

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

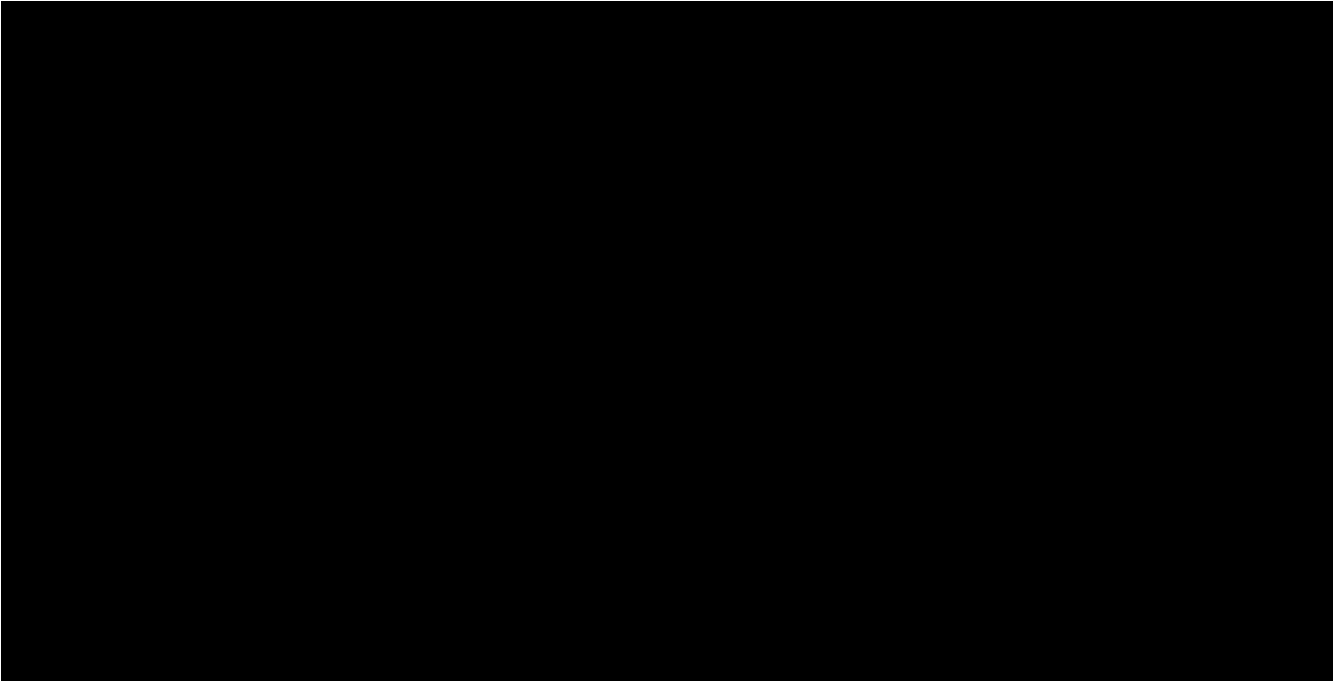
INFOEXPRESS INC.,
Patent Owner.

IPR2024-00539
U.S. Patent No. 8,051,460

PATENT OWNER RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. INTRODUCTION	1
II. PETITIONER'S UNPATENTABILITY GROUNDS.....	1
III. THE 460 Patent.....	2
A. Date of Invention.....	2
B. Person of Ordinary Skill in the Art (POSITA)	2
C. Overview of the 460 Patent	2
IV. THE CITED ART.....	8
A. Krantz	8
B. Herrmann.....	10
V. CLAIM CONSTRUCTION	12
A. "Protected Network".....	13
B. "Reconfiguring the Communication Port"	13
VI. GROUND 1: KRANTZ FAILS TO RENDER CLAIMS 1-6, 10-14, 16-22, 27, and 29-30 OBVIOUS	14
A. Krantz Does Not Disclose Nor Render Obvious "Reconfiguring The Communication Port ...".....	14
1. Mapping #1	15
2. Mapping #2	15
3. Mapping #3	18
B. Krantz Does Not Disclose A Restricted Subset Of The Protected Network Including A Gatekeeper	19
C. Krantz Does Not Disclose "Applying A Security Policy To The Access Device" Or "Using The Gatekeeper To Determine If Requirements Of The Security Policy Are Satisfied By The Access Device" Or "System Data"	25
VII. GROUND 2 – KRANTZ AS MODIFIED BY HERRMANN FAILS TO RENDER CLAIMS 1-6, 10-14, 16-22, 27, and 29-30 OBVIOUS	27

A.	All Claims.....	27
1.	Petitioners Have Failed To Demonstrate The Combination	27
2.	Herrmann Confirms “Applying A Security Policy To The Access Device” Would Not Have Been “Minimal,” “Simple”, or Merely An “Additional Check” For Krantz’s Server	30
3.	Herrmann’s Client-Side System Teaches Away From Combination with Krantz’s Server-Side System	33
B.	Dependent Claim 22	36
C.	Dependent Claim 27	38
VIII.	OBJECTIVE EVIDENCE DEMONSTRATES NON-OBVIOUSNESS	39
A.	At the Time of the Invention and at Present, InfoExpress’s Products Embody the Claimed Inventions and are Coextensive	
		
IX.	All Grounds: Neither Reference Constitutes Prior Art	64
A.	Legal Standard.....	64
B.	The Inventors Conceived of the Inventions Prior to the Critical Dates of Both References.....	65

C.	InfoExpress Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.	69
D.	The Inventors Achieved a Constructive Reduction to Practice by Filing U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003	82
X.	Conclusion	83

TABLE OF AUTHORITIES

FEDERAL CASES

<i>Apple Inc. v. Samsung Elecs. Co.</i> , 839 F.3d 1034 (Fed. Cir. 2016)	43
<i>ATI Techs. v. Iancu</i> , 920 F.3d 1362 (Fed. Cir. 2019)	64, 70
<i>Fox Factory, Inc. v. SRAM, LLC</i> , 944 F. 3d 1366 (Fed. Cir. 2019)	40
<i>Ortho-McNeil Pharmaceutical v. Mylan Labs.</i> , 520 F.3d 1358 (Fed. Cir. 2008)	22
<i>Perfect Surgical Techniques v. Olympus America</i> , 841 F.3d 1004 (Fed. Cir. 2016)	65
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc)	12
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	12
<i>Ricoh Co., Ltd. v. Quanta Computer Inc.</i> , 550 F.3d 1325 (Fed. Cir. 2008)	35
<i>Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling U.S., Inc.</i> , 699 F.3d 1340 (Fed. Cir. 2012)	39, 40
<i>Volvo Penta of the Ams., LLC v. Brunswick Corp.</i> , 81 F.4th 1202 (Fed. Cir. 2023)	40

FEDERAL STATUTES

<u>37 C.F.R. § 42.6(d)</u>	85
<u>37 C.F.R. § 42.6(e)(4)</u>	86
37 C.F.R § 42.24(b)	85
37 C.F.R. § 42.24(b)(1)	85
35 U.S.C. § 102(e)	64, 65
35 U.S.C. §§ 119(e) & 112, ¶ 1	82

STATE STATUTES

According to the Institution Decision, Mapping #2	15
---	----

rules. EX2504.....	59
--------------------	----

OTHER AUTHORITIES

“Policy Server.” EX1006, Figure 4.....	31
<i>Barnesandnoble. com, Inc</i>	12, 13
<i>Cisco Systems, Inc. v. InfoExpress Inc.</i> , IPR2024-00540, Paper No. 13 (PTAB Sept. 24, 2024)	41
<i>Google LLC v. DDC Tech., LLC</i> , IPR2023-00707, Paper No. 78.....	64
Herrmann’s “IA_HEARTBEAT”	36
https://en.wikipedia.org/wiki/RADIUS	9
IPR2024-00678, Paper 14	26
IPR2025-0549, Paper 13	26
<i>Quanergy Sys., Inc. v. Bodyne Lidar Inc.</i> , IPR2018-00255, Paper No. 59 (PTAB May 23, 2019).....	46, 47, 49
Rather, “Network 213”	22
report on February 10, 2003. EX2075	74
U.S. Patent 5,987,611	34
U.S. Patent 8,051,460	1, 40, 41, 51

EXHIBIT LIST

Exhibit Number	Description
2001	Declaration of Dr. Eric Cole
2002	Curriculum Vitae of Dr. Eric Cole
2003	Declaration of Stacey C. Lum
2004	Intentionally Left Blank
2005	U.S. Provisional App. No. 60/505,582
2006	U.S. Provisional App. No. 60/513,080
2007	Declaration of Hugh Smith, Ph.D.
2008	Curriculum Vitae of Hugh Smith, Ph.D.
2009	Conception of the '460 Patent
2010	Constructive Reduction to Practice of the '460 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	Windows 2000 Registry – 2nd Edition – Little Black Book
2273-2410	Intentionally Left Blank
2411	Tim Greene, InfoExpress Simplifies Security Devices, NetworkWorld (Dec. 6, 2004), available at https://www.networkworld.com/article/875004/lan-waninfoexpress-simplifies-security-devices.html
2412	InfoExpress's Objections and Responses to Cisco's First Set of Interrogatories (Nos. 1-12), served in InfoExpress Inc. v. Cisco Systems, Inc., Case No. 4:23-cv-2698-YGR (N.D. Cal.).
2413	Cisco Systems, Inc., Network Admission Control White Paper (2004).
2414	Correspondence with Cisco
2415	Email attachment to EX2414
2416	Correspondence with Cisco
2417	Email attachment to EX2416
2418	Correspondence with Cisco
2419	Correspondence with Cisco
2420	Correspondence with Cisco and KeyLabs
2421	Email attachment to EX2420
2422	Correspondence with Cisco
2423	Correspondence with Cisco
2425	Excerpt from InfoExpress Inc.'s Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2, Exhibit B,

Exhibit Number	Description
	served in InfoExpress Inc. v. Cisco Systems, Inc., Case No. 4:23-cv-2698-YGR (N.D. Cal.).
2426	Intentionally Left Blank
2427	Declaration of Aaron R. Striegel, PhD
2428	Intentionally Left Blank
2429	Declaration of Yuhshiow Alice Lee
2430	LAN Based Policy Enforcement Engineering Specification
2431	Metadata for EX2430
2432	LAN Based Policy Enforcement Engineering Specification
2433	Metadata for EX2432
2434	Internal InfoExpress Correspondence
2435	Internal InfoExpress Correspondence
2436	Additional Metadata for EX2011
2437	LAN Based Policy Enforcement Engineering Specification
2438	Metadata for EX2437
2439	Internal InfoExpress Correspondence
2440	Internal InfoExpress Correspondence
2441	Internal InfoExpress Correspondence
2442	Internal InfoExpress Correspondence
2443	Design Specifications
2444	Design Specifications
2445	RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS) July 2024
2446	Tim Greene, Deceiving Ciscos NAC (April 3, 2007)
2447	Hasham Ud-Din Qazi, Comparative Study of Network Access Control Technologies
2448	Thumann and Rocher, Hacking the Cisco NAC Framework Blackhat USA 2007 Whitepaper
2449	Deposition of Henry Houh, December 4, 2024
2450	Dkt 121 – Claim Construction Order dated September 25, 2024 [InfoExpress, Inc. v, Cisco Systems, Inc. [4:23-cv-02698-YGR]
2451	Mobile Agent Deployment Guide
2452	Reference Manual
2453	Server User’s Guide
2454	CGX 2.3 – Standalone Guide
2455	CGX 2.2 Complete Guide
2456	CGX Appliance Specifications

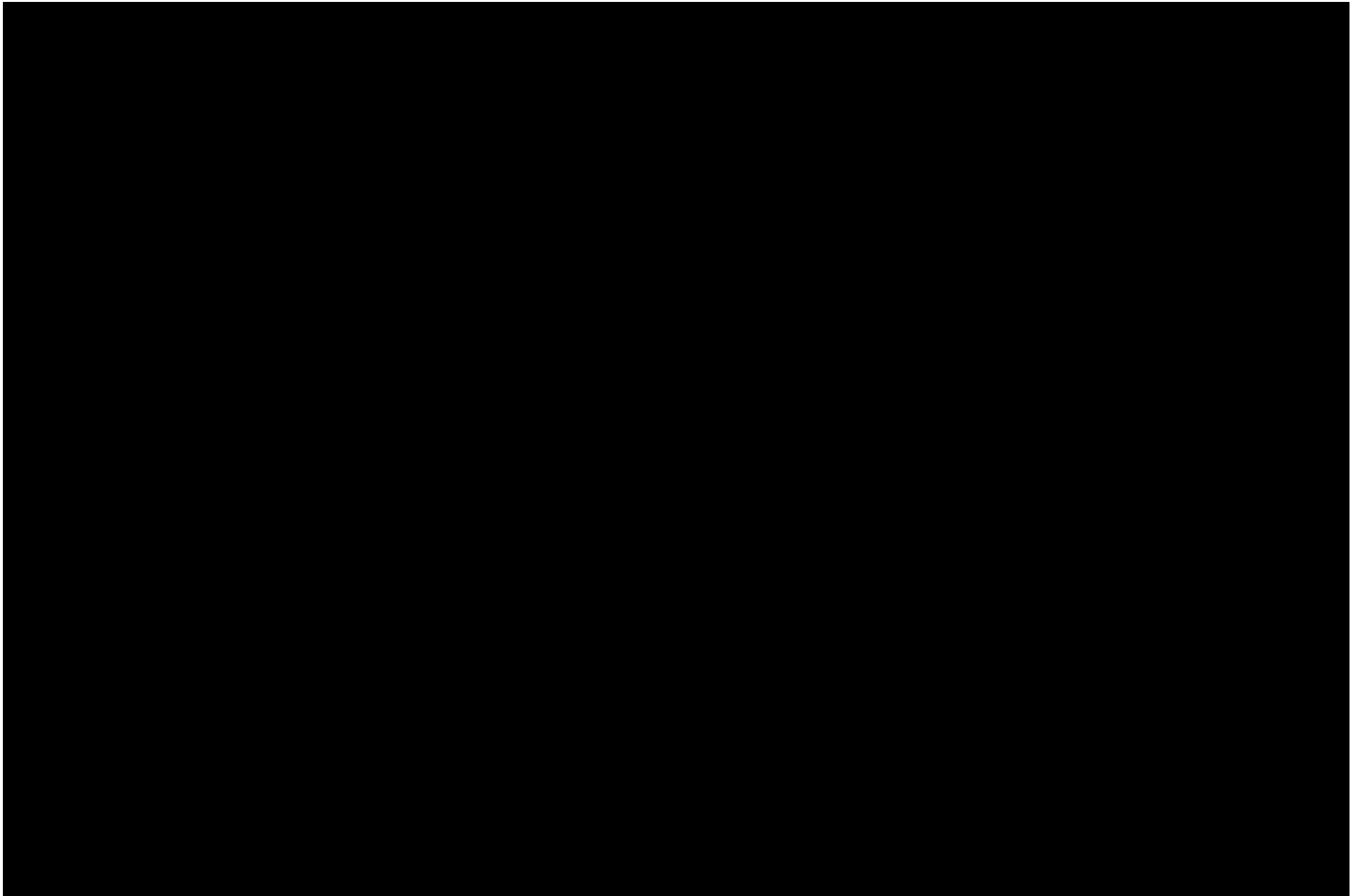
Exhibit Number	Description
2457	Solutions Guide
2458	Intentionally Left Blank
2459	CGX Access Deployment Guide
2460	Installation Guide v9.0
2461	About CGX
2462	CGX 1.0 Frequently Asked Questions
2463	CGX Access - Frequently Asked Questions
2464	CGX Access Guide
2465	Solutions Guide
2466	CGX 2.2 Complete Guide
2467	Solutions Guide
2468	Installing CGX
2469	Correspondence with Scotia Bank
2470	Correspondence with Cisco
2471	Internal InfoExpress Correspondence
2472	Cisco Announces Continued Momentum within Network Admission Control Industry Initiative
2473	Correspondence with Cisco
2474	Correspondence with Cisco
2475	Cisco NAC and CyberGatekeeper Technical White Paper
2476	Internal Cisco Correspondence
2477	Correspondence with Cisco
2478	LAN Technology Presentation
2479	Correspondence with Cisco
2480	NAC Overview
2481	Correspondence with Cisco
2482	Correspondence with Cisco
2483	Partner Solution Brief – NAC Deployment
2484	Cisco NAC + CyberGatekeeper vs. Competitive Enforcement Solutions
2485	Correspondence Between Cisco, InfoExpress and Burton Group
2486	RSA Conference 2005 Slide Deck
2487	Internal InfoExpress Correspondence
2488	RSA Conference 2005 Slide Deck
2489	Correspondence with Cisco
2490	Cisco NAC + CyberGatekeeper vs. Competitive Enforcement Solutions

Exhibit Number	Description
2491	Partner Solution Brief – NAC Deployment
2492	Correspondence with Cisco
2493	Internal InfoExpress Correspondence
2494	NAC IVT Test Plan/Report
2495	Correspondence with Cisco
2496	Correspondence with Cisco
2497	Virtual Machine Preparation for Cisco
2498	Internal InfoExpress Correspondence
2499	Virtual Machine Preparation for Cisco
2500	InfoExpress NAC Demo
2501	Internal InfoExpress Correspondence
2502	Protected Network, ScienceDirect Topics
2503	Correspondence with Cisco
2504	Introduction to CyberGatekeeper
2505	Correspondence with Cisco
2506	Correspondence with Cisco
2507	Correspondence with Cisco
2508	Correspondence with Cisco
2509	Correspondence with Cisco
2510	Internal Cisco Correspondence
2511	Correspondence with Cisco
2512	Internal Cisco Correspondence
2513	Correspondence with Cisco
2514	Internal InfoExpress Correspondence
2515	Internal Cisco Correspondence
2516	Correspondence with Cisco
2517	Correspondence with Cisco
2518	Intentionally Left Blank
2519	NAC2 Beta Deployment Guide
2520	Internal InfoExpress Correspondence
2521	U.S. Patent No. 5,987,611
2522	Request for Comment: 2865
2523	Internal InfoExpress Correspondence
2524	Winning with CyberGatekeeper from InfoExpress
2525	Tim Greene, Burning NAC questions – Part 2, Network World (Oct 17, 2007)

Exhibit Number	Description
2526	Paul Roberts, Black Hat: NAC Solutions Vulnerable to Attack, ComputerWorld (Aug 3, 2006)
2527	Correspondence with Cisco
2528	Memorandum re: Product Announcement
2529	LAN Technology PowerPoint
2530	Posture Plugin Development
2531	Product Guidelines
2532	Technical File Information
2533	Project File
2534	Project File
2535	Project File
2536	Project File
2537	Project File
2538	Project File
2539	Project File
2540	Project File
2541	Technology Overview
2542	Policy Manager Reference Manual
2543	CGS Reference Manual
2544	LAN Enforcement Module Reference Manual
2545	EAP Enforcement Module Reference Manual
2546	8021X Authentication Procedures
2547	Internal InfoExpress Correspondence
2548	Correspondence with Cisco
2549	Cisco Release Notes
2550	Cisco Trust Agent Administrator Guide
2551	Internal InfoExpress Correspondence
2552	NAC AVP Specification
2553	NAC Architecture Overview
2554	HCAP
2555	Correspondence with GTI
2556	Engineering Specifications
2557	LAN Based Policy Enforcement Components
2558	LAN Based Policy Enforcement Engineering Specifications
2559	LAN Based Policy Enforcement Engineering Specifications
2560	LAN Based Policy Enforcement Components
2561	LAN Based Policy Enforcement Engineering Specifications

Exhibit Number	Description
2562	LAN Based Policy Enforcement Engineering Specifications
2563	LAN Based Policy Enforcement Components
2564	Supplemental Declaration of Stacey Lum
2565	Supplemental Declaration of Dr. Eric Cole
2566	Tanenbaum Excerpts
2567	IEEE 802.1 1x (2001)
2568	Diligence Calendar

I. INTRODUCTION



II. PETITIONER'S UNPATENTABILITY GROUNDS

Petitioner raises two obviousness grounds. Ground 1 asserts claims 1, 2, 10-14, 16, 17, 27, 29 and 30 are obvious in view of U.S. Patent Application Publication 2004/0111520 ("Krantz") (EX1005). Ground 2 asserts claims 1-6, 10-14, 16-22, 27, 29, and 30 are obvious in view of Krantz further in view of U.S. Patent Application Publication 2004/0107360 ("Herrmann") (EX1006).

III. THE 460 PATENT

A. Date of Invention

Patent Owner submits for the reasons discussed in section 0 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)

Petitioner's and Patent Owner's position on a POSITA are similar. Petitioner contends a POSITA "would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields." Pet. at 4. Patent Owner agrees on the educational background, and contends that at least three years of experience in networking operating systems and cybersecurity" or "a master's degree in one of the foregoing and at least two years of experience..." is appropriate. Patent Owner does not contend this difference in the amount of experience would affect the outcome.

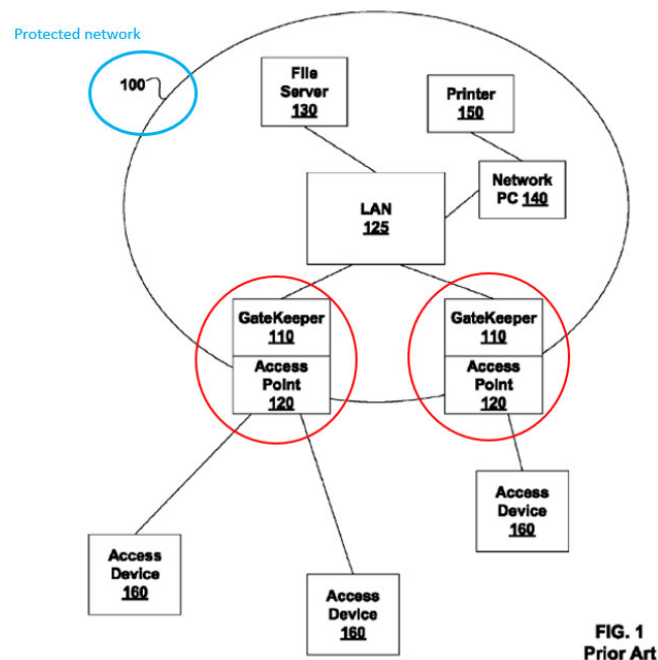
C. Overview of the 460 Patent

The 460 Patent is directed to a seminal approach to addressing computer network security concerns and controlling access to a protected network while overcoming shortcomings in the prior art with scalability and slowed network traffic. Before Patent Owner's inventions, network security required multiple "gatekeepers" placed directly between clients (*i.e.*, users) and the protected network, *i.e.*, inline. EX1001, Fig. 1, 2:41-44; EX2001, ¶¶44-46. Like a security guard at a front gate,

each user would present credentials so the guard could determine whether he or she was authorized to pass through the gate.

The patent explains prior art network control approaches included providing systems outside of or at the periphery of a protected network for authenticating a user or device, such as by checking user ID and password or MAC address. *Id.*, 1:31-40. The patent explains that reliance on authentication alone suffers from disadvantages including not assuring the device meets network security policies, such as out-of-date virus software. *Id.*, 1:41-46.

The patent describes as "prior art" architecture having the identified shortcomings.



EX1001, Fig. 1 (annotated). The protected network 100 included multiple access points, each including a Gatekeeper 110 with one or more access devices connecting

with each access point. All access devices attempting to connect to the protected network must pass through an access point and its gatekeeper. The 460 Patent explains protected networks can have many access points and 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." EX1001, 2:35-38. The inline gatekeeper then becomes a limiting bottleneck on the bandwidth of the system. EX1001, 2:38-41.

An example of utilizing only authentication is Krantz, and an example of access device compliance with a security policy is Herrmann. The 460 Patent, however, improved on the acknowledged problems with prior art approaches to network security (*note*: Krantz and Herrmann are not prior art). The 460 Patent addressed these particular shortcomings with scalability and bandwidth by designing a gatekeeper to operate on a subpart of the protected network itself, and providing for reconfiguring an access point so previously authorized devices can access without tying up as many computer resources and bandwidth.

The 460 Patent discloses a protected network 200 including a restricted subset 205 with a gatekeeper 225 thereon, and one or more less-restricted subsets 210 of the protected network with other network resources.

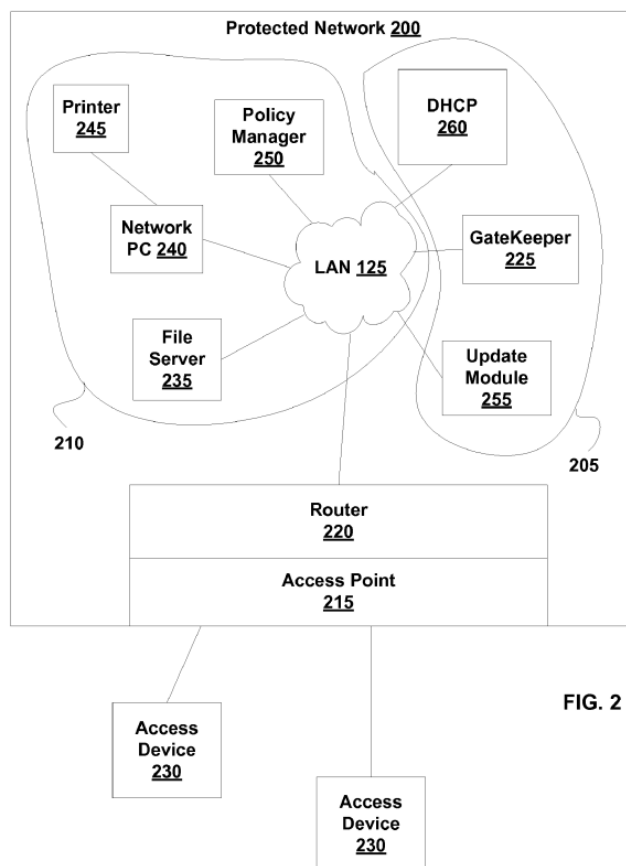


FIG. 2

EX1001, Fig. 2, 5:55-7:54. Before an access device is granted access to a less-restricted subset 210, its request is first passed to the restricted subset 205 of the protected network 200. EX1001, 2:54-56, 5:33-37. A gatekeeper in the restricted subset of the protected network evaluates whether the access device satisfies security policies, and if so, the access device is granted access to a less-restricted subset of the protected network. EX1001, 2:56-60.

The 460 Patent further describes evaluating access devices against a security policy, *i.e.*, device auditing to determine compliance of the **device**, as contrasted with user authentication, such as determining compliance with necessary software

requirements. EX1001, 6:42-45. If the access device configuration satisfies access-device security policy requirements, it may be granted access to the restricted subset of the protected network. EX1001, 2:58-60.

A key claimed feature of the 460 Patent is the reconfiguration of communication ports of the access point after access-device compliance with a security policy is determined, so the device can access the less-restricted subset without passing through the gatekeeper. EX1001, Claims 1 & 16. The specification provides as an example a network "characterized by Virtual Local Area Networks (e.g., VLANs)...." EX1001, 2:62-54. The 460 Patent explains "reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." *Id.*, 3:22-25. The patent further explains reconfiguring the communication ports of an access point of a network comprising multiple VLANs.¹

¹ While the "typical" embodiment discussed utilizes VLANs, the 460 Patent further explains other access point embodiments may be utilized, including "wireless access point and MAC addresses, or the like, are used instead of VLANs to separate traffic from different instances of Access Device 230." *Id.*, 15:25-30.

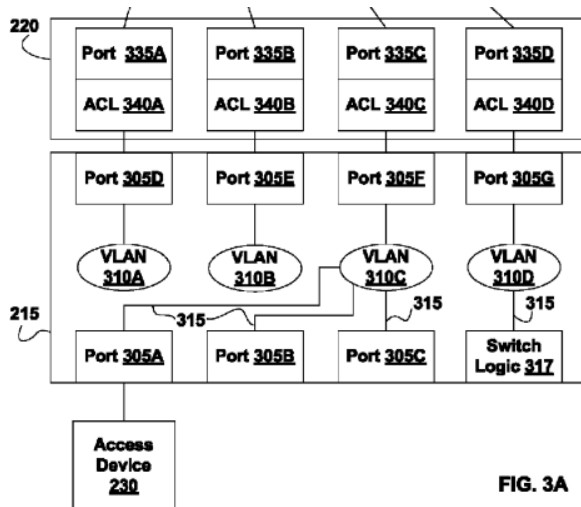


FIG. 3A

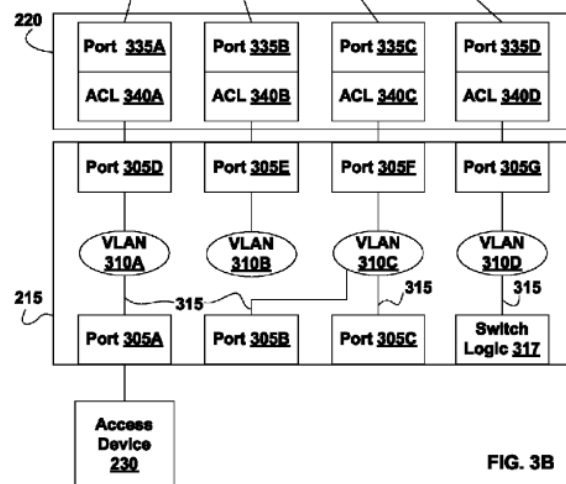


FIG. 3B

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. EX1001, 8:20-27.

By reconfiguring the communication ports of the access point, network traffic for authorized devices (authenticated and audited) can pass to the less-restricted subset of the protected network without first passing through the gatekeeper on the restricted subset of the protected network. Thus, after access has been granted to authorized and audited devices, network traffic bypasses the gatekeeper and reduces bandwidth usage and not requiring the expense of numerous access points and gatekeepers as the 460 Patent teaches was required by the prior art.

IV. THE CITED ART

Petitioner's art is not prior art. Even if so, the references are distinctly different from the patent. Instead of even recognizing the problems in the prior art identified by the patent, the references are merely examples of the art for which shortcomings are identified and overcome by the patent.

A. Krantz

Petitioner's primary reference, Krantz (filed December 6, 2002), relates to “provisioning” and accessing the Internet via an Internet Service Provider (ISP). EX1005, [0005] (“before a computer system can communicate electronically on the Internet, a user of the computer system is often required to register with an Internet Service Provider ... that can authorize access to the Internet.”). Some popular ISPs at that time included America Online (AOL).

Krantz describes the basic concept for accessing virtually any network: “[a] user must first send 'credentials' to the server, which can be a 'Remote Authentication Dial-In User Service ('RADIUS') server.”² *Id.* Such credentials are explained as being “user identifier and password.” *Id.*, [0076].

² RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a

Krantz's purported enhancement relates not to network security but to “automation when **provisioning** a computer system” (EX1005, title). In the late-1990's, "users wishing to access the Internet are subjected to contacting an ISP telephonically and waiting for appropriate access software and/or hardware to be delivered.” *Id.*, [0008]. Krantz explains "many [ISP] services are proprietary and each service may require different computer system configurations and/or registration information for authorizing access to the Internet" *Id.*, [0011]. To provision a user's device with ISP software, Krantz downloads “provisioning files,” rather than waiting for ISP software in the mail. *Id.*, [0032], [0085].

Dodging the “provisioning,” Petitioners rely on an aspect of Krantz explaining how the user's data, after the user is authorized, is directed to the Internet in the context of Virtual Local Area Networks (VLANs).

[A]ccess to resources located on network 413 can be restricted by the use of Virtual Local Area Networks (“VLANs”). In these embodiments, ***networks 411, 412 and 413*** may each be a portion of a different VLAN. ***VLAN aware devices in network architecture 400 can "Tag" data frames*** to indicate to data routing device 414 where the data frames are to be routed. For example, when client 405 is not authorized to access resources located network 413, components in network 411 or logical communication link 433 can ***Tag data frames from client 405*** indicating that the data frames are to be routed to server 415 (or other resources located on network 412). When client 405 is authorized to access network 413, components in network 411 or

network service. RADIUS was developed as an access server authentication protocol and later brought into IEEE 802 standards. <https://en.wikipedia.org/wiki/RADIUS>.

logical communication link 433 can *Tag data frames from client* 405 indicating that the data frames are to be routed to resources on network 413 (e.g., to the Internet) or to resources on network 412 (e.g., server 412) as appropriate.

Id., [0052].

Krantz teaches nothing about device configuration security compliance, and Krantz's authorization occurs when *data from the client* is tagged. I.e., Krantz teaches the VLAN-aware access point relabels *client* data routing information and the client data is routed according to access point's configuration. EX2565, ¶62. Krantz does not disclose, however, *reconfiguring* the access point itself. *Id.*, ¶¶73-82; *see also id.*, ¶¶57-58, 62-64

B. Herrmann

Herrmann discloses a system for security policy enforcement before allowing a client device's access to a protected network. In the same manner as the prior art discussed by the patent, Herrmann teaches including an access point, a Network Access Server (NAS) positioned outside of a protected network and between a client device and protected network resources. *See* Fig. 4.

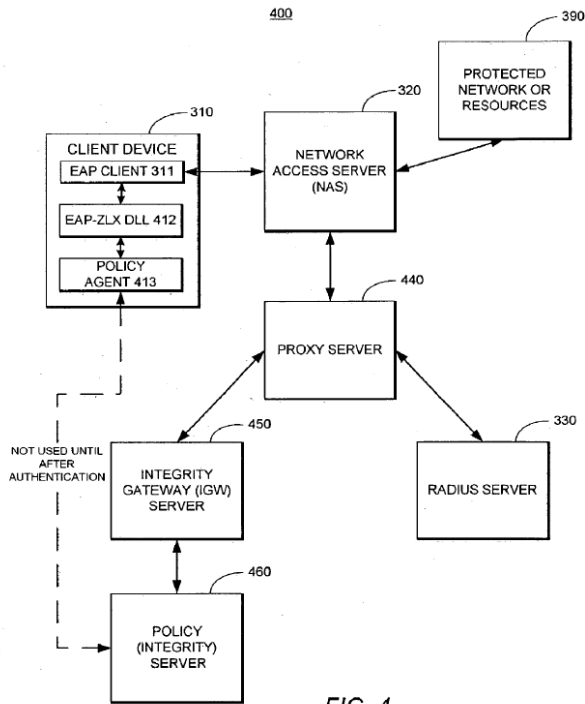


FIG. 4

As shown in Fig. 4 and as Herrmann explains, a client device must first pass a Network Access Server (NAS) to access a protected network. EX1006, [0063]. The NAS then, through a Proxy Server, must authenticate the user with a Radius Server. EX1006, [0073-76]. After authenticating user identity, an agent on the client gathers information about the client device, which is communicated to the NAS, then to the Proxy Server, and then to the Integrity Gateway Server (IGW). EX1006, [0074, 0077-0079]. The IGW then formats and packages the data for transmission to the Policy (Integrity) Server. EX1006, [0096]. This Policy (Integrity) Server then unpacks the data and determines if the client device includes anti-virus software. EX1006, [0068]; EX2565, ¶66

All requests from a client to access the protected network must first pass through the NAS, the authentication server, and the policy server before the client is permitted to access the protected network. EX2565, ¶67. After the session is approved, there is no further explanation in Herrmann of further monitoring of the client device during the session or modifications to the system components in view of the approval process. *Id.*, ¶68.

V. CLAIM CONSTRUCTION

The "words of a claim 'are given their ordinary and customary meaning,'" which "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). The Board must construe disputed terms to the extent necessary to resolve the controversy. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019). Petitioner offers no construction for any claim term, and instead contends under any claim construction the asserted art discloses each claimed limitation. Petition at 7. Petitioner conflates claim construction with patentability, which is improper. *Amazon. com, Inc. v. Barnesandnoble. com, Inc.*, 239 F. 3d 1343, 1351 (Fed. Cir. 2001) ("[T]he first step of an invalidity analysis ... in view of prior art references is no different from that of an infringement analysis. ... [T]he first step is to determine the meaning and scope of each claim in suit.") (quotation omitted).

A. "Protected Network"

A term in each Challenged Claim is "protected network." E.g., claim 1 is directed to a "method of granting access to a protected network." Petitioner provides no definition for this term nor explanation for the plain and ordinary meaning. In computer science, a "protected network" refers to a network environment with implemented security measures to safeguard information from unauthorized access, essentially a secure network that actively protects data and resources through firewalls, access controls, and other security protocols. *See* EX2502; EX2565, ¶¶91-92. There are several requirements for the claimed protective network. *See*, EX1001, claims 1 & 16. These include specified subsets of the protected network:

- a less-restricted subset; and
- a restricted subset having a gatekeeper.

Id.

B. "Reconfiguring the Communication Port"

In the Institution Decision, the Board found "the recited 'reconfiguring the communication port' at least encompasses changing the association between the input port and the output port of the access point." ID at 10. However, the Board did not confirm this phrase was "limited" to changing the connection between the input port and the output port, because this type of reconfiguration was purportedly "not necessarily ... of this type." *Id.* at 11.

The Board misapprehended Patent Owner's arguments in the POPR at 6-7. Patent Owner stated the "plain meaning for 'reconfiguring the communication port of an access point' requires there to be a change to the communication port of an access point; not a change to something else." POPR at 7. In support, Patent Owner referenced the same examples later cited in the Institution Decision, but did not propose a construction limited to these examples. The Board's finding that "reconfiguring the communication port" "at least encompasses changing the association between the input port and the output port of the access point," is consistent with Patent Owner's proposed construction that the limitation requires there to be a change to the communication port of an access point. As before, Patent Owner contends this limitation requires changing the ports of the access point without limiting precisely how they are changed. This is what the plain words of the claim state. Patent Owner further contends redirecting data traffic by re-addressing data frames from the user is *not* reconfiguring the communication port, because the ports themselves are not changed.

VI. GROUND 1: KRANTZ FAILS TO RENDER CLAIMS 1-6, 10-14, 16-22, 27, AND 29-30 OBVIOUS

A. Krantz Does Not Disclose Nor Render Obvious "Reconfiguring The Communication Port ..."

Each of the Challenged Claims requires "reconfiguring the communication port for communicating data between the access device and the less-restricted subset

of the protected network without passing the data through the gatekeeper, when the requirements of the security policy are satisfied." EX1001, 16:15-19.

The claims plainly recite "reconfiguring the *communication port*" – not reconfiguring something else. Krantz does not disclose this. Krantz reconfiguring client data by inserting a Tag Header into the device's data so it is directed according to the access point's predetermined configuration.

Petitioner offers three "Mappings", none of which demonstrates unpatentability by a preponderance of the evidence.

1. Mapping #1

Mapping #1 argues "[p]ort 251 is '*reconfigured*' because it was previously configured to only transfer data to VLAN B" but then transfers data to VLAN C. Pet. at 41. EX2565, ¶75. As the Board determined, Mapping #1 does not teach making changes to a communication port 251 of access point 209. Inst. Dec. at 15; EX2565, ¶ 75. For the reasons cited, the Board's determination was correct.

2. Mapping #2

According to the Institution Decision, Mapping #2 is "Krantz's disclosure of access point 209 'as a VLAN aware device [that] can insert Tag Headers into data frames received from client 205 ... that are to be transferred to VLAN B and/or VLAN C' is a disclosure of reconfiguring the communication port." ID at 16. The Board further stated Petitioner argued "when Krantz's access point switches from

inserting Tag Headers that enable access only to VLAN B to inserting Tag Headers that enable access to VLAN C, communication port 251 is reconfigured. ... [P]ort 251 does the actual insertion of Tag Headers within access point 209." *Id.* The Board then found Petitioner had sufficiently shown "Krantz teaches or suggests a change within the range of possible meanings of reconfiguration by shifting from inserting Tag Headers that enable access to VLAN B to inserting Tag Headers that enable access to VLAN C." *Id.* at 16-17.

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

As background, when establishing a switched network with VLAN aware devices, the VLAN devices must first be configured. *See* EX2565, ¶77. To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation. *Id.* The format of VLAN-tagged frames is defined in the IEEE 802.1Q standard. *Id.* A network device handles an incoming

frame depending on whether the frame is VLAN tagged, and information about the VLAN tags, if any. *Id.*

In Krantz, after a user is authenticated (user ID and password), data fields from the user's device are tagged to allow access to the Internet. The communication ports of the access point are not changed. Rather, data with a particular VLAN ID is directed to the preprogrammed VLAN based on this new tag *in the same manner as rejected Mapping #1*. EX2566.

When a data frame from a device is received, the VLAN-aware device checks to see if it has a VLAN tag that is in the VLAN database. If it does, the data is sent to the assigned VLAN, which in Krantz is VLAN C. If the VLAN does not have a tag, the data frame is sent to where the access point is configured, i.e., preprogrammed, to send untagged data. In Krantz, the data goes to VLAN B. If server 215 determines that data frame is from an authorized user (user ID and password) then the access point, according to its predetermined configuration, inserts a different Tag Header into the data frame to reroute data to VLAN C. Essentially, when the RADIUS server notifies the access point that the user is authorized, the access point changes the label on the user data per its preconfigured programming. EX2565, ¶79.

Notably, however, the configuration of the communication ports of the access point in Krantz are not changed. *Id.*, ¶80. If one considers access point 209 as being

the claimed “access point,” the association of ports 251 and 252 remain unchanged. *Id.* If one disregards Krantz’s actual words and considers data routing device 214 to be the claimed “access point,” there is still no change to the port associations. *Id.* Instead, data bearing a Tag Header assigned to VLAN B or untagged will go to VLAN B, and data bearing a Tag Header assigned to VLAN C will go to VLAN C, just as was the case before the client data was authorized. It is the data frame itself that is changed, not the communication port associations. *Id.*

It was well-understood to POSITA at the time of the invention, that reconfiguration of the ports themselves could be done by changing the port's instructions. For example, rather than being sent to a RADIUS server for user authentication, the communication ports of the access point could be reprogrammed so that incoming data without a tag header are dropped. *Id.*, ¶81. While Krantz teaches changing a data frame's label (tag header), the Challenged Claims require something different, namely, changing how the configuration ports of the access point operate. *Id.*, ¶¶81-82. This is missing entirely from Krantz.

3. Mapping #3

Mapping #3 is essentially a repeat of Mapping #2, except that instead of relying on access point 209 to purportedly meet the claimed access point, Petitioner argues it would have been obvious to combine access point 209 and data routing device 214. Nonetheless, the same Tag Header argument is made for this hindsight

combination of devices. For the reasons discussed with Mapping #2, the insertion of tag headers is not reconfiguring of the communication ports of an access point.

Further, arbitrarily combining these distinct components finds no support in Krantz. Petitioner's own cited portions of Krantz expressly teaches access point 209 and a different component data routing device 214. EX1005, [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's teaching confirms any reconfiguration is of user identification data, not an access point as claimed, because "EAP-Response/Identity messages" expressly relate to user authentication.³

B. Krantz Does Not Disclose A Restricted Subset Of The Protected Network Including A Gatekeeper

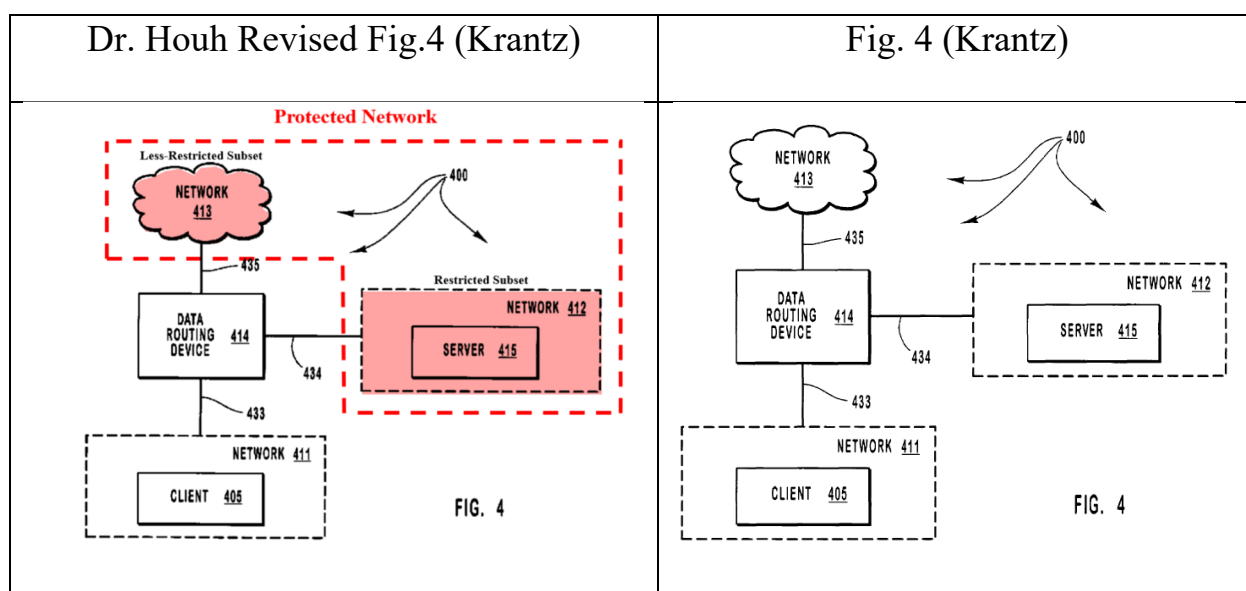
The Challenged Claims specifies a "protected network" that includes a "less-restricted subset" and a "restricted subset." EX1001, 16:5-10, 15-19. The "restricted subset" is also required to "include[e] a gatekeeper." *Id.*

These claimed features provide advantages over the art which included inline gatekeepers that resulted in network bottlenecks and limited scalability. EX1001, Fig. 1, 2:26-42. By establishing "subsets" to the "protected network," and including

³ This understanding is consistent with how POSITA understand EAP-Response/Identity. *See* EX2528.

the gatekeeper on the restricted subset of the network as claimed, these shortcomings are remedied.

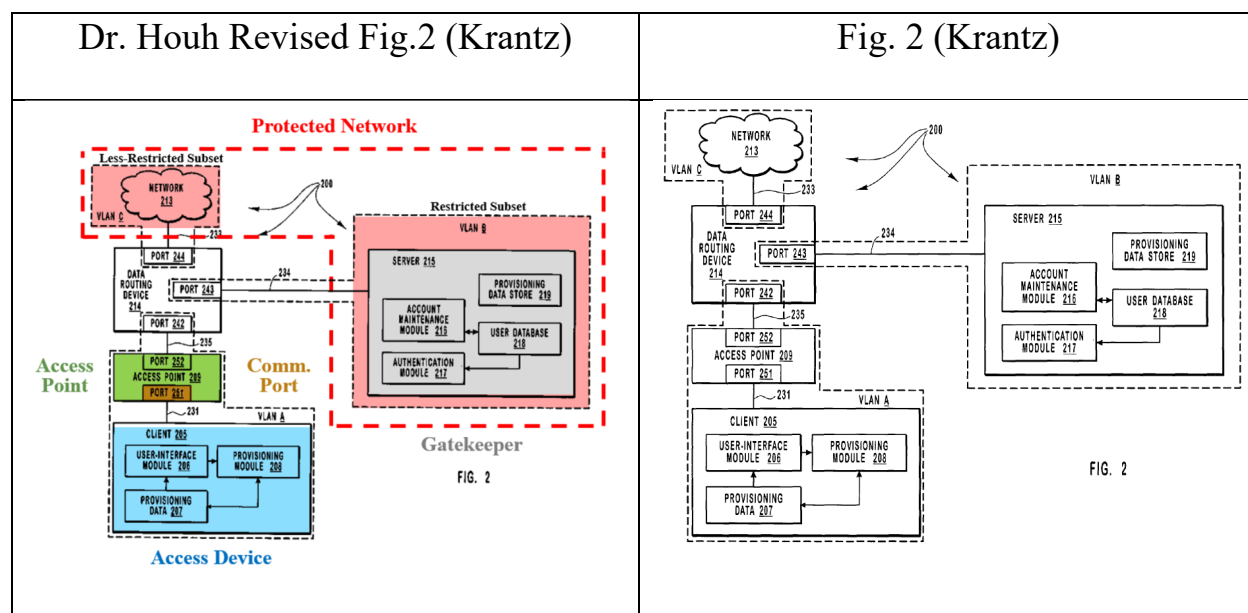
To try and get to “subsets”, Petitioner cobbles together Krantz's teaching of multiple *separate and distinct* networks to fit the Challenged Claims. Petitioner's repackaging is nothing more than Krantz's Fig. 4 redrawn using the claimed invention as a blueprint.



Krantz has two separate and different networks – “Network 413” and “412”. These are not subsets. Indeed, Petitioner admits these are two different networks. Pet. at 22 (“... the combination of second network VLAN C and first network VLAN B constituted a protected network.”). Krantz confirms these two distinct networks: “a network architecture 400 that can provide access to a *first network* while restricting access to a *second network*.” EX1005, [0030]; EX1005, [0060]

("data routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C.").

Regarding Fig. 2, Petitioners similarly misrepresent Krantz's actual disclosure by using the 460 Patent as a blueprint for redrawing Fig. 2 to portray a "protected network" despite Krantz not reciting any "protected network."



As with Fig. 4, Krantz's disclosure of Fig. 2 recites separately "Network 213" and "Server 215." Petitioners are unable to point to any teaching in Krantz of subsets of a protected network. Indeed, Petitioners fail to point to any instance in Krantz where any of a "protected network" or network "subsets" is recited.⁴

⁴ It is further notable that Krantz does not teach with Fig. 4 that Network 412 may communicate directly with Network 413 or with Fig. 2 that network 213 may

One must view a reference for what it teaches, not what it could have with hindsight knowledge—as Petitioner does—of the claimed invention. *Ortho-McNeil Pharmaceutical v. Mylan Labs.*, 520 F.3d 1358, 1364 (Fed. Cir. 2008). Petitioner's redrawn figures are of no moment.

Further, nothing in Krantz suggests this cobbled-together network is “protected.” Rather, “Network 213” is generally just referred to as the “Internet.” EX1005, [0016], [0031] (“A server includes the functionality to authorize clients to access a second network (e.g., the Internet”)); [0012] (“most hotel and airport services authorize Internet access for only a short period of time”); [0010] (“If the registration information is appropriate, the user can be authorized to access the Internet using the service.”); [0006]-[0009]. This is not “protected.” EX2565, ¶¶87-92; EX1001, 5:33-54, 16:5-10, 16:15-19.

Ground 1 also fails because the claims require that “protected network” includes a “restricted subset” having a gatekeeper. EX1001, claim 1. Krantz does not have this either.

With Krantz's Fig. 2, server 215 is disclosed as authenticating a user. EX1005, [0016]. Again, server 215 is not a “subset” of network 213. Instead, Krantz expressly

communicate directly with Server 215. Rather, all communication must pass through a data routing device.

states data routing device 214 is configured to separate network architecture 200 into VLANs A, B, and C, *i.e.*, three distinct networks. EX2565, ¶90; EX1005, [0060]. Thus, server 215 fails to meet the restricted subset of a protected network having a gatekeeper, because it is a separate network from network 213.

Recognizing that Krantz's multiple networks communicating with one another are distinctly different from a protected network with subparts, Petitioner argues as a fallback if the claimed "protected network" must be a single network, Krantz discloses this as well. Pet. at 18. Petitioner mischaracterizes the claims, which require the "protected network" include a "restricted subset" and a "less-restricted subset" where the gatekeeper is on the restricted subset. Even if Krantz discloses a single network embodiment, which is not explained in any detail with either Fig. 2 or Fig. 4, there is no disclosure of a restricted subset of the single network and a less restricted subset of the single network, where a gatekeeper is on the restricted subset. EX2565, ¶91. Further, Krantz's disclosure of authorizing a user to access a "selected computer system" says nothing about whether the network has restricted or less restricted subsets. *Id.*

Petitioner fails to explain how the mere disclosure of a single network teaches that a less-restricted subset of a protected network includes a gatekeeper. Instead, Petitioner's only argument of a gatekeeper on a restricted subset of a protected network is based on Krantz's Fig. 2. As discussed above, however, Fig. 2 only

discloses separate networks VLAN B (Server 215) and VLAN C (Network 213), and it is only Dr. Houh's drawing based on hindsight that revises the reference to disclose a "protected network." Nowhere in Krantz, however, are server 215 and network 213 described as a "protected network" or a "network" at all. EX2565, ¶92. Moreover, even with Krantz's passing reference to a single network, there is no disclosure of placing the gatekeeper inside the network, as opposed to outside the network. *Id.*

Notably, Petitioners rely solely on Krantz for this limitation. This is hardly surprising given that Herrmann also fails to disclose a gatekeeper on a restricted subpart **of the protected network**. Herrmann expressly discloses a "protected network or resources" and the RADIUS server 330 and Policy (Integrity) Server 460 are separate therefrom. See EX1006, Fig. 4 (element 390).

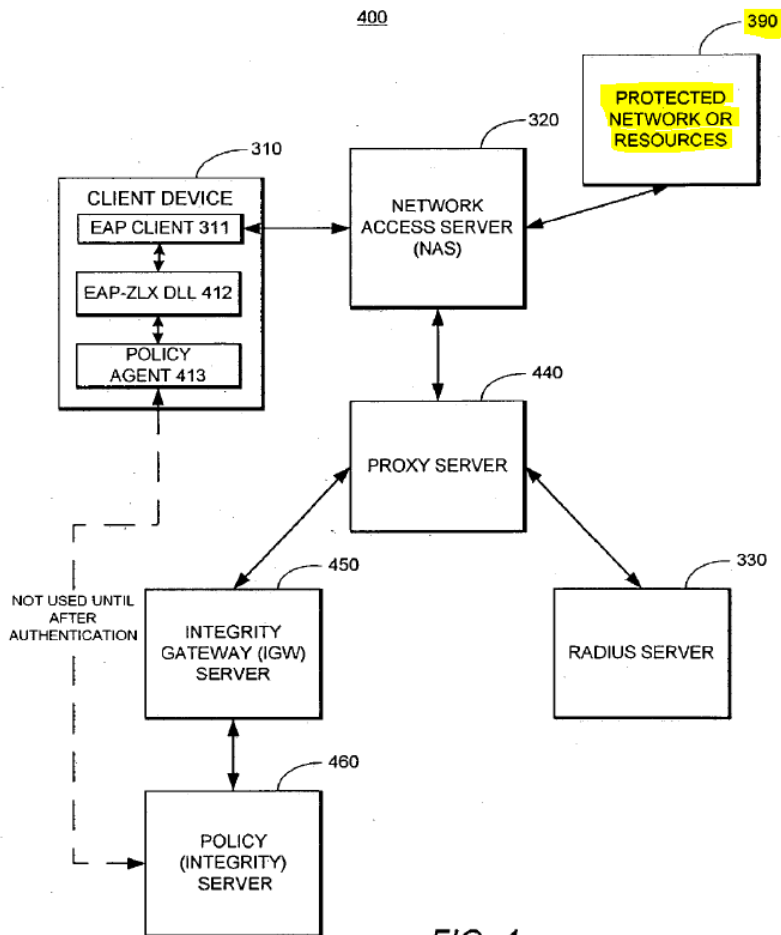


FIG. 4

C. **Krantz Does Not Disclose "Applying A Security Policy To The Access Device" Or "Using The Gatekeeper To Determine If Requirements Of The Security Policy Are Satisfied By The Access Device" Or "System Data"**

Each of the Challenged Claims require: “applying a security policy to the access device in response to the request” as well as “using the gatekeeper to determine if requirements of the security policy are satisfied by the access device.” Further, dependent claims 3-6 and 18-21 require obtaining and/or using “system data”. Krantz only discloses user authentication, and fails to disclose anything about

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

“Thus, Petitioner has not shown sufficiently that Krantz teaches the step of auditing the device in accordance with a security policy.” IPR2025-0549, Paper 13 (Inst. Denial) at 14.

“The ‘350 patent distinguishes between user authentication using a username and password and application of a security policy.” *Id.* at 12.

“Although the ‘350 patent describes both user authentication and application of a security policy as being carried out by a gatekeeper, this is accomplished in separate process steps... . user authentication and application of a security policy are separate processes.” *Id.* at 12-13.

"As such, Petitioner relies on essentially the same analysis based on Krantz for teaching two processes that are expressly distinguished in the specification of the '645 patent. Because Petitioner fails to develop a coherent unpatentability theory with respect to both the 'audit' and 'authentication' limitations, we find that Petitioner has not shown sufficiently that Krantz teaches or suggests 'a gatekeeper... to: formulate an audit request." IPR2024-00678, Paper 14 (Inst. Denial) at 15.

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

Accordingly, the Board relied on Herrmann's teaching of applying a security policy to the access device and “system data” claims; not Krantz. *Id.* As discussed below, such teaching in Herrmann still does not render the claims unpatentable.

Nonetheless, Ground 1 must fail.

VII. GROUND 2 – KRANTZ AS MODIFIED BY HERRMANN FAILS TO RENDER CLAIMS 1-6, 10-14, 16-22, 27, AND 29-30 OBVIOUS

A. All Claims

Krantz’s authentication-only disclosure dooms Ground 1. Ground 2 argues Herrmann fills the gap through disclosure of "applying a security policy" or "using the gatekeeper to determine if requirements of the security policy are satisfied by the access device." Not only has Petitioner failed to meet its burden, but the evidence definitively shows why a POSITA would not want to, and in some instances, would not be able to, combine Krantz and Herrmann.

1. Petitioners Have Failed To Demonstrate The Combination

With respect to the combination, the Petition offers only bald rationales:

- “A POSITA would recognize that checking for anti-virus software would merely be an *additional item* for authentication module 217 (of server 215) to *check* in the authentication process already disclosed by Krantz.” Pet. at 59; Ex. 1203, ¶ 52.
- “Krantz’s authentication module, which *compares the credentials of a user against a database* (e.g., a user-identifier and password), as modified by Herrmann, would additionally *compare* a virus protection program on an access device against approved antivirus programs. Ex. 1203, ¶ 52.
- “... implementing these techniques into a combined Krantz/Herrmann system as doing would involve *minimal changes* to the existing Krantz system.” Pet. at 65.

Petitioner's argument essentially distills to: Krantz says user authentication is a good thing and Herrmann says device auditing is a good thing, so one would be motivated to put them together by “checking” and “simple” or “minimal” software modifications. But Petitioners’ bald conclusion are divorced from the art.

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

With regard to authenticating a user, Krantz merely references established authentication paradigms of user-names, passwords, and RADIUS protocols. Indeed, Krantz’s touchpoints on authentication is little more than checking whether the user has an paid-up account with the ISP.

“It may be that a presented user-interface includes only “YES” and “NO” controls for authorizing further credit card payments or other electronic payment options.” EX1005, [0103].

“A user may be presented with an interface to enter information for registration (e.g., name, room number, credit card number, etc.). If the registration information is appropriate, the user can be authorized to access the Internet using the service.” EX1005, [0010].

None of this is related to the claimed invention including “applying a security policy to the access device,” obtaining and using “system data” or accessing a “protected

network.” *See, e.g.*, EX1001, 16:2-19, 16:61-17:12. Accordingly, Petitioner have failed to meet its burden.

In actuality, the evidence demonstrates that Krantz and Herrmann would not be combined because, as the 460 Patent explains: “The method used to support auditing functionality over the existing 802.1x protocol implementations is complicated and not an obvious variation of the 802.1x protocol.” EX1001, 14:5-7. As Dr. Cole explains, authentication and auditing and/or applying a security policy to the access device was complicated. EX2565, ¶118. In particular, he explains that the security infrastructure for authentication was distinct from that for security policy (or auditing) enforcement. *Id.* For example, authentication generally required a RADIUS server, supplicant, and authentication protocols. *Id.*, ¶¶119-21. These were incompatible with processing, analyzing, and handling policy information. *Id.*, ¶121. In contrast, auditing functionality (*e.g.*, applying a security policy to the access device) required a separate infrastructure. *Id.*

This complexity is the reason why Petitioner Cisco tried, but could not figure out a NAC solution for “applying a security policy to the access device” or obtaining and using “system data.” *See* Section VIII(A). It is also one of the reasons why InfoExpress took almost a year to conceive, work diligently, and reduce it to practice. *See* Section IX(D). Further, as set forth below, Krantz and Herrmann themselves confirm such a combination would make little sense. Accordingly,

Petitioner failed to meet its burden demonstrating unpatentability based on the combination of Krantz and Herrmann.

2. Herrmann Confirms “Applying A Security Policy To The Access Device” Would Not Have Been “Minimal,” “Simple”, or Merely An “Additional Check” For Krantz’s Server

Petitioners say combining Herrmann with Krantz would merely require “simple” and “minimal” modifications to Krantz’s sever 215. Pet. at 65. They provide no analysis or no reasoning.

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

Tellingly, Herrmann has its own authentication “RADIUS server 330,” and does not use it for policy enforcement. EX1006, FIG. 4. Rather than simply change the RADIUS 330 as shown in FIG. 3, Herrmann designs its own unique policy evaluation infrastructure. EX1006, FIG. 4 (“Policy (Integrity) Server 460,” “Integrity Gateway (IGW) Server 450, Proxy Server 440). Herrmann’s new policy infrastructure also adds a “policy agent 413” and custom EAP-ZLX extension. EX1006, (comparing FIG. 3 and FIG. 4). The reason for this new policy infrastructure—as Herrmann suggests—is that you cannot modify the RADIUS

server to evaluate a security policy of the access device. *See* EX2522⁵ (RADIUS Specification RFC 2865 stating: “A forwarding server MAY need to modify attributes to enforce local policy. *Such policy is outside the scope of this document...*”)

Recognizing that this was not possible, Herrmann creates a complex infrastructure of servers, components, and its own proprietary protocols to conduct a policy evaluation.⁶ Herrmann needs a system of interconnected servers including a “Proxy Server,” “Integrity Gateway Server,” and “Policy Server.” EX1006, FIG. 4. All of these are specifically designed to work with one another to “unwrap,” (Id., [0082]-[0083], FIG. 7A, 708) “wrap,” (Id., [0090], FIG. 7A, 705) “transform” (Id., [0095], FIG. 7B, 714), “reformat” (Id., [0096], FIG. 7C, 718), and send and receive various data packet transmission and messaging.

⁵ Herrmann incorporates RFC 2865 entitled Remote Authentication Dial In User Service (RADIUS) by reference. EX1006, [0009].

⁶ Notably, while Herrmann’s complex infrastructure discloses a policy evaluation, this infrastructure runs afoul of other key claim requirements including “reconfiguring” the communication port and doing so “without passing data through the gatekeeper.” Put differently, Herrmann does not solve the “bottleneck” issue.

Not only that, but Herrmann creates a new and unknown proprietary data packet – EAP-ZLX—to transmit “policy data” within its construct of servers. EX1006, [0058], [0062], [0064]; EX2565, ¶¶133-35 (Cole saying EAP-ZLX is not known); EX2449, 259:9-275:9 (Dr. Houh agreeing that “EAP-ZLX” was not and is not known).

The policy data in EAP-ZLX would be rejected by Krantz’s RADIUS server 215. *See* EX2522 (“NAS is not required to implement all of these service types, and ***MUST treat unknown or unsupported Service-Types as though an Access-Reject*** had been received instead.”).

This is confirmed by Dr. Cole who explained the different infrastructures of authentication and those of policy evaluation was different and complex. Dr. Cole explains why in a typical policy evaluation, there are many types, different ways to check, file histories and registries. EX2565, ¶143; *see also* EX2449, 195:4-197:20 & 246:19-247:24 (Dr. Houh testifying that there are “thousands” of networking protocols and each must be specifically designed to work with other components in the network).

Even if Krantz’s server 215 could work with Herrmann, applying a security policy regarding antivirus software would not “merely be an additional item for authentication module 217 (of server 215) to check in the authentication process...” Pet. at 59; Ex. 1003, [0052]. The reason is because a “check” would be insufficient.

Rather, “applying a security policy to the access device” requires an evaluation that the anti-virus software is actually running and cannot be bypassed. In fact, mere “checking” results in the industry-wide problem of spoofing or the presenting of deceptive policy information.

Cisco itself admitted that RADIUS servers that merely “check” are susceptible. See EX2445, 1 (Cisco: “RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by an on-path attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response...”). Further, Cisco’s early NAC attempt failed in part because of this problem. EX2446 (“Cisco’s NAC can be fooled into thinking non-compliant PCs actually meet the security posture NAC is designed to enforce”); EX2447.

Accordingly, a POSITA would not be motivated to combine Krantz with Herrmann.

3. Herrmann’s Client-Side System Teaches Away From Combination with Krantz’s Server-Side System

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

For example, Krantz’s server 215 (the alleged “gatekeeper”) is nothing more than a centralized RADIUS server. EX1005, [0058]. This means that it

receives authentication data originating from various client sources. Upon receipt, the server processes the authentication data. EX2565, ¶143.

In contrast, Herrmann is a client-side solution. EX1006, [0062]. That means the client device processes the information. As incorporated by reference⁷, Herrmann explains that for enforcement of anti-virus policies: **“In accordance with the present invention, a central filter is not employed. Instead, the present invention provides a client-side filter** that is controlled by the centralized authority as long as the centralized authority has a way of enforcing non-compliance.” EX2521, 12:45-53. Thus, a centralized solution (e.g. non-client side)—like that in Krantz—would not work. EX2565, ¶¶147-58.

Herrmann explains the shortcomings of a server-side solution:

"Both strategies are based on a centralized filter mechanism, with most of the filtering work being performed at the server (as opposed to the individual client PCs). Such an approach is problematic, however. Because of the centralized nature of firewalls and proxy servers, each approach extracts **significant performance penalties**. During operation of a typical system employing either approach, a single server might have to do the filtering work for hundreds or even thousands of PCs or workstations. **This represents a major bottleneck to overall system performance.**" EX2521, 2:38-47.

⁷ Herrmann incorporates by reference U.S. Patent 5,987,611 (EX2521) for explaining the **“policy definition and enforcement”** for, *inter alia*, **anti-virus policies**.). EX1006, [0070].

"As another problem, ***centralized filter architectures are missing vital information*** to correctly interpret the data packets because the underlying protocols were designed for effective data transfer and not for data monitoring and interception. *Id.*, 2:59-63.

“There are still other disadvantages to centralized filtering. The approach is difficult to configure and administer. The task of setting up different rights for different users, workstations, or workgroups, for instance, is particularly difficult.” *Id.*, 3:4-8.

A reference teaches away "when a person of ordinary skill ... would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant." *Ricoh Co., Ltd. v. Quanta Computer Inc.*, 550 F.3d 1325, 1332 (Fed. Cir. 2008). Here, Herrmann specifically teaches away from including a device auditing function on a server based application, such as Krantz's authentication server.

This is hardly surprising from a technical viewpoint. There are critical differences between the codebases for client-side and server-side enforcement solutions. In particular, client-side codebase tends to be lightweight with lower processing memory. EX2565, ¶156. Server-side code is more intensive and requires significant resources. *Id.*, ¶157. In addition to defeating Herrmann's goal of defeating the centralized "bottleneck," combining these codebases would make little sense and not be compatible. Thus, it would not be obvious to combine Herrmann's client-side approach into Krantz.

B. Dependent Claim 22

In addition to the reasons discussed, Petitioner fails to demonstrate dependent claim 22 is unpatentable because neither Krantz nor Herrmann disclose a “program... to monitor security status of the access device after reconfiguring the communication port...” EX1001, 17:35-18:1.

For Ground⁸ 2, Petitioner relies on Krantz’s “authentication”: “[i]t may be that the server 215 sets a session timeout, such as, for example, one hour, after which access point 209 will request client 205 to *re-authenticate*.” Pet. at 77. As discussed, Krantz’s “authentication is not “applying a security policy to the access device.” Pet. at 36-40. Moreover, Krantz does not disclose “monitor[ing]” the security status of the access device.” Indeed, mere “re-authentication” (asking someone once again for a username and password) based on a predetermined “timeout” period would have nothing to do with “monitoring security status of the access device.”

As backup, the Petition argues Herrmann’s “IA_HEARTBEAT” constitutes an “agent executing on the access device” including “after reconfigur[ation].” Pet. at 79. The Petition stops short of asserting the “heartbeat” is something that would “monitor security status.” The reason, as Herrmann explains, is because a heartbeat

⁸ Petitioners’ Ground 1 does not challenge claim 22.

is nothing more than a “status message.” EX1006, [0080]. Such a message does not contain substantive policy data about a “security status.” Rather, it only carries minimal information to confirm if an access point is connected and active (i.e., proof of life). EX2565, ¶¶161-63. By contrast, the claimed “security status” relates to whether the device configuration is still compliant with the security policy. CITE. A heartbeat message confers no such information. Moreover, the claim requires that the communication is between the gatekeeper and the agent. In contrast, Herrmann’s heartbeat “status message” is “sent from the client directly to the policy server.” EX1006, [0080].

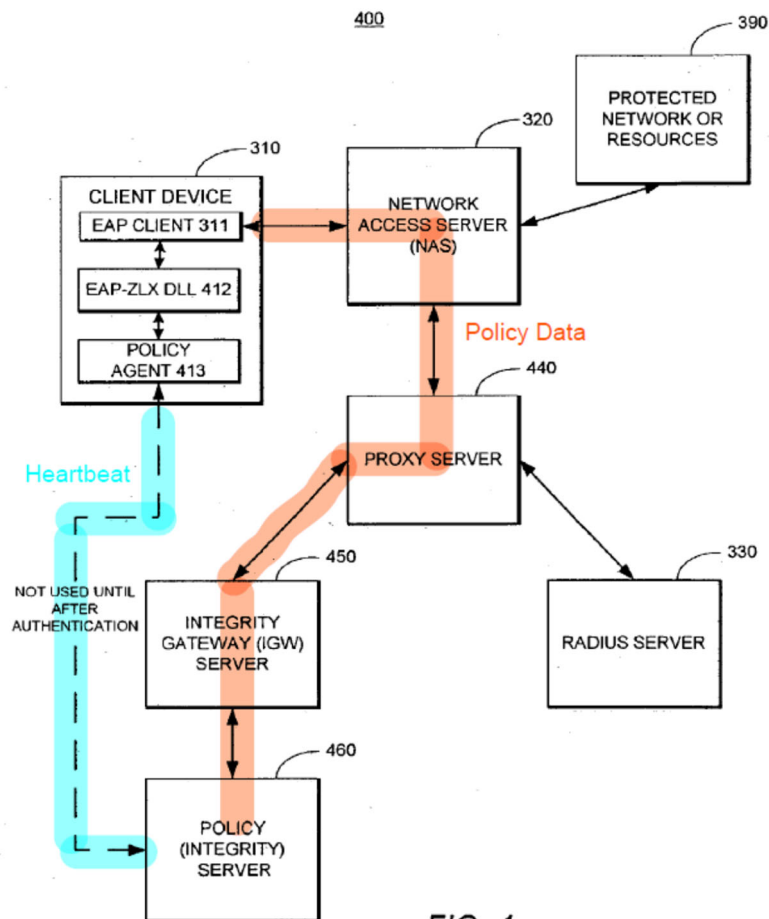


FIG. 4

Accordingly, this is an additional reason for the validity of dependent claim 22.

C. Dependent Claim 27

Petitioners' rely solely on Krantz to disclose the limitation "wherein the program is further executable to update the access device when requirements of the security policy are not satisfied." Pet. at 56. As discussed above, Krantz only discloses authentication, and thus cannot teach this limitation.

Notwithstanding, Petitioner's "provisioning files" argument is equally wrong. The Petition cites Krantz's disclosure of "provisioning files [] for gaining full access [to] resources located on the second network." Id. But "provisioning files" are not related to "requirements of the security policy." Provisioning files merely give devices software necessary to connect to and operate on a network. EX1005, [0013]-[0014]. These files ensure that the device can access network services without requiring manual configuration by the end-user. EX2565, ¶¶166-69; EX1005, [0112] ("[d]uring the registration process with the ISP, the computer system may download provisioning files for the wireless hotspot."). As discussed above, Krantz explains different ISP's have different proprietary software to enable a user to access the Internet. Section IV(A). Rather than require a user to wait for software to arrive in the mail, Krantz's provisions the user by automatically providing the software when establishing an account. Relative to claim 27, these provisioning files have

nothing to do with compliance with a security policy. Instead, they are nothing more than the ISP software, e.g., AOL's mailed software.

Even if “provisioning” files did relate to “requirements of the security policy,” the claim requires that the “the program is further executable to update the access device.” Petitioner’s proposed gatekeeper of Krantz (e.g., RADIUS server 215) takes no part in administering provisioning files and the Petition does not say it does.

With respect to Herrmann, Petitioner makes no express analysis of claim 27. Pet. at 58-65. This is not surprising because Herrmann makes no such disclosure. At best, Herrmann only discloses: “The rules enforced by the policy server 460 may also be changed from time to time by a *user or administrator.... a network administrator* may require all users access the network to implement a virus definition update (e.g. DAT file) that is targeted at a particular virus.” EX1006, [0071]. Just like in Krantz, Herrmann does not teach or suggest how a “program” would conduct the “update the access device when the requirements of a security policy are not satisfied.” Accordingly, claim 27 is valid for this additional reason.

VIII. OBJECTIVE EVIDENCE DEMONSTRATES NON-OBVIOUSNESS

Objective indicia of nonobviousness include: (1) commercial success, (2) copying, (3) industry praise, (4) skepticism, (5) long-felt but unsolved need, and (6) failure of others. *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling U.S., Inc.*, 699 F.3d 1340, 1349-56 (Fed. Cir. 2012). “[E]vidence of

secondary considerations may often be the most probative and cogent evidence in the record. It may often establish that an invention appearing to have been obvious in light of the prior art was not.” *Transocean*, 699 F.3d at 1349.

There must be nexus between the merits of the claimed invention and the objective evidence. *Volvo Penta of the Ams., LLC v. Brunswick Corp.*, 81 F.4th 1202, 1210 (Fed. Cir. 2023). Nexus is typically shown by: (1) a presumption, or (2) direct evidence of the unique characteristics of the claimed invention. *Id.* A patent owner is entitled to a presumption of nexus if the patentee shows the asserted evidence is tied to a specific product and the product “is the invention disclosed and claimed.” *Fox Factory, Inc. v. SRAM, LLC*, 944 F. 3d 1366, 1373 (Fed. Cir. 2019).

A. At the Time of the Invention and at Present, InfoExpress’s Products Embody the Claimed Inventions and are Coextensive with the Patent.

InfoExpress’s CyberGatekeeper LAN (“CG LAN”) and CGX products embody the claims of the ‘460 Patent and are coextensive with them. Striegel Decl., ¶¶44-46 and Appx. C (claim chart). To be sure, the CG LAN and CGX products are marked with the InfoExpress patents. EX2451-EX2457; EX2459-2468. Accordingly, there is a presumed nexus between the secondary consideration evidence below and the ‘460 Patent claims.

In addition, the evidence demonstrates [REDACTED]

[REDACTED], is narrowly targeted to not only the claim limitations themselves, but

to the inventive combination of claim elements that Petitioners concede are missing in Krantz and supplied by Herrmann (“system data” and “applying a security policy to the access device.”).

[REDACTED]

⁹ The claims of the ‘460 Patent are directed to both authentication and auditing in accordance with a security policy. *E.g.*, claims 1, 16 (and dependents) (auditing, i.e. “applying a security policy to the access device . . .”); claims 2, 17 (authentication); claims 3-6 and 18-21 (system data); Paper No. 13 at 21 n.5.

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹⁰ Such industry praise from Cisco itself (a top potential competitor) is further evidence of nonobviousness. *See Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1053 (Fed. Cir. 2016) (noting “if there is evidence of industry praise of the claimed invention in the record, it weighs in favor of the non-obviousness of the claimed invention,” and further stating that “internal documents from the patentee’s top competitor represent important admissions, *acknowledging the merits of the patented advance over the then state of the art* and can be used to establish industry praise”); EX2470 (Cisco: “InfoExpress appear[ed] quite far along in [its] product development.”)

The image consists of a single, uniform black rectangle that fills the entire frame. There are no discernible features, text, or patterns other than the solid black color.

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[Redacted text line]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹¹ *See also* EX2485; EX2486 at 14-17; EX2487; EX2488.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

12 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The image consists entirely of a solid black field with no visible features, text, or patterns.

¹⁴ See also EX2501 (cover email).

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

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

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹⁶ Citing EX2530, EX2551, EX2552, EX2531, EX2532, EX2533, EX2534, EX2535, EX2536, EX2537, EX2538; EX2539; EX2540; EX2550; EX2553; EX2554.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

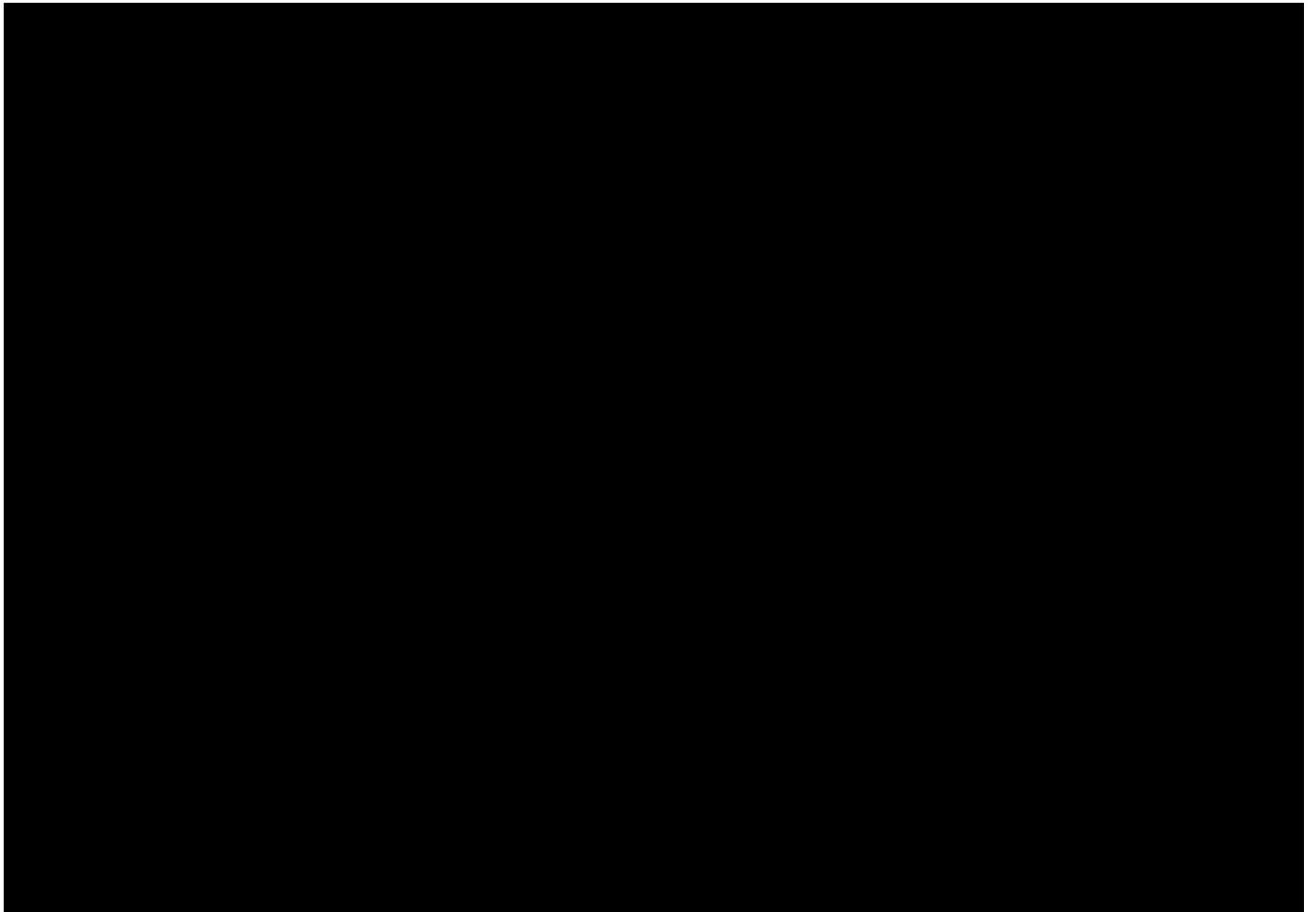
[REDACTED]

[REDACTED]

[REDACTED]

¹⁷ Cisco had multiple occasions to observe the CG LAN, including at least the following:

- **The NAC Developers Conference** in December 2004. EX2508; EX2509.
- **The Systems Engineer Virtual Team (SEVT)** in April 2005. EX2510; EX2511.
- **Networkers World of Solutions** in June 2006. EX2512-EX2514.
- **Cisco Networkers EMEA** in December 12-15, 2005. EX2515; EX2516.
- **Cisco Networkers Live 2007**. EX2517.



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

IX. ALL GROUNDS: NEITHER REFERENCE CONSTITUTES PRIOR ART

Neither reference constitutes prior art because the inventors conceived of the invention before the effective dates and exercised reasonably continuous diligence in reducing the 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).

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 reference until reduction to practice. *ATI Techs. v. Iancu*, 920 F.3d 1362, 1369 (Fed. Cir. 2019). "No general standard, by which diligence can be estimated, has been established by the law, nor, in the nature of things, is such a standard possible." *Id.* at 1374.

For reasonably continuous diligence, an inventor need not work on reducing the invention to practice daily, and periods of inactivity do not automatically vanquish a claim of reasonable diligence. *Id.* at 1369. An attorney's work preparing

a patent application can demonstrate diligence. *Perfect Surgical Techniques v. Olympus America*, 841 F.3d 1004, 1009-1012 (Fed. Cir. 2016).

Inventor declarations submitted to establish conception and diligence must be corroborated. *Id.* 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. *Id.* 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 Inventions Prior to the Critical Dates of Both References.

Petitioner asserts Krantz has an effective date of December 6, 2002 (Pet. at 7) and Herrmann has an effective date of March 13, 2003.¹⁸ *Id.* at 10. InfoExpress conceived of the claimed invention earlier.

¹⁸ 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

On November 14, 2002, co-inventor Lee e-mailed "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification" (EX2011) demonstrating that the claimed inventions were conceived of at least by then. EX2012; EX2564 (Supplemental Lum Declaration), ¶12; EX2520; EX2429 (Lee Declaration), ¶13.

Conception is demonstrated in Dr. Smith's claim chart mapping the EX2011 to the Challenged Claims as set forth in EX2009. EX2007.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

submit, mention, or analyze its provisional filing in the Petition. Notwithstanding, the Herrmann provisional date is still later than the November 14, 2002 conception and is not prior art regardless.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

InfoExpress exercised reasonably continuous diligence up to and through at least the filing of U.S. Patent Application No. 60/513,080 on October 21, 2003. The filing of that application constitutes constructive reduction to practice. Section IX(D); EX2007; EX2010.

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.

This was groundbreaking because preexisting security technologies did not include the implementation of auditing support functionality over authentication protocols such as 802.1x.

InfoExpress diligently reduced the inventions to practice from conception until constructive reduction to practice on at least October 21, 2003. This diligence is shown by evidence including:

- i. emails;
- ii. technical specifications and analyses; and
- iii. the declarations of InfoExpress CEO Stacey Lum (EX2564) and Alice Lee (EX2429).

As further detailed in the diligence calendar (EX2568), 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 (finding that Patent Owner's evidence did "not point to the remotest suggestion of abandonment or setting aside" where a calendar demonstrated activity on the majority of days in the diligence period and a declaration summarized 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).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

██████████

[REDACTED]

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

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

- [REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]

1 [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

[REDACTED]

1 [REDACTED]

[REDACTED]

○

■

■

■

■

■

■

■

■

██████████

114

██████████

[REDACTED]

████████████████████

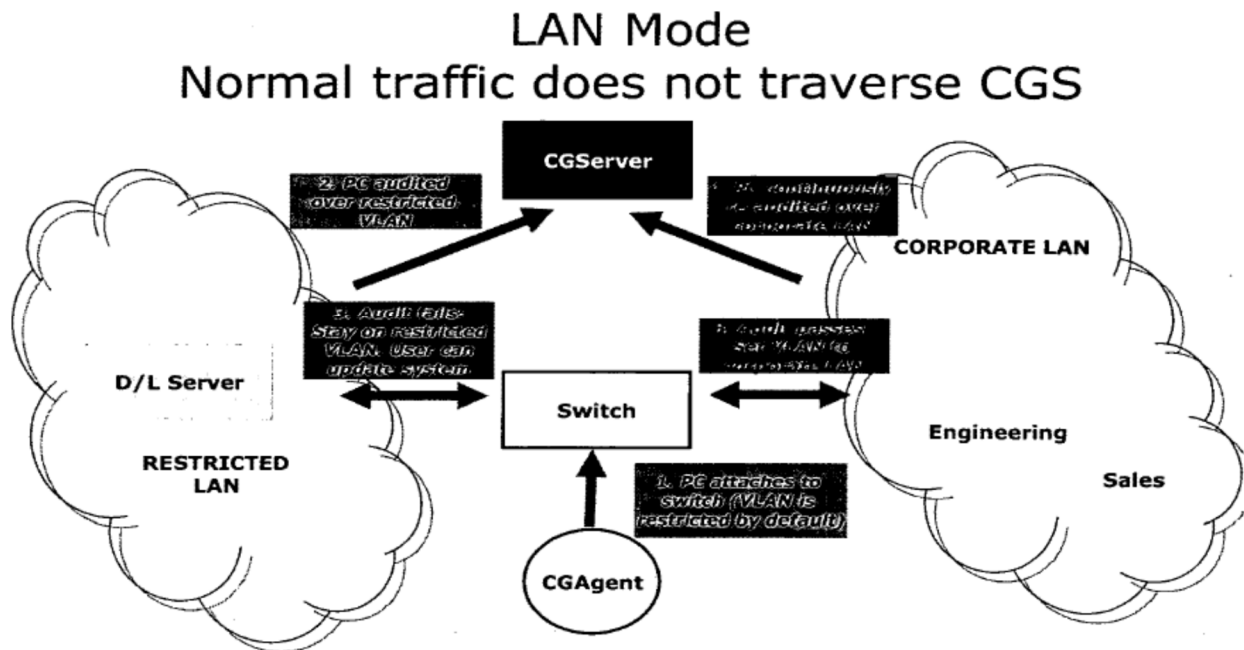
████████████████████

[REDACTED]

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

As discussed by Dr. Smith (EX2007 & EX2010), 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.

For example, the EX2006 disclosed a protected network including a “RESTRICTED LAN” and “CORPORATE LAN” (the latter mapping to the recited “less-restricted subset”) as discussed, *e.g.*, at EX2010 at 1-12 and EX2006 at 19 (excerpted below).



As depicted, “an AP may be programmed to prohibit access by the PC until ... an audit with the software agent with the GK passes”. *E.g.*, at EX2010 at 3 (citing EX2006 at 6). The gatekeeper (CGServer) sits outside of the Corporate LAN; that

is, it is in the “restricted subset” and accessible for before an audit passes (or on audit failure) as discussed, *e.g.*, in EX2010 at 2-12.

EX2006 discusses auditing throughout, *e.g.*, in steps 2 and 3 depicted above. As depicted above and discussed, *e.g.*, at EX2010 at 21, “Normal traffic [*e.g.*, traffic after successful audit] does not traverse CGS [the gatekeeper]”. Instead, the switch is reconfigured after a successful audit so that traffic can flow to the right to the “CORPORATE LAN”.

The evidence demonstrates diligence on the part of the inventors to a constructive reduction to practice.

X. CONCLUSION

For these reasons, Patent Owner respectfully requests the Board reject the Petition.

Respectfully submitted,

Dated: <u>January 13, 2025</u> Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	<u>/Joseph M. Kuo/</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@saul.com Joseph M. Kuo (Reg. No. 38,943) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 joseph.kuo@saul.com Brian Landry (Reg. No. 62,074) Saul Ewing LLP 131 Dartmouth Street, Suite 501 Boston, MA 02116 Tel: (617) 912-0969 Brian.Landry@saul.com Andrew Schwerin (Reg. No. 72,999) Saul Ewing LLP 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186 Tel: (215) 972-7184 Andrew.Schwerin@saul.com Counsel for Patent Owner
--	---

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

The undersigned hereby certifies that the foregoing complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the document contains 14,000 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: **January 13, 2025**

/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: **January 13, 2025**

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