062.htm.

D. Claims 5-7 Are Not Obvious In View of Krantz With Herrmann

Claims 5-7 (depending from claim 1) include limitations related to updated audit data. For at least the reasons discussed, Krantz's failure to disclose anything about audit data pertaining to a device means the challenge to claims 5-7 must fail.

Just like Krantz failed to disclose device "audit data," it also fails to disclose "receiving, from the agent, updated audit data pertaining to the device" as required by claims 5-7. Petitioners' attempt to transform user authentication into "updated audit data pertaining to the device" (Pet. at 77-81) only demonstrate why such contortion does not work. Petitioners claims a subscription paid for by a user can expire, and Krantz provides for checking of the user's subscription. *Id.* 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.³ But, the claim requires that the audit data relates to the device and a security policy – something different from Krantz. EX2001, ¶¶56-59.

³ 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).

E. Claim 22 Is Not Obvious In View of Krantz In Combination With Herrmann

Claim 22 is an independent claim, but shares many of the limitations from claim 1. In addition, claim 22 includes the requirement of receiving, from the agent, updated audit data pertaining to the device while the device has access to a less-restricted subset of the network. This limitation is also found in claim 6. For the reasons discussed previously with respect to claims 1 and 6, Krantz in combination with Herrmann fails to render claim 22 unpatentable as obvious.

Claim 22 further requires re-auditing of the device based on the received updated audit data. Petitioners argue that this limitation is met by "submitting appropriate credentials to server 215." Pet. at 88. Again, user credentials are not audit data pertaining to a device. Therefore, Petitioners' unpatentability arguments for claim 22 must fail for failure to disclose this re-auditing limitation as well.

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).

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. *E.g., ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019).

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, 2003.⁴ *Id.* at 10. InfoExpress conceived of the claimed invention before that.

⁴ 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

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 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 were 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.

later in time than the November 14, 2002 conception of the claimed inventions and thus would not be prior art regardless.

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]
 - [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]

○

[REDACTED]

■

[REDACTED]

■

[REDACTED]

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

March 2003:

•

[REDACTED]

■

[REDACTED]

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

April 2003:

•

[REDACTED]

- [REDACTED]
- [REDACTED]

May 2003:

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

June 2003:

- [REDACTED]

○

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

•

[REDACTED]

July 2003:

•

[REDACTED]

■

[REDACTED]

■

[REDACTED]

- [REDACTED]

[REDACTED]

August 2003:

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

September 2003:

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

October 2003:

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

D. The inventors exercised achieved a constructive reduction to practice by the filing of U.S. Provisional Patent Application Serial No. 60/513,080 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 17, 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 12,340 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: July 17, 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 17, 2024

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