

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.

IPR2024-00675
U.S. Patent No. 7,523,484

PATENT OWNER PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. Introduction.....	1
II. The '484 Patent	1
A. Date of Invention.....	1
B. Person of Ordinary Skill in the Art (POSITA)	1
C. Overview of the '484 Patent	1
III. Claim Construction.....	5
A. "Access Control Configured To Reconfigure The Communication Device ... If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy"	5
IV. Petitioners' References.....	11
A. Krantz	12
B. Herrmann.....	14
V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims.....	16
A. Ground 1: Krantz Is Missing Claimed Limitations.....	16
1. Krantz Does Not Disclose "An Access Control Configured To Reconfigure The Communication Device Such That Data Sent From The Access Device Is Received By The Less-Restricted Subset Of The Protected Network ... If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy"	17
2. Krantz Fails To Disclose "A Policy Auditor Configured To Audit The Access Device Using The At Least One Security Policy"	22
B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious The Challenged Claims.....	27

VI.	All Grounds: Neither Reference Constitutes Prior Art	30
A.	Legal Standard.....	31
B.	The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....	32
C.	The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.	34
D.	The Inventors Exercised 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	43
VII.	Conclusion	44

TABLE OF AUTHORITIES

FEDERAL CASES

<i>ATI Techs. v. Iancu</i> , 920 F.3d 1362 (Fed. Cir. 2019)	31, 35, 43
<i>Bey v. Kollonitsch</i> , 806 F.2d 1024 (Fed. Cir. 1986)	32
<i>Monsanto Co. v. Mycogen Plant Sci., Inc.</i> , 261 F.3d 1356 (Fed. Cir. 2001)	31, 35
<i>Globus Med., Inc. v. Depuy Synthes Prods., LLC</i> , No. IPR2015-00107 (P.T.A.B. May 1, 2015)	33
<i>LG Elecs., Inc. v. Wi-LAN Inc.</i> , No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018)	30, 31
<i>Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.</i> , 841 F.3d 1004 (Fed. Cir. 2016)	31, 32
<i>Polaris Indus., Inc. v. Arctic Cat, Inc.</i> , 882 F.3d 1056 (Fed. Cir. 2018)	30
<i>SAS Institute Inc. v. Iancu</i> , 138 S.Ct. 1348 (2018)	33
<i>Sequenom v. Leland Stanford Junior Univ.</i> , No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014)	31
<i>Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc.</i> , 774 F.3d 968 (Fed. Cir. 2014)	31

FEDERAL STATUTES

35 U.S.C. § 102(e)	31, 32
35 U.S.C. §§ 119(e) & 112, ¶ 1	43

STATE STATUTES

ECL	39
-----------	----

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 '484 Patent
2010	Constructive Reduction to Practice of the '484 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 submits this Patent Owner Preliminary Response to the Petition related to claims 1-5, 11, 12, 16-19 and 23-25 (the "Challenged Claims") of U.S. Patent 7,523,484. Patent Owner requests the Board reject the Petition because the Grounds presented and art relied on fail to render any of the Challenged Claims unpatentable because the art fails to render obvious all of the claimed limitations, because the art does not qualify as prior art.

II. The '484 Patent

A. Date of Invention

For the reasons discussed in section VII, 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)

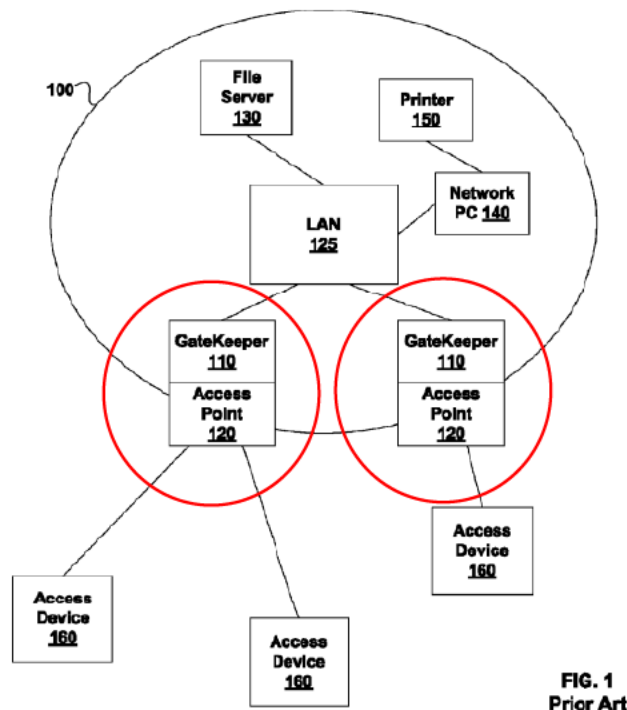
A POSITA would have a working knowledge of computer network security art. A POSITA would have a bachelor's degree in computer science, computer engineering, or electrical engineering, and at least three years of experience in networking operating systems and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields.

C. Overview of the '484 Patent

The patent is directed to a novel security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required a

"gatekeeper" between each client/user and the network. EX1501, Fig. 1, 1:53-60; EX2001, ¶¶ 44-45. But as the patent explains, access control is improved by evaluation of accessing device's hardware and software, *e.g.*, virus protection, before the gatekeeper granted such access—thus consuming substantial network resources and creating bottlenecks. EX1501, 1:41-52.

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



The protected network 100 includes two Gatekeepers 110, each associated with a different instance of an Access Point 120. All devices attempting to access the protected network are required to be evaluated by a gatekeeper. 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." EX1501, 2:31-34. The gatekeeper then becomes a limiting bottleneck. *Id.*

The patent addressed this previously unidentified problem with a novel and non-obvious approach relieving computer resources by configuring an access point in response to approval of a device by the gatekeeper. By configuring the access point to allow devices vetted by the gatekeeper to meet both authentication requirements and device compliance (auditing), to access the protected network, subsequent evaluation of the user/device by the gatekeepers when the previously evaluated device accesses the network again is obviated.

The patent discloses a protected network including a restricted subset with a gatekeeper and less-restricted subsets.

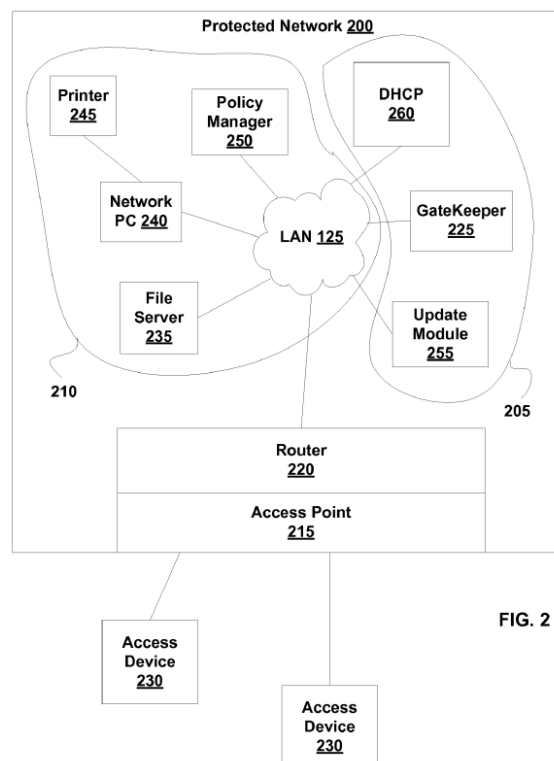
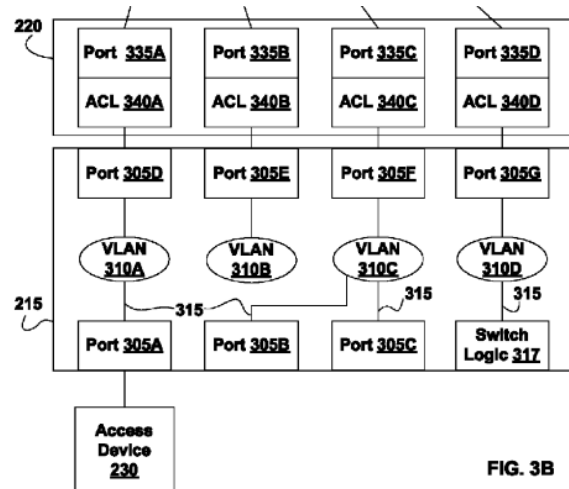
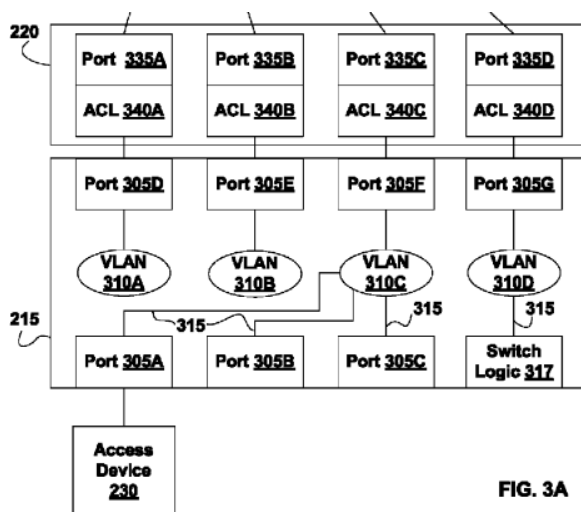


FIG. 2

EX1501, Fig. 2. Before a device is granted access to a less-restricted subset 210, its request is passed to the restricted subset (indicated as 205). EX1501, 2:52-56, 5:51-54. A gatekeeper in the restricted subset audits the device against security policies pertaining to device configurations (e.g., virus protection software). EX1501, 6:34-48; 7:42-45. Determining whether the user/device is authenticated (e.g., username, password, MAC address) to access the protected network may also be performed. *E.g.*, EX1501, 6:41-49. In this embodiment, if the device passes both the audit and authentication, it is granted access to a less-restricted subset of the protected network. EX1501, 11:10-67, 12:1-43.

An improvement over the earlier approaches is that rather than require all device communications to pass through the gatekeeper, the access point itself is configured in response to approval of the device by the gatekeeper. The patent explains:



Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-23.

By configuring the access point in response to approval of the device, network traffic for previously approved devices passes to the less-restricted subset without passing through the gatekeeper, thereby alleviating the burden on computer resources.

III. Claim Construction

Petitioners assert the claims should be given their ordinary as understood by a POSITA. Pet. at 7. Petitioners avoid providing any explanation and then deviate from the ordinary meaning by way of their arguments regarding how the cited references supposedly meet the claimed limitations.

Patent Owner contends the claims should be given their ordinary meaning in the context of the intrinsic evidence, as discussed herein. Patent Owner provides the following context for certain claim terms to properly frame the appropriate ordinary meaning.

- A. "Access Control Configured To Reconfigure The Communication Device ... If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy "**

The Challenged Claims require "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network ... if the audit results in a determination that the access device meets the requirements of the at least one security policy...." EX1501 at 16:11-17. The ordinary meaning of this limitation requires reconfiguration **of a communication device**—not merely a change to the user device (i.e., "access device") or to user identification data. The claimed "reconfiguration" is also required to be "if the audit results" in the device being qualified. As discussed herein, this "audit" pertains to whether the device includes the software/hardware necessary to comply with a security policy – a distinct evaluation from authentication.

One must first look to the words of the claim. "Configure" means to arrange something.¹ "Reconfigure" just means to change an existing configuration.

Further, reconfiguration must be of the "communication device." And, this reconfiguring must be in response to approval of a device based on an audit request.

The specification is consistent with this plain meaning, and teaches: "[t]o grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected. The

¹ See <https://www.merriam-webster.com/dictionary/configure>.

reconfiguration typically includes assigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 3:20-25. The specification provides an example of configuring the "access point" 215 involving reassigning ports.

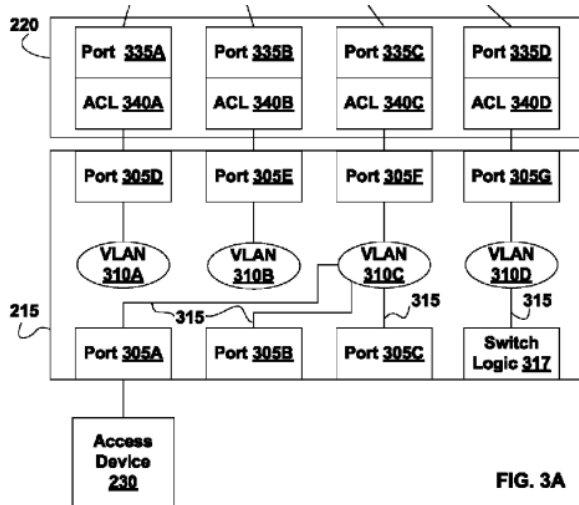


FIG. 3A

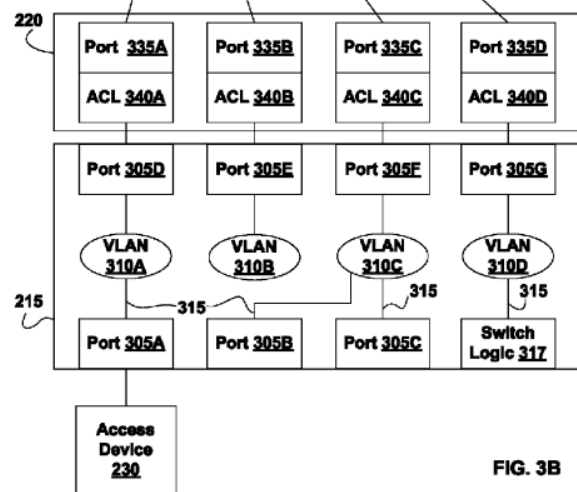


FIG. 3B

Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F.

EX1501, 8:16-26.

Switch Logic 317 is controlled by an Access Control 320 included in GateKeeper 225. Access Control 320 is configured to send commands to Switch Logic 317 in order to reconfigure members of Ports 305A-305G. This reconfiguration includes modifying the association of members of Ports 305A-305G with different members of VLANs 310A-310D.

Id., 9:20-25.

Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed. This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317. For example, in some embodiments, if Security Policy 330A applies and if Access Device 230 satisfies requirements of Security Policy 330A, then Policy Auditor 325 provides a notice to Access Control 320. In response, Access Control 320 sends appropriate commands to Switch Logic 317. These commands cause changes in Port 305A, such that communication from Access Device 230 is no longer blocked by ACL 340C and can now be received by elements of Less-restricted Subset 310.

FIG. 3B is a block diagram showing further details of Access Point 215, Router 220 and GateKeeper 225 of FIG. 2, after access has been granted to elements of Less-Restricted Subset 210, according to various embodiments of the invention. Port 305A has been reconfigured to be associated with VLAN 310A rather than VLAN 310C.

Id., 9:30-62.

Thus, ordinary meaning for "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network ... if the audit results in a determination that the access device meets the requirements of the at least one security policy..." is a network component that rearranges the communication device, such as the ports of an access point itself, in response to auditing of the device.

A further part of the limitation deserved of discussion is the requirement that the reconfiguration occurs "if the audit results in a determination that the access device meets the requirements of the at least one security policy." Of particular relevance are "audit" and "security policy."

The specification, which is the best guide for determining the meaning of claim terms, is clear. A security policy can include authentication, i.e., identification, which pertains to confirmation that the user or user's device is what they or it purports to be. A security policy can also include determining whether the device complies with software/hardware requirements of the network. As such, the claimed audit and determination that the device meets the requirement of a security policy means the device's hardware/software meets network device requirements. Notably, "auditing" is not authentication.

Various embodiments of the invention include a network gatekeeper comprising at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, ***a policy auditor configured to audit an access device using the at least one security policy***, in response to a request to access the less-restricted subset of the protected network, ***the request being sent from the access device to the gatekeeper via a communication device, and an access control configured to reconfigure the communication device*** such that data sent from the access device can be received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, ***if the audit results in a determination that the access device meets the requirements of the at least one security policy***, the restricted subset of the protected network including the gatekeeper.

EX1501, 3:60-67, 4:1-9.

Access Control 320 is responsive to a Policy Auditor 325 included in GateKeeper 225. ***Policy Auditor 325 is configured to receive a request for access to Less-Restricted Subset 210 from Access Device 230, to determine which of Security Policy 330A or optional Security Policy 330B applies to the current request, to perform a security audit of Access Device 230 based on the appropriate member of Security Policies 330A-330B, and to notify Access Control 320 if the audit is passed.*** This notice typically causes Access Control 320 to reconfigure a member of Ports 305A-305G using Switch Logic 317.

EX1501, 9:30-43.

The specification also establishes "auditing" and "authentication" are two different evaluations: "[r]eliance 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." EX1501, 1:41-44. The specification also distinguishes between the claimed "audit " and "authentication":

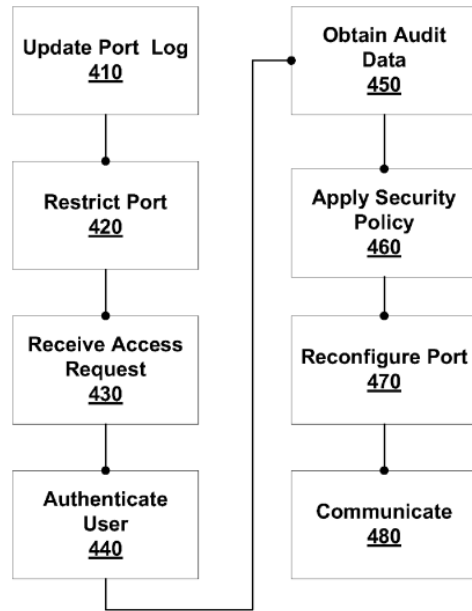


FIG. 4

... Update Port Log Step 410 and a Restrict Port Step 420 are used to prepare an open (unused) communication port on Access Point 215 for receiving a request for access to Less-Restricted Subset 210. 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.*

EX1501, 10:26-40.

IV. Petitioners' References

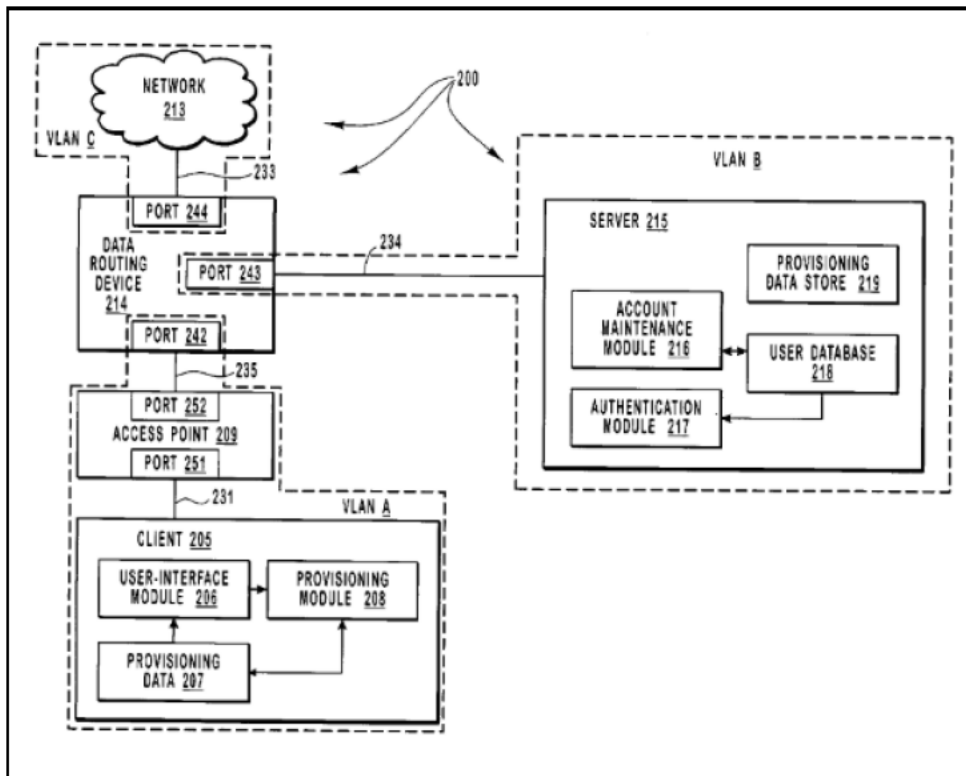
Krantz and Herrmann are not prior art. Krantz and Herrmann are also readily distinguished from the Challenged Claims, and merely illustrate examples of the earlier network security approaches improved upon by the '484 Patent.

A. Krantz

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.

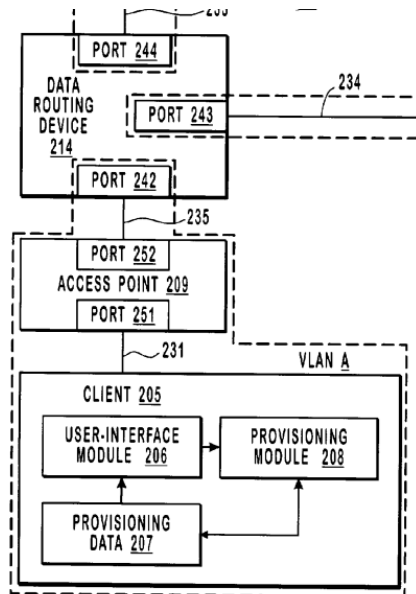
EX1505, Abstract. Krantz discloses the concept wherein upon the failure of a computer system to **authenticate a user** to one network, the user can access a second network for the limited purpose of downloading files by a server. EX2001, ¶¶47-49. This authentication by Krantz is further explained below.



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.

EX1505, [0016]. As shown, in the excerpted portion of Fig. 2, an access point 209 is identified and the client communicates via access point 209 through port 251. *See*

id., [0063]. 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 of arranging or rearranging the access point 209 in response to approval of a device (including both user authentication and device security policy compliance) by a gatekeeper. EX2001, ¶¶ 49, 64. Krantz does not teach arranging the access point in response to anything, let alone in response to evaluating a user or device attempting to access a network. Ports 251 and 252 are never arranged in response to any evaluation by a gatekeeper. EX2001, ¶¶ 59-60. Instead, Krantz teaches only modifying data on the user device.

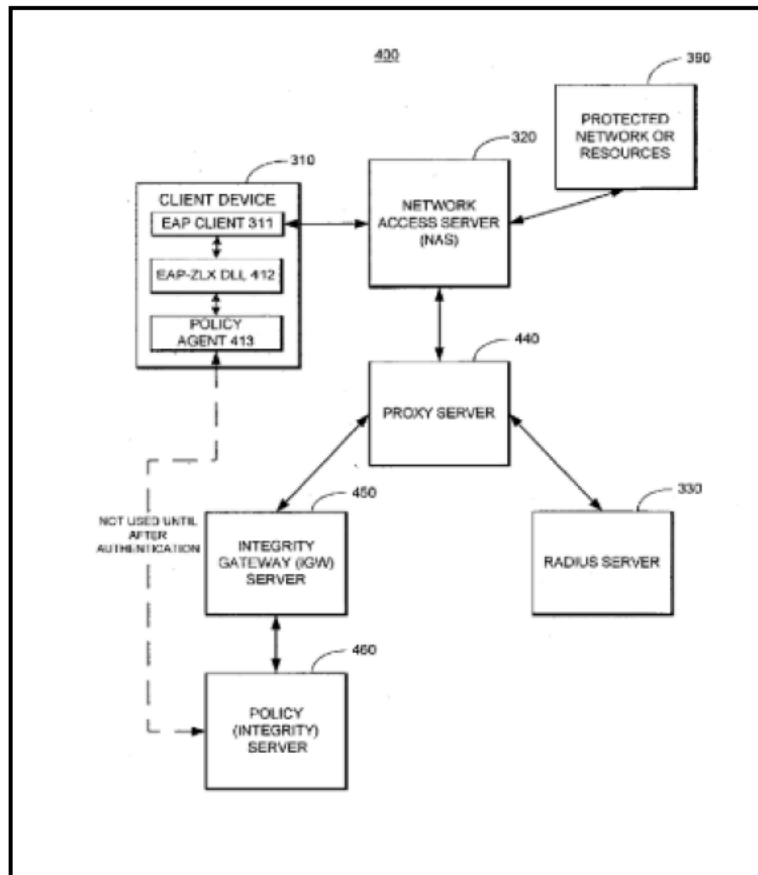
B. Herrmann

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.

EX1506, Abstract. Like the prior art discussed in the '484 Patent, Herrmann utilizes servers between the client device and the protected network, and all 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; *see also id.*, ¶ 62.



EX1506, Fig. 4, *compare id. to* EX1501, Fig. 1. Unlike the '484 Patent, Herrmann requires all data from client device 310 to pass through the NAS 320. There is no disclosure where the client device is ever able to access the protected network without going through the NAS. Nor, is there any teaching of configuring an access point in response to an access device having satisfied an audit.

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

Ground 1 asserts invalidity based on Krantz alone, and Ground 2 asserts invalidity based on Krantz in combination with Herrmann. For both Grounds, key claim limitations are missing. Institution must be denied.

A. Ground 1: Krantz Is Missing Claimed Limitations

Krantz fails to disclose at least the following limitations: (1) "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network ... if the audit results in a determination that the access device meets the requirements of the at least one security policy"; and (2) "a policy auditor configured to audit the access device using the at least one security policy." Accordingly, the petition based on Ground 1 should be denied.

1. Krantz Does Not Disclose "An Access Control Configured To Reconfigure The Communication Device Such That Data Sent From The Access Device Is Received By The Less-Restricted Subset Of The Protected Network ... If The Audit Results In A Determination That The Access Device Meets The Requirements Of The At Least One Security Policy"

The Challenged Claims require "an access control configured to reconfigure the communication device such that data sent from the access device is received by the less-restricted subset of the protected network ... if the audit results in a determination that the access device meets the requirements of the at least one security policy." Krantz does not disclose this. EX2001, ¶¶ 58-60. Rather, Krantz only discloses inserting "tag headers" into client data; not changing the communication device.

The patent explains configuring a communication device so that data is sent to a less-restricted subset of the protected network "typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 3:22-25. Thus, there are changing pathway assignments for the ports of *the "access point."*

Indeed, as discussed in § II(C), configuration of an access point in response to approval of a device by the gatekeeper involves changing the VLAN to which a port may communicate.

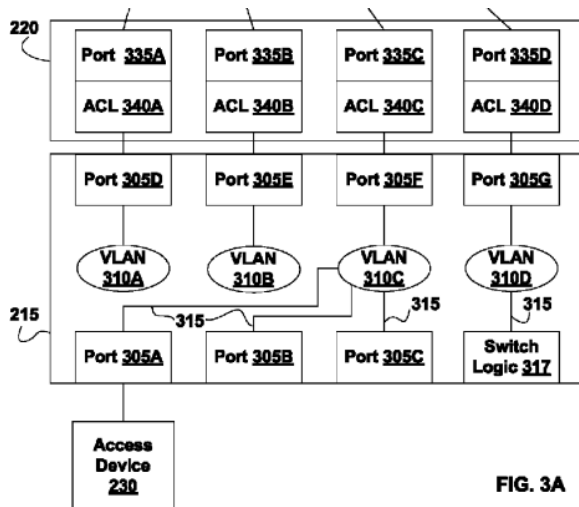


FIG. 3A

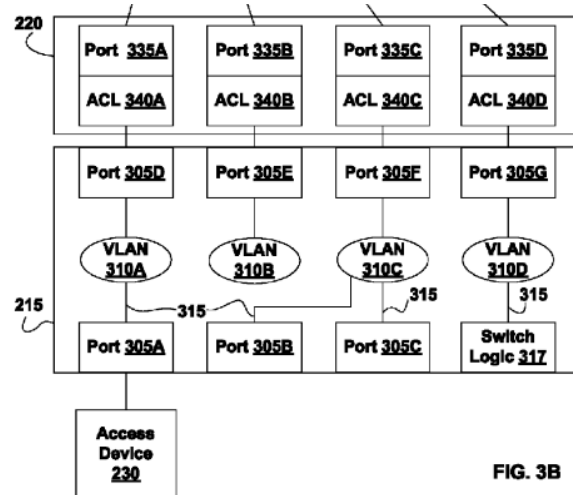


FIG. 3B

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.

EX1501, 7:62-67, 8:1-3.

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., 8:16-23.

Petitioners strain to argue Krantz supposedly discloses the subject limitation by way of "tag header" insertion into client data. Pet. at 41-48. Adding a tag header

to client data is not the claimed configuring of an access point. If anything, it is modification of client information.

Petitioners assert Krantz's "access point 209" is "the communication device." Pet. at 40-42. Petitioners then argue Krantz discloses the claimed reconfiguration of the access point: "Krantz discloses "[w]hen client 205 is authorized to access resources located on VLAN C, access point 209 may enable protocols that are currently blocked for port 251 and may insert Tag Headers indicating that data from client 205 is to be transferred to VLAN C []. Server 215 can send commands to access point 209 to cause access point 209 to enable protocols and cause access point 209 to insert appropriate Tag Headers." Pet. at 48. Petitioners also argue port 251 is "reconfigur[ed]" in a way "such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network" because it facilitates the transfer of data between client 205 ("the access device") and ultimately VLAN C (the "less-restricted subset of the network.") as depicted below." Pet. at 44-46.

Petitioners arguments fall flat. Krantz discloses configuration or reconfiguration of client data, not the communication device. The '484 Patent is clear: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1501, 2:22-25. Ss 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 is "configured" to send data to VLAN 310A. Krantz has no reconfiguration of the communication device. Instead, the Krantz ports in access point 209 send data to the same location (e.g. port 243 to VLAN B and port 244 to VLAN C). Krantz's only teaching is adding identification data to client information.

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.*

EX1505, [0061].

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. Alternately, access point 209 access point 209 and/or data routing device 214 may strip the 802.1X encapsulation and instead encapsulate the EAP-Response/Identity message within an EAP-RADIUS message that is transferred onto VLAN B. ... 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).

EX1505, [0073]-[0076]. It is undeniable Krantz fails to disclose **any** reconfiguration of access point 209. EX2001, ¶ 63. While 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 and may redirect the data based on the user's tagged identification information, there is no "reconfiguring" *of the access point 209*, which Petitioners argue is the claimed "communication device."

Further, Krantz explains it is not the access point, but rather, the data routing device 214 which directs the traffic to VLAN B or VLAN C. EX1505, [0060]; EX2001, ¶59. Even this, however, depends on configuration of client data, not the data routing device itself.

Lastly, as a fallback, Petitioners argue it would have been obvious for one to combine the access point 209 and the data routing device 214. Pet. at 52-55. Regardless of whether access point 209 could be combined with data routing device 214, configuring client data with tag headers is not configuring of the access point – it is only manipulating "data from client 205." EX1505 at, e.g., [0061]. As such, the different data paths of Krantz still require the data routing device to check user identification information, namely, the tag header.

Further, Krantz recites separate access point 209 and data routing device 214. Arbitrarily combining these distinct components finds no support in Krantz. To the contrary, Krantz expressly teach access point 209 and a different component, namely a data routing device 214. EX1505, [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."). Krantz further confirms any configuration is of user identification data, not an access point as claimed, because "EAP-Response/Identity messages" expressly relate to user authentication.² Even if 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 EX1505, [0060].

Krantz's failure to disclose the reconfiguration of the communication device alone requires denial of institution.

2. Krantz Fails To Disclose "A Policy Auditor Configured To Audit The Access Device Using The At Least One Security Policy"

The Challenged Claims recite "a policy auditor configured to audit the access device using the at least one security policy." Despite Petitioners' attempts to conflate authentication with auditing, Krantz lacks *any* device *auditing*.

Petitioners argue Krantz discloses the claimed "policy auditor" as "server 215." Pet. at 32-36.

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

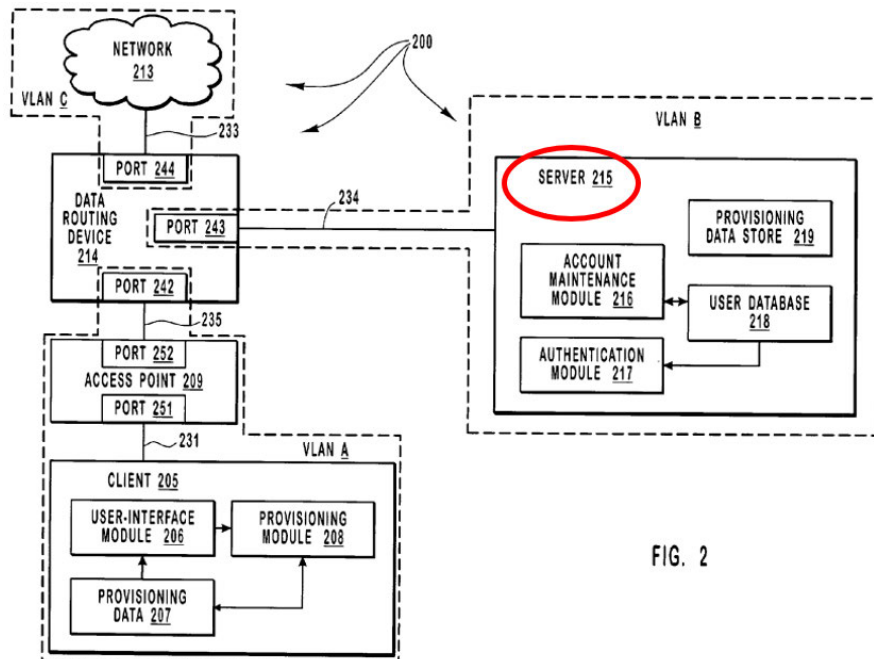


FIG. 2

But the Krantz server 215 is only for authentication. By contrast, the Challenged Claims recite a "policy *auditor*." As discussed, the correct construction of a policy audit is an evaluation of device information related to whether it complies with software/hardware requirements of the network. Krantz fails to disclose any evaluation of the "device information." Petitioners rely on Krantz's disclosures regarding client *authentication*, which, as discussed is a different evaluation from device auditing. Indeed, Krantz's disclosure is clearly limited to client authentication and silent on device auditing.

The '484 Patent expressly distinguishes between evaluating "authentication" information and "auditing" a device. The '484 Patent explains auditing relates to evaluating data about the device's software and/or hardware that is necessary to comply with a security policy, such as "operating system status (version, updates,

etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230[.]" EX1501, 11:45-47. In contrast, authentication merely confirms identity. EX1501, 1:31-37 ("A first level of access control is achieved by requiring authentication of a user. This may be accomplished by requiring the user to enter a username and password or by reading a MAC address or other identifying information from an access device. ")

Authentication is a different technical concept, process, and implementation from the claimed "evaluate device information received from the device in response to the audit request." Indeed, a user can be properly authenticated, but if the access device does not have the proper antivirus software, then the network can be at risk. EX1501, 6:41-48.

Yet, Krantz only discloses user authentication, and fails to disclose anything about "evaluat[ing] device information in response to the audit request":

- "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 40-41.
- "If an **authenticated user** of client 205 . . . is authorized to access resources..." EX1505, [0076] (cited in Pet. at 26-27, 35, 40, 49).
- "Krantz discloses that the 'method 300 includes [the act of client 205] sending credentials to a server to **authenticate**" Pet. at 28.

- "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**) . . ." EX1505, [0019].

With no evidence for Krantz of auditing a device—checking the device for compliance with network security policies—Petitioners repeatedly cite to user authentication protocols and incorrectly conclude this is "device information" or an "audit request." *See* Pet. at 56-59. As Dr. Cole explains, such device authentication is different from device auditing. *See* EX2001, ¶¶ 49, 58-59.

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

[Krantz] discloses that the "server (based at least in part on received credentials) may authorize the client for at least partial access to the single network.

Pet. at 32. Petitioner's "credentials" argument fails immediately. The '484 Patent explains user authentication data and audit data are different. *Compare* EX1501, 1:33-42 (authentication) *with* 11:48-54 (audit data). Next, the Krantz "credentials" are the "user-identifier[s] and password[s]" which the '484 Patent expressly explains relate to authentication; they are not audit data. *See* Pet. at 33; EX1501, 1:33-37. Indeed, a user may access different devices using the same username and password. Third, Petitioners claim credentials also "can include sending an Extensible Authentication Protocol ('EAP') Response/Identity message..." Pet. at 33. EAP is for authentication. In fact, it is an acronym that stands for Extensible **Authentication**

Protocol. EX1501, 8:29-30. EX2001, ¶ 57. Fourth, Petitioners assert "authentication module 217 can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in user database 218. If credential information matches an entry in user database 218, the identity of the user is authenticated[.]" Pet. at 35. Again, on its face, this is user data unrelated to audit data for the device. EX2001, ¶¶ 57-58.

Additionally, Petitioners baldly claim Krantz's disclosures are "consistent with the disclosure of the 484 Patent that describes security policies having requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), ... or to authenticate an access device or user." Pet. at 27. This is wrong for several reasons. First, this is not what the '484 Patent says. Rather, the '484 Patent 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* EX1501, Fig. 4, 10:26-44. Nowhere does it say that audit data is the same thing as authentication information. Second, the claim requires "a policy auditor configured to audit the access device." Not to "authenticate a *user*" which is a distinct type of evaluation.

Petitioners' secondary reference, Herrmann, even confirms authentication is distinct from security policy compliance. "One problem that is not addressed by current NAS and RADIUS [authentication] technology is ensuring that all devices

that connect to a network comply with and enforce applicable security policies."

EX1506, [0011].

The '484 Patent also expressly 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.**

EX1501, 13:57-67, 14:1-3 (ALL CAPS emphasis of "AND" in original).

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

B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious The Challenged Claims

Petitioners argue, to the extent Krantz is deemed not to disclose certain claim limitations, a POSITA would have found it obvious to and been motivated to incorporate Herrmann with Krantz.

Ground 2 fails first because even the asserted combination of Krantz and Herrmann fails to disclose at least the "access control configured to reconfigure the communication device such that data sent from the access device is received by the

less-restricted subset of the protected network ... if the audit results in a determination that the access device meets the requirements of the at least one security policy " limitation.³ Regardless of whether one considers Krantz alone or in combination with Herrmann, this specifically required limitation of the Challenged Claims is missing.

In addition, the Petition relies on Krantz alone for several of the claimed limitations of claim 1. With respect to the limitations Petitioners identify as 1.1-1.3, Petition cherry-picks portions of Herrmann to fill them. Petitioners' contentions regarding these limitations still fail. Also, the motivation to combine isolated teachings from Herrmann with Krantz argued in the Petition do not pass muster.

The Petition argues, "[t]o the extent [] one asserts [] Krantz does not disclose 'at least one security policy including requirements that must be satisfied,' it would have been obvious in view of Herrmann. Pet. at 65-66. But Petitioners' application of Herrmann continues to conflate authentication and auditing just as with Krantz. Petitioners argue "[c]hecking for anti-virus software would merely be an additional item for server 215 ("gatekeeper") to *evaluate in the authentication process* already disclosed by Krantz[.]" Pet. at 70.

³ Notably, Petitioners do not argue that Herrmann teaches the "configure an access point in response to approval of the device by the gatekeeper" limitation.

Thus, Petitioners claim that Herrmann's "policy requiring that a specific virus protection program is operational on each client device that is connected to a network" would be evaluated through Krantz "authentication process," and that doing such would "merely be an additional item for server 215." Pet. at 66. Petitioners' conclusory assertion of the ease of including the separate auditing evaluation with the authentication process is contrary to the evidence. The '484 Patent expressly says: "The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol." EX1501, 14:1-3. The '484 Patent then provides a specific explanation for exactly how to do this complicated process. *See, e.g.*, EX1501, 14:42-45 ("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" (Pet. at 66) to add to the authentication process.

Petitioners argue a POSITA would have modified Krantz based on the generalized notion that Krantz is "specifically focused on network authentication and security." Pet. at 66-67. Krantz, however, is limited to authentication and includes nothing about device auditing. EX2001, ¶¶ 57-59. Indeed, the lack of any

recognition in Krantz of auditing 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 citations omitted). Krantz's lack of recognition of security policy compliance highlights the smoke and mirrors of the Petition's reliance on Krantz's paragraph [0019] for Krantz's purported goal of "security." Petitioners even go so far as to rely on the '484 Patent for a motivation to combine by stating that "[t]he 484 Patent itself confirms that a POSITA would recognize the need for the server/authentication module of Krantz to check for up-to-date and approved antivirus programs." In so doing, Petitioner expressly rely on the patent to provide a roadmap for combining references, which is quintessential impermissible hindsight. *Ruiz v. AB Chance Company*, 357 F.3d 1270, 1275 (Fed. Cir. 2004).

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

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

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

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

The purpose of diligence is to show that the invention was not abandoned, set aside, or unreasonably delayed, not to "scour the patent owner's corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity." *Id.*

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

Petitioner asserts that 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.

On November 14, 2002, the InfoExpress inventors had the "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification" (EX2011: "LAN Engineering Specification") prepared demonstrating that the claimed inventions were conceived of at least as of that date. 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 had started diligently working.

On October 7, 2002, inventor Stacey Lum told the InfoExpress team that:

"All, It may be possible to use 802.1x to audit [enforce] a system rather than switching them between VLANs. There's an authentication specific component in 802.1x, so we might be able to use that instead of VLANs." EX2015; EX2016.

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

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

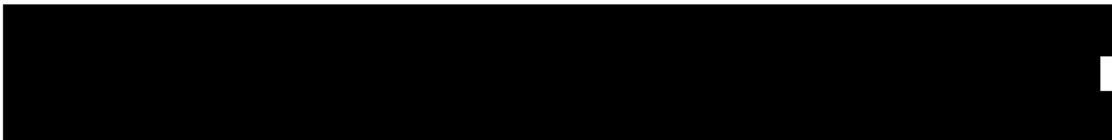
The InfoExpress inventors, employees, and team members diligently pursued reducing the claimed invention to practice from conception until constructive reduction to practice on at least October 21, 2003. This diligence is shown by substantial InfoExpress evidence including:

- 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 (Court finding substantial diligence evidence where the Patent Owner identified record evidence showing activity multiple times per month during the critical period, and there was no reason to doubt that the activity was relevant in reducing the invention to practice).

December 2002:

- 

[REDACTED]

[REDACTED]

[REDACTED]

- 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]

○

■

■

■

■

■

■

■

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

March 2003:

•

■

[REDACTED]

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

April 2003:

- [REDACTED]

- [REDACTED]

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

May 2003:

- [REDACTED]

- [REDACTED]

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

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

June 2003:

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

[REDACTED]

- See EX2003, ¶53 (Lum Declaration).

July 2003:

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

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

August 2003

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

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

- See EX2003, ¶52 (Lum Declaration).

September 2003

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

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

October 2003

- [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- See EX2003, ¶¶14, 23, 25, 64-66 (Lum Declaration).

D. The Inventors Exercised 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 24, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	<u>/s/ Brian R. Michalek</u> 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@saull.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@saull.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saull.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 13,959 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