

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 PRELIMINARY RESPONSE

TABLE OF CONTENTS

	<u>PAGE</u>
I. Introduction.....	1
II. The '460 Patent	1
A. Date of Invention.....	1
B. Person of Ordinary Skill in the Art (POSITA)	1
C. Overview of the '460 Patent	2
III. Claim Construction.....	5
IV. Petitioners' Cited References	7
A. Krantz	7
B. Herrmann.....	10
V. Krantz Alone (Ground 1) or the Combination of Krantz and Herrmann (Ground 2) Fail to Render Obvious Any of the Challenged Claims.....	12
A. Ground 1: Krantz Alone Fails To Disclose All The Claimed Limitations.....	12
1. Krantz Fails To Disclose “Reconfiguring The Communication Port For Communicating Data Between The Access Device And The Less-Restricted Subset Of The Protected Network”	12
2. Krantz Fails To Disclose “Without Passing The Data Through The Gatekeeper, When The Requirements Of The Security Policy Are Satisfied”	20
3. Krantz Fails To Disclose “Applying A Security Policy To The Access Device”	23
4. Krantz Also Fails To Disclose The Other “Applying A Security Policy To The Access Device” Limitations From The Dependent Claims.....	27
B. Ground 2: Krantz in Combination with Herrmann Fails To Render Obvious The Challenged Claims.....	28

VI.	All Grounds: Neither Reference Constitutes Prior Art	28
A.	Legal Standard.....	29
B.	The Inventors Conceived of the Claimed Inventions Prior to the Critical Dates of Both Krantz and Herrmann.....	31
C.	The Inventors Exercised Reasonably Continuous Diligence Up and Through Constructive Reduction to Practice.	32
D.	The Filing of U.S. Provisional Patent Application Serial No. 60/513,080 on October 21, 2003 Constitutes Constructive Reduction to Practice.....	40
VII.	Conclusion	40

TABLE OF AUTHORITIES

FEDERAL CASES

<i>ATI Techs. v. Iancu</i> , 920 F.3d 1362 (Fed. Cir. 2019)	29, 33, 40
<i>Bey v. Kollonitsch</i> , 806 F.2d 1024 (Fed. Cir. 1986)	30
<i>Monsanto Co. v. Mycogen Plant Sci., Inc.</i> , 261 F.3d 1356 (Fed. Cir. 2001)	29, 33
<i>Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.</i> , 841 F.3d 1004 (Fed. Cir. 2016)	29, 30
<i>SAS Institute Inc. v. Iancu</i> , 138 S.Ct. 1348 (2018)	31
<i>Tyco Healthcare Grp. v. Ethicon Endo-Surgery, Inc.</i> , 774 F.3d 968 (Fed. Cir. 2014)	29

FEDERAL STATUTES

35 U.S.C. § 102(e)	29, 31
35 U.S.C. § 103	1
35 U.S.C. § 112	40
35 U.S.C. § 119(e)	40

OTHER AUTHORITIES

<i>Globus Med., Inc. v. Depuy Synthes Prods., LLC</i> , No. IPR2015-00107 (P.T.A.B. May 1, 2015)	31
<i>LG Elecs., Inc. v. Wi-LAN Inc.</i> , No. IPR2018-00704, Paper No. 14 (P.T.A.B. Sept. 5, 2018)	28
<i>Sequenom v. Leland Stanford Junior Univ.</i> , No. IPR2013-00390 (P.T.A.B. Nov. 25, 2014)	29

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

I. Introduction

Patent Owner InfoExpress, Inc. submits this Patent Owner Preliminary Response to the Petition for *Inter Partes* Review by Petitioners related to claims 1-6, 10-14, 16-22, 27 and 29-30 (the "Challenged Claims") of U.S. Patent 8,051,460 (the '460 Patent"). Patent Owner respectfully requests the Board reject the Petition and not institute an *inter partes* review of the Challenged Claims. Patent Owner submits the Grounds presented and the prior art relied on by Petitioners fail to render any of the Challenged Claims unpatentable under 35 U.S.C. § 103 because the prior art fails to disclose or render obvious all of the limitations of the Challenged Claims. Moreover, the art relied on by Petitioners does not qualify as prior art.

II. The '460 Patent

A. Date of Invention

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

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

A POSITA in at the time of the invention would have had a working knowledge of computer network security art. A POSITA would have had a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems

and cybersecurity, or a person with a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields.

C. Overview of the '460 Patent

The '460 Patent is directed to a novel and seminal approach to a security solution for controlling access to a protected network. Before Patent Owner's inventions, network security required multiple "gatekeepers" placed directly between clients, i.e., users, and the network. 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, and the guard would also need to direct them where to go. These preexisting solutions required individual checking of each device's hardware and software, *e.g.*, virus protection and operating systems, for granting access. This consumed substantial network resources, resulting in a bottleneck. EX1001, 2:35-41.

An example of the prior art architecture is shown in annotated FIG. 1 of the '460 Patent.

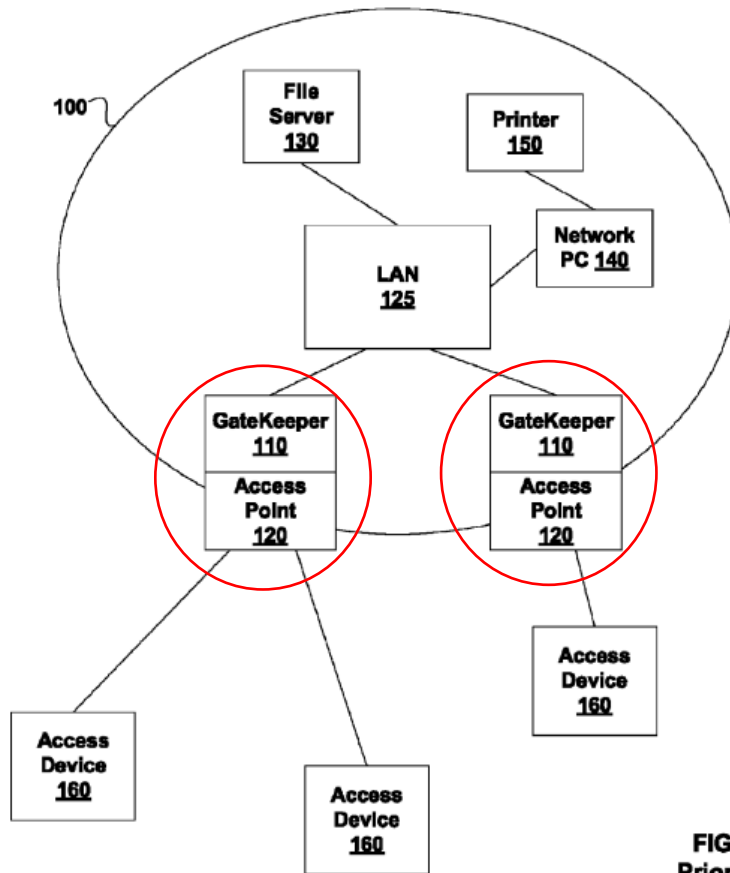
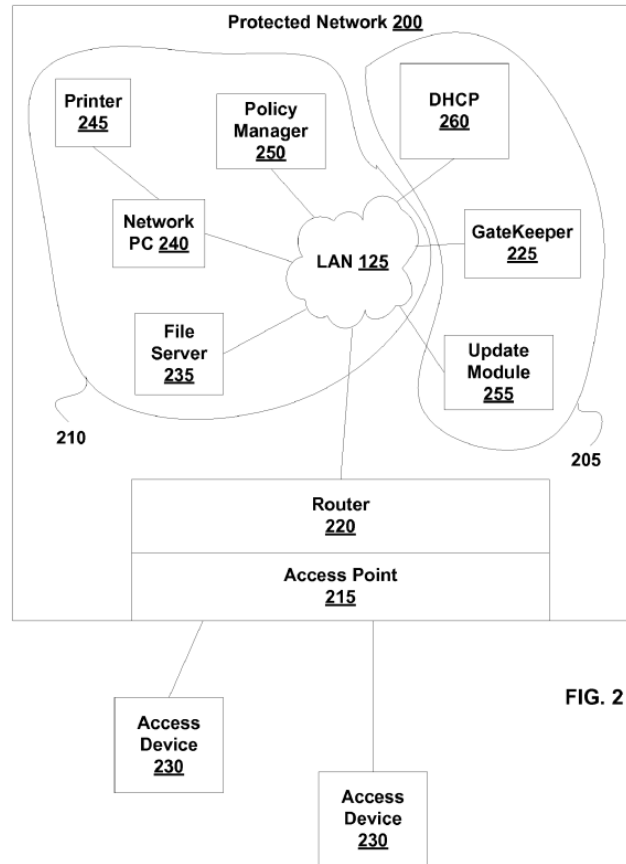


FIG. 1
Prior Art

The protected network 100 included two Gatekeepers 110, each associated with a different instance of an Access Point 120. With large corporate networks including many access points, the "use of one instance of GateKeeper 110 to support numerous instances of Access Device 160 is limited by bandwidth and required sophistication (e.g., cost) of GateKeeper 110." EX1001, 2:35-38. The gatekeeper then becomes a limiting bottleneck on the bandwidth of the system. EX1001, 2:38-41.

The '460 Patent addressed this particular problem with a new, novel, and non-obvious approach that relieves computer resources by reconfiguring an access point for previously authorized devices to access a protected network.

By way of example, the '460 Patent discloses a protected network that includes a restricted subset with a gatekeeper and one or more less-restricted subsets.



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

A key feature of the '460 Patent is that rather than require all device access requests to pass through the gatekeeper, the access point itself is reconfigured. The Detailed Description give the following example of reconfiguring the access point.

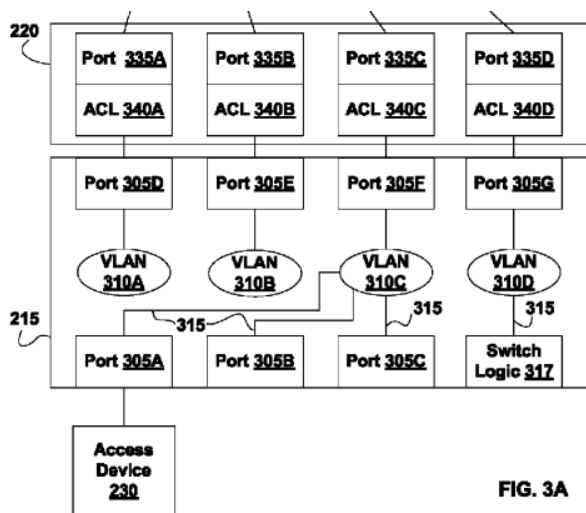


FIG. 3A

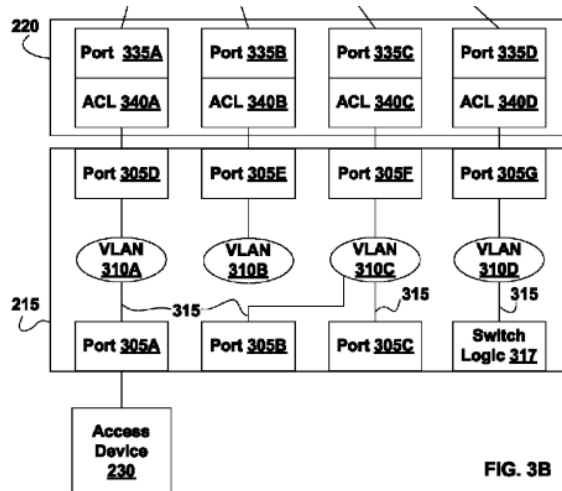


FIG. 3B

Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F. EX1001, 8:20-27.

By reconfiguring the access point, network traffic for certain devices can pass from the access device to the less-restricted subset of the network without needing to pass through the gatekeeper. Thus, after access has been granted, most network traffic does not need to pass through the gatekeeper.

III. Claim Construction

Petitioners assert claims should be given their ordinary and customary meaning as understood by a POSITA, and contends the Board need not expressly

construe the claim terms. Petition at 7. Petitioners, however, avoid providing any explanation and deviate from the plain meaning for any claim term is.

Patent Owner contends the claims should be given their plain meaning in the context of the intrinsic evidence.

Reconfiguring an Access Point

The Challenged Claims require "reconfiguring the communication port." With regard to "reconfiguring," one must first look to the words of the claim. "Reconfiguring" means to rearrange something into an altered form or to configure something in a new way.¹ And it must be for a "communication port."

The '460 Patent specification is consistent with this plain meaning: "The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1001, 3:24-29.

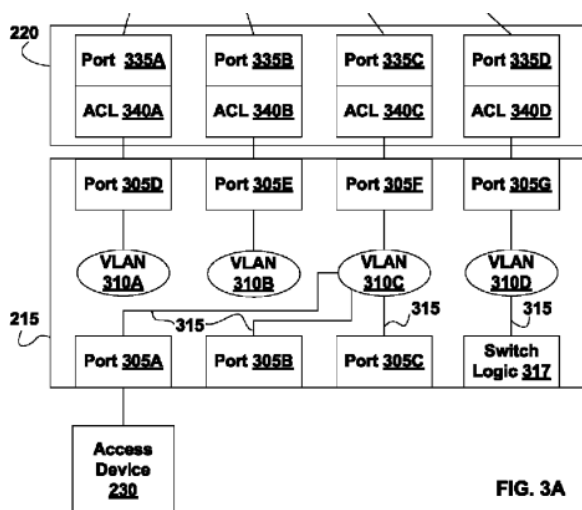


FIG. 3A

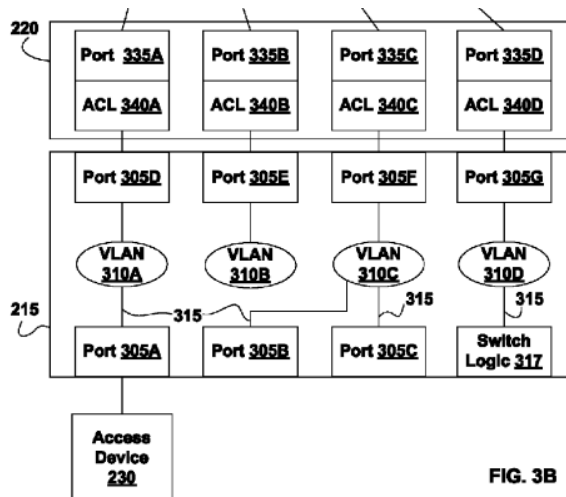


FIG. 3B

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

This “reconfiguring” is shown above and explained by the ‘460 Patent:

Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. VLANs 310A-310D are logical associations between members of Ports 305A-305G. Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other. These associations are illustrated in FIGS. 3A and 3B by Lines 315. EX1001, 7:66–8:8.

Thus, 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.

IV. Petitioners' Cited References

Petitioners' cited references, Krantz and Herrmann, are not prior art to the Challenged Claims as discussed herein. In addition, Krantz and Herrmann are readily distinguished from the Challenged Claims, and merely illustrate examples of the earlier network security approaches improved upon by the '460 Patent.

A. Krantz

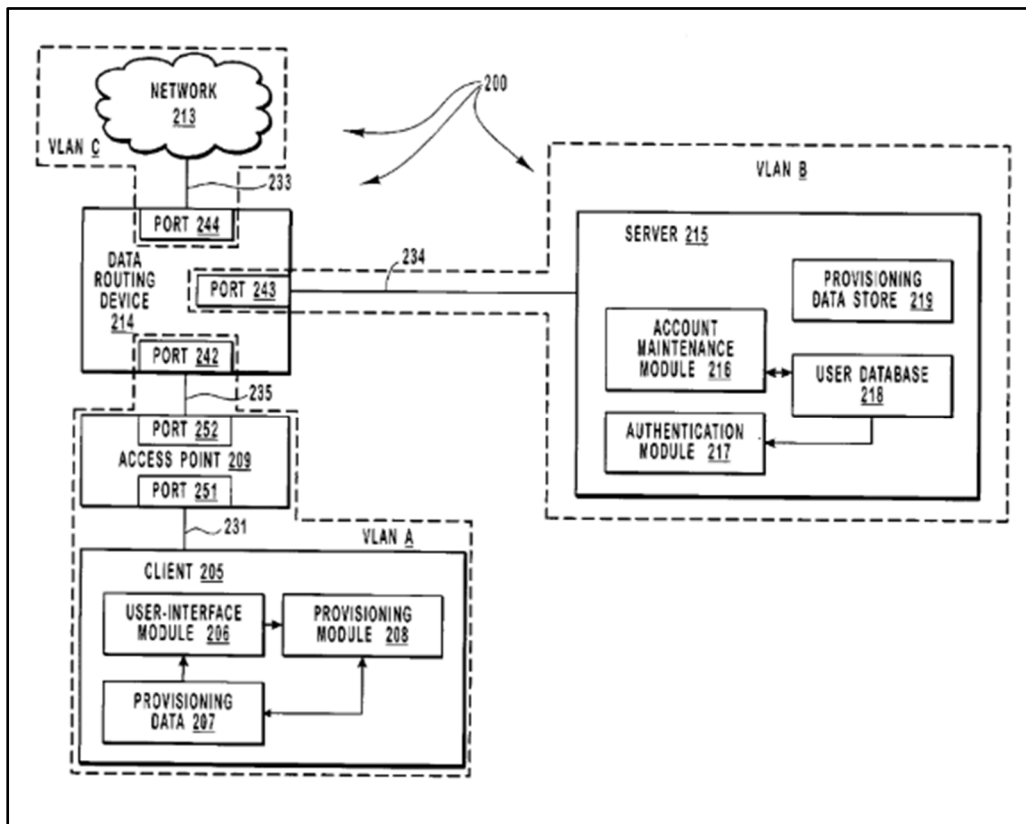
Petitioners primary reference is U.S. Patent No. 2004/0111520 ("Krantz"), which was filed on December 6, 2002. Krantz is described as follows:

A computer system attempts to authenticate with a server to gain authorization to access a first network. It is determined by the server that the computer system is not authorized to access the first network. The computer system is given authorization to access a second network for at least the purpose of downloading files (e.g., signup and configuration files) needed to access the first network. A user-interface for receiving user-entered signup information is automatically

presented at the computer system. A first schema-based document including user-entered information is transferred to the server. If the server determines that the user-entered information is appropriate, a second-schema document, which includes an indication of authorization to access the first network (e.g., a user-identifier and password), is received. A third schema-based document is executed at the computer system to compatible configure the computer system for accessing the first network.

EX1005, Abstract. Krantz discloses the concept wherein upon the failure of a computer system to authenticate to one network, the computer system is permitted to access a second network for the limited purpose of downloading files by a server.

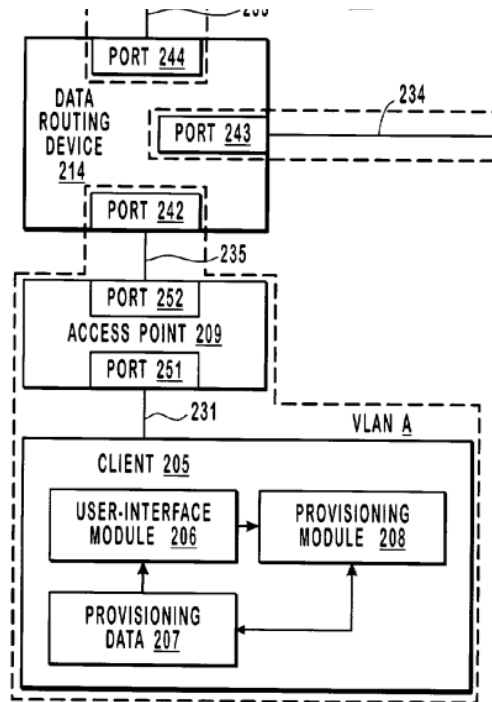
EX2001 (Cole. Decl.), ¶¶ 47-49



EX1005, cover page. Krantz discloses:

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

EX1005, [0016]. As shown, in the excerpted portion of Fig. 2 from Krantz, an access point 209 is identified and the client communicates via access point 209 through port 251. The access point 209 then sends data to data routing device 214 via port 252. This data routing device directs data through either port 244 or port 243.



There is no teaching in Krantz of changing any configuration for any port, and more specifically, Krantz does not teach changing the configuration of any port of the access point 209. EX2001, ¶ 59. Instead, all data pass ports 251 and 252 and then pass to the data routing device.

B. Herrmann

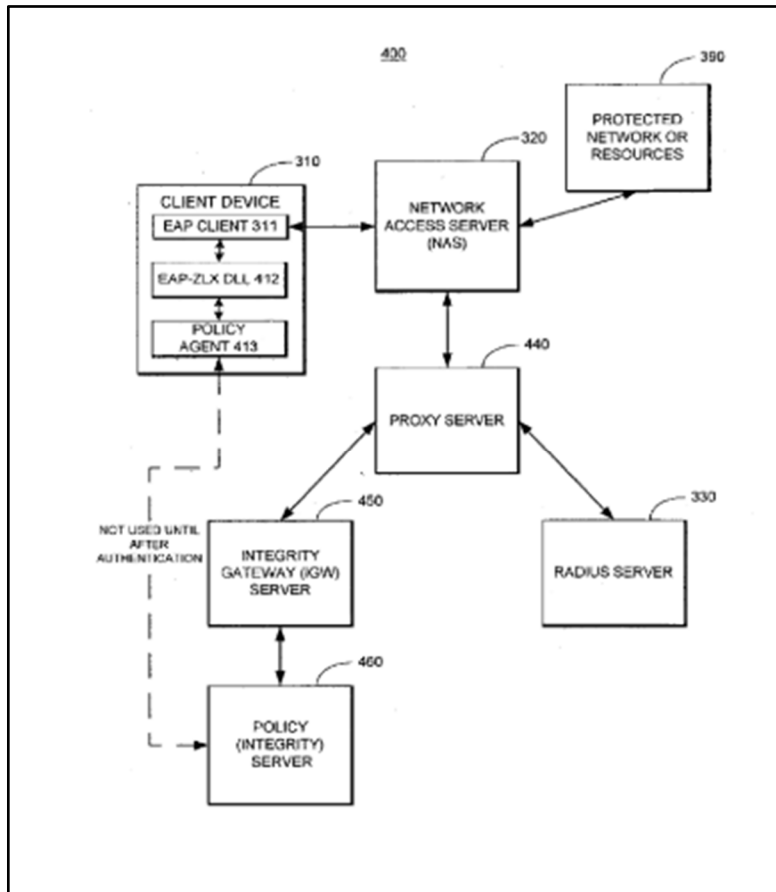
Petitioners cite to U.S. Patent App. No. 2004/0107360 ("Herrmann") in Ground 2 to be used in combination with Krantz. Herrmann was filed on March 3, 2003, and published on June 3, 2004.

Herrmann describes a system as follows:

A system and methodology for policy enforcement during authentication of a client device for access to a network is described. A first authentication module establishes a session with a client device requesting network access for collecting information from the client device and determining whether to authenticate the client device for

access to the network based, at least in part, upon the collected information. A second authentication module participates in the session with the client device for supplemental authentication of the client device for access to the network. The supplemental authentication of the client device is based, at least in part, upon the collected information and a policy required as a condition for network access.

EX1006, Abstract; EX2001, ¶¶ 50-53. Like the prior art discussed in the '460 Patent, Herrmann utilizes servers between the client device and the protected network, and any attempts to access the protected network must first be checked for security policy compliance by at least a Network Access Server (NAS), which would create the bottleneck problems. EX2001, ¶ 53



EX1006, Fig. 1, *compare id. to* EX1001, Fig. 2.

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

Petitioners' Ground 1 asserts invalidity of each of the Challenged Claims based on Krantz alone. Petitioners' Ground 2 asserts invalidity of each of the Challenged Claims based on Krantz in combination with Herrmann. For both Grounds, key claim limitations are expressly missing. Institution must be denied.

A. Ground 1: Krantz Alone Fails To Disclose All The Claimed Limitations

Petitioners' Ground 1 relies on Krantz alone for obviousness. Krantz, however, fails to disclose the following limitations: (1) “reconfiguring a communication port of an access point” (2) “without passing the data through the gatekeeper, when the requirements of the security policy are satisfied; (3) “applying a security policy to the access device” and (4) various dependent claim limitations. Accordingly, the petition for institution of an IPR based on Ground 1 should be denied.

1. Krantz Fails To Disclose “Reconfiguring The Communication Port For Communicating Data Between The Access Device And The Less-Restricted Subset Of The Protected Network”

The ‘460 Patent claims require "reconfiguring an access point to allow access to the less restricted subset of the network in response to the security policy audit." The specification explains that: “[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.”

EX1001, 3:26-29. Thus, there are changing pathway assignments for the ports of the “access point.”

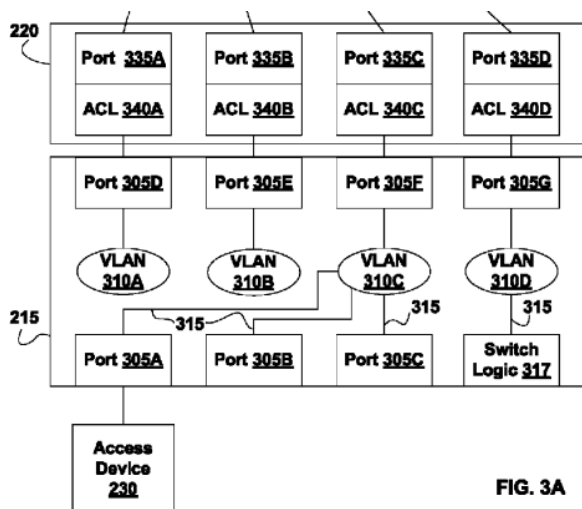


FIG. 3A

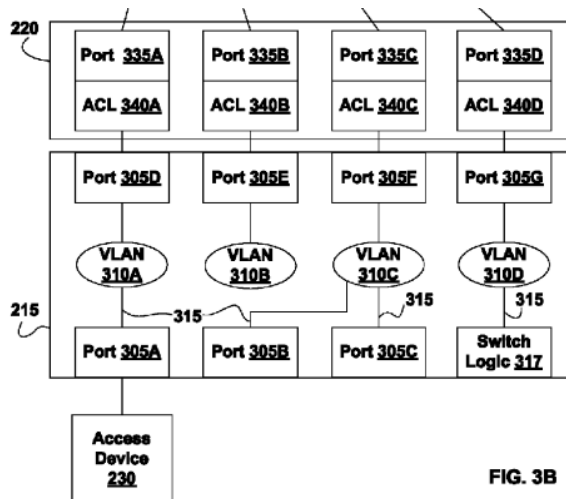


FIG. 3B

Communication received at one member of Ports 305A-305G is directed internally to another member of Ports 305A-305G via a member of VLANs 310A-310D. VLANs 310A-310D are logical associations between members of Ports 305A-305G. Typically, any members of Ports 305A-305G that are configured to be associated with the same member of VLANs 310A-310D are in bi-directional communication with each other. These associations are illustrated in FIGS. 3A and 3B by Lines 315. EX1001, 7:66–8:7.

...

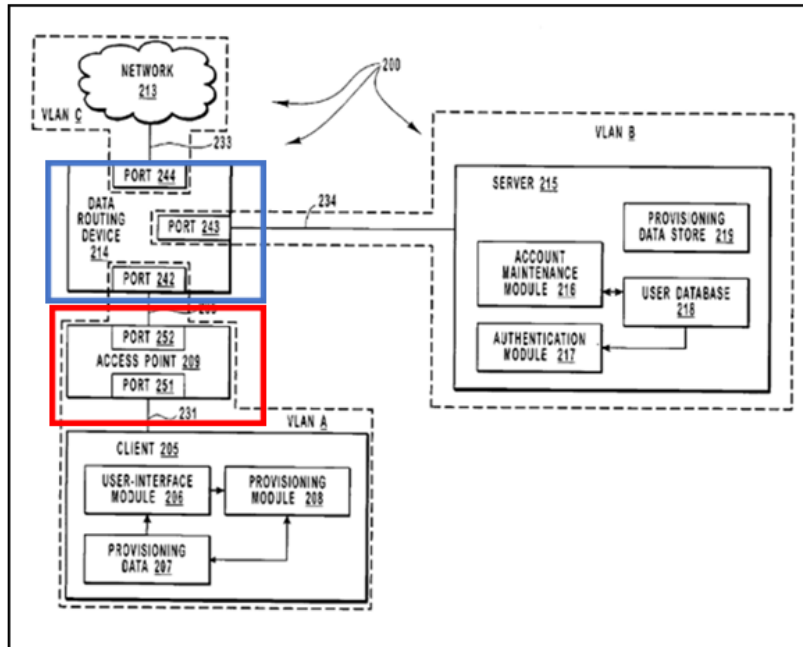
Switch Logic 317 is configured for configuring and reconfiguring members of Ports 305A-305G responsive to received commands. For example, by receiving an appropriate command, Switch Logic 317 is configured to reconfigure Port 305A to be associated with VLAN 310A, as illustrated in FIG. 3B below. In this configuration, data received at Port 305A is directed to Port 305D via VLAN 310A, rather than to Port 305F. EX1001, 8:20–27.

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

Petitioners' Mapping #1:

Petitioners' first argument for how Krantz supposedly discloses “reconfiguring of a communication port” requires one to ignore what Krantz actually discloses. Petitioners argue that “[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. This, however, does not support making any changes to a communication port 251 of access point 209.

Petitioners argue that “access point 209” (red annotation) is configured to transfer data from client 205 via port 251 to data routing device 241 via port 252. Pet. at 27. Petitioners then argue that communication ports of a different element (not the access point)—the data routing device 214 (blue annotation)—permits data to first communicates with VLAN B. After authentication of the user, Petitioners argue that “[p]ort 251 is “reconfigured” because it was previously configured to only transfer data to VLAN B”; then it can transfer data to VLAN C. ” Pet. at 41-42.



The '460 Patent is clear: "[t]he reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN." EX1001, 3:24-29..

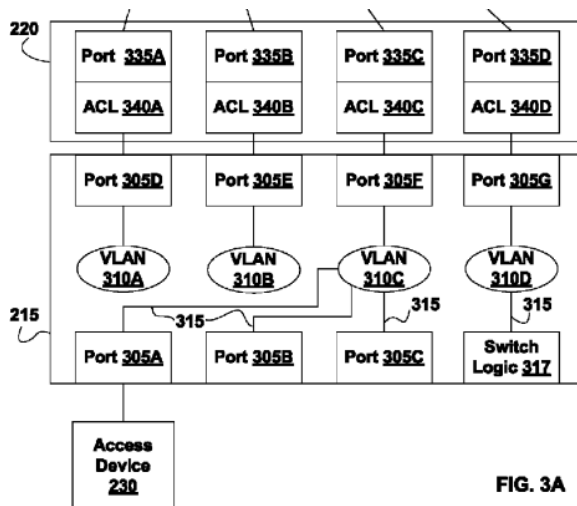


FIG. 3A

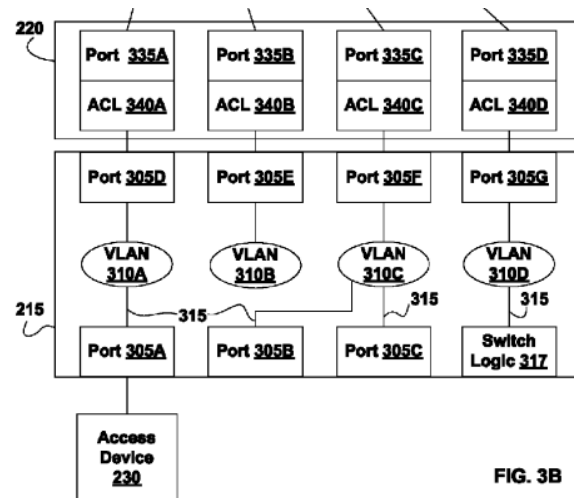


FIG. 3B

This means that depending on the "reconfiguration" the same port may send data to different locations. For example, as shown in FIG. 3A of the '460 Patent

above, port 305A of access point 215 sends data via 315 to VLAN 310C. In FIG. 3B, however, that same port 305A has been “reconfigured” to send data to VLAN 310A.

Krantz has no “reconfiguration.” Instead, the Krantz ports send data to the same location (e.g. port 243 to VLAN B and port 244 to VLAN C). Further, Krantz explains that it is not the access point, but rather, the data routing device 214 which directs the traffic and acts as the gatekeeper to direct users either to VLAN B or VLAN C. EX1005, [0060]; EX2001, ¶59.

In contrast, Krantz only discloses the use of “tag headers” with respect to the user identification.

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 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). If an authenticated user of client 205 is authorized to access resources located on VLAN C (e.g., the user is up to date on payments for their account), client 205 can then be authorized to access resources located on VLAN C.

EX1005, [0073]-[0076].

Thus, the Krantz “data routing device 214” directs the traffic to either the VLAN B or VLAN C based on consideration of the user’s identification information. There is no change or “reconfiguring” of the ports of the access point 209 disclosed in Krantz. EX2001, ¶ 59. As such, Mapping #1 fails.

Petitioners' Mapping #2:

Petitioners' second argument avoids any action on the “access point” altogether. Rather, it asserts that “[a]ccess point 209 can be configured as a VLAN aware device and can insert Tag Headers into data frames received from client 205 ... that are then transferred to VLAN B or VLAN C.” Pet. at 44 (quoting EX1005, [0064]. As discussed above, the Krantz “tag headers” are different from the claimed “reconfiguring of the communication port.”

Recognizing this deficiency, Petitioners try to combine Krantz with three additional references in an attempt to transform “tag headers” into “reconfiguring the communication port. *See* Pet. at 28-29 (§ VIII.A.1.iv) (citing Exs. 1008, 1009, and 1010). None of these references, however, save Krantz from the fact that its clear disclosure is that the tag header is inserted into “data from client 205:”

A tagged data frame is a data frame that includes an indication, such as, for example, a Tag Header, that identifies a VLAN and/or frame classification associated with the tagged data frame. A Tag Header can be inserted into a data frame by a VLAN aware device to indicate to data routing device 214 a VLAN ID of the VLAN from which a tagged data frame was received. For example, access point 209 can insert a Tag Header into data from client 205 to indicate to data routing device 214 that the data was received from VLAN A. A Tag Header can also

include other control information that can be used by data routing device 214 to classify a corresponding data frame. An untagged data frame is a frame that does not include a Tag Header. A port VLAN ID ("PVID") may be used to indicate a VLAN from which an untagged data frame was received. For example, untagged data frames received at port 243 may be classified as being received from VLAN B.

EX1005, [0061].

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

Lastly, the '460 Patent explains that "GateKeeper 225 *reconfigures the communication port* of Access Point 215." EX1001, 10:42-43. For Krantz, Petitioners claim that the "[d]ata routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs..." Pet. at 32. Even assuming this constitutes "reconfiguring," Petitioners take the position that it is the RADIUS server 215—not the "data routing device 214"—that is the gatekeeper. *See* VI. A. 2 below. Accordingly, Mapping #2 fails.

Petitioners' Mapping #3:

Petitioner's third argument appears to be that it would have been obvious for one to take the access point 209 and the data routing device 214 and combine these

so that the Tag Headers can be configured to either be directed to VLAN C or VLAN B. There are numerous flaws with such an argument.

As discussed configuring client data with tag headers is not reconfiguring of the access point. Rather, it is only manipulating “data from client 205.” As such, the different data paths of Krantz still require the data routing device to check user identification information, namely, the tag header.

Even if “tag headers” could be reconfiguration, Krantz expressly recites separate access point 209 and data routing device 214. Arbitrarily combining these separate and distinct component finds no support in Krantz. To the contrary, Petitioners' own cited portions of Krantz expressly teaches access point 209 and a different component data routing device 214. 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.”). This teaching from Krantz further confirms that any reconfiguration is of user identification data, not an access point as claimed, because “EAP-Response/Identity messages” expressly relate to user authentication.² Lastly, even it were possible to combine access point 209 and data routing device

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

214, this would not resolve the bottleneck problem with the prior art, such as Krantz. Instead, all traffic would still go through access point 209 and data routing device 214, which acts as a gatekeeper. See EX1005, [0060].

2. Krantz Fails To Disclose “Without Passing The Data Through The Gatekeeper, When The Requirements Of The Security Policy Are Satisfied”

The Challenged Claims require “reconfiguring the communication port for communicating data... without passing the data through the gatekeeper.” Indeed, the ‘460 Patent explains that “[a] disadvantage of the use of Gatekeeper 110, as practiced in the prior art, is that all communications between the Access Device 160 and LAN 125 pass through the GateKeeper 110.” EX1001, 2:30-32. The problem is that for large networks, this is a “significant burden” on bandwidth, expense, and scalability. EX1001, 2:35-38.

Petitioners argue that the server 215 of VLAN B is the gatekeeper. Pet. at 37. But Krantz’s server 215 is just a RADIUS server. EX1005, [0058] (“In some embodiments, server 215 logically represents a Remote Authentication Dial-In User Service (“RADIUS”) server.”). This is the same type of server that the ‘460 Patent identifies as prior art. EX1001, FIG. 5 (“EAP over 802.1x/RADIUS”); 8:29-33 (“This communication between GateKeeper 225 and Switch Logic 317 may be accomplished using ...RADIUS (Remote Authentication User Dial-In Service)...”)

The '460 Patent explains that the claimed gatekeeper cannot be merely a RADIUS server. By way of example, the '460 Patent describes the claimed “gatekeeper” as much more:

- “using the gatekeeper to *determine if requirements of the security policy* are satisfied by the access device.” EX1001, claim 1.
- “GateKeeper 225 *reconfigures the communication port* of Access Point 215” EX1001, 10;42-43.

Krantz’s RADIUS server 215 does not perform those functions.

Petitioners avoid the fact that Krantz identifies its “data routing device 214” as what could more closely be considered a gatekeeper. This, however, is a problem because “data routing device 214” is no better than what the '460 Patent explains did not work in the prior art. EX1001, 2:30-32. (“A disadvantage of the use of Gatekeeper 110, as practiced in the prior art, is that all communications between the Access Device 160 and LAN 125 pass through the Gatekeeper 110.”)

Krantz explains that it is the “data routing device 214” that acts closer to a gatekeeper. For example, the “data routing device 214” controls data traffic.

As depicted in network architecture 200 data routing device 214 is connected to network 213, server 215, and access point 209 by corresponding logical communication links 233, 234, and 235 respectively. Network 213 can be virtually any type of network, such as, for example, a corporate or enterprise-wide network or the Internet. Data routing device 214 can be a device capable of grouping computer systems together in a single broadcast domain based on criteria other than physical location (e.g., a physical location on a particular side of a router). Thus, data routing device 214 can be configured to separate computer systems into different VLANs. As depicted in FIG. 2, data

routing device 214 has been configured to separate network architecture 200 into VLANs A, B, and C. Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.

EX1005, [0060].

Similarly, in Fig. 4, which is identified as "a network architecture that can provide access to a first network while restricting access to a second network" that data routing device 414 again controls data traffic.

As depicted in network architecture 400 data routing device 414 is connected to network 411, network 412, and network 413 by corresponding logical communication links 433, 434, and 435 respectively. Data routing device 414 logically represents a computer system that can determine where to transfer data received from network 411, such as, for example, data received from client 405. That is, when data routing device 414 receives data from network 411, data routing device 414 can determine if the data is to be transferred to network 412 or network 413. As such, data routing device 414 can be configured to allow access to one network (e.g., network 412) while at the same time restricting access to another network (e.g., network 413). Data routing device 414 can make this determination using a variety of different techniques.

EX1005, [0051].

In all instances, Krantz expressly teaches that data from client 205 passes through access point 209 to data routing device 214 before it is routed to either VLAN C or VLAN B. As such, Krantz fails to disclose the claim limitation "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."

3. Krantz Fails To Disclose “Applying A Security Policy To The Access Device”

Each of the Challenged Claims recite: “applying a security policy to the access device in response to the request.” Krantz only discloses user authentication, and fails to disclose anything about applying a security policy to an access device. Despite Petitioners’ attempts to conflate user authentication with application of a **security policy to an access device**, Krantz is expressly missing this limitation.

The '460 Patent explains that user authentication is different than security policy compliance of an access device. Authentication is something done to the user (e.g., is the user who they say they are?). Security policy to an “access device” has nothing to do with the user. *E.g.* EX1001, 2:24-26(the “Access Device 160 has up-to-date virus software and encryption protocols as proscribed by the security policy”). Indeed, a user can be properly authorized, but if the “access device” does not have proper security policy compliance (e.g. antivirus software), then the network can be at risk.

The '460 Patent explains various “access device” security policies relating to: "operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry

information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230." *See* EX1001, 11:43-54.

In contrast, the '460 Patent describes "authentication of a user" as something much different: "requiring the user to enter a username and password..." EX1001, 1:31-33.

Krantz *only* teaches user authentication:

- "Krantz discloses that . . . '**authentication module 217** can receive the credentials (e.g. user-identifier and password) and compare the credentials to entries in the user database 218.'" Pet. at 47-48.
- "If an **authenticated user** of the client 205 . . . is authorized to access resources..." *Id.* at 48.
- "Krantz explains that the 'method 300 includes act of [client 205] sending credentials to a server to attempt to **authenticate** with the server..." *Id.* at 21.
- "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**) . . ." EX1005, [0019]

With no evidence for Krantz of applying a security policy to a device, Petitioners rely on Krantz's user authentication protocols. *See* Pet. at 38-40 (referencing Extensible Authentication Protocols; including EAP-TLS and EAP-MSChapV2). These are not security policies for an "access device." *See* EX2001, ¶¶ 56-59.

"EAP," by definition, is an "Extensible Authentication Protocol." It says nothing about device compliance with a security policy. Specific to EAP-TLS, this

is identity authentication that uses digital certificates.³ Similarly, EAP-MSChapV2 is used to verify the identity of a user or device trying to establish a connection to a network or a remote server.⁴

As explained by the '460 Patent, user authentication and security policy compliance are different.

[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.

EX1001, 13:54-67 (ALL CAPS emphasis of "AND" in original); EX2001, ¶ 58.

Furthermore, the '460 Patent even explains that mere reliance on authentication techniques, including the conventional EAP authentication credentials discussed in Krantz such as usernames, passwords, etc., is insufficient to ensure that a device attempting to access a protected network meets network security policies. *See* EX1001, 1:45-56. To that end, the '460 Patent teaches the separate security

³ See <https://www.securew2.com/blog/what-is-eap-tls>

⁴ See <https://www.portnox.com/cybersecurity-101/mschapv2/>

evaluation for the device by expressly claiming “applying a security policy” to a device. *E.g.*, EX1001, 16:11-12.

Petitioners also suggest that user authentication can be a “security policy.” Pet. at 37-38 (isolated citation to EX1001, 6:40-45 for the proposition that “the security policies may include requirements for user identification.”). But this is for something different—a security policy relating to a user authentication is not a security policy that is applied to the claimed “access device.” In other words, that a security policy may involve both user authentication and device requirements, does not mean that a security policy applied to a device would be satisfied by user authentication. To do so would read out the actual claim limitation which requires “applying a security policy to the access device.” As discussed, security policy compliance for an “access device” is whether the *device* includes the right software and/or hardware to satisfy security requirements, *e.g.*, virus software, updated OS, etc. An authorized user can still infect a security network with virus and trojans. *See* EX1001, 1:27-31; *see also id.* 1:45-48 (“mere user authentication” alone does not work because “there are no provisions to assure that an access device used by the authenticated user meets network security policies.”); *and also* EX2001, ¶¶ 56-58.

Claim 2 of the ‘460 Patent further illustrates this line of demarcation:

2. “The method of claim 1, further comprising authenticating a user of the access device.”

This makes clear that “applying a security policy to the access device” cannot be Krantz’s user authentication. Accordingly, Krantz fails to disclose or suggest the claim limitation of “applying a security policy to the access device.”

4. Krantz Also Fails To Disclose The Other “Applying A Security Policy To The Access Device” Limitations From The Dependent Claims

As set forth above, Krantz does not teach or suggest “applying a security policy to the access device.” Challenged Claims 3-6 and 18-20 recite “applying a security policy to the access device” with specific device data which is not taught by Krantz:

- “... wherein applying the security policy includes using the *system data* to determine that the access device satisfies the requirements of the security policy.” Claims 3 and 5.
- “... wherein applying the security policy includes using the *system data* to determine that the access device satisfies the requirements of the security policy.” Claims 18 and 20.
- “The method of claim 3, wherein the system data includes *antivirus software status*. Claim 4.
- “...wherein the system data includes *antivirus software version data*.” Claim 19.

In addition to not disclosing “applying a security policy to the access device,” nothing in Krantz discloses such a device security policy including “system data” or “antivirus software” status or version data. *See* EX2001, ¶ 49.

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

Petitioners argue that to the extent that Krantz is deemed to disclose certain claim limitations, that a POSITA would have found it obvious to and been motivated to incorporate Herrmann with Krantz. Ground 2, however, fails because even Herrmann does not disclose the “reconfiguring” limitation or the “without passing data through the gatekeeper” limitation. Notably, Petitioners do not argue that Herrmann teaches either the "reconfiguring" limitation or the "without passing data through the gatekeeper" limitation. Instead, Petitioners rely on Herrmann only for its teaching of comparing an access device's data with a security policy. In so doing, Petitioners effectively concede that Ground 1 based on Krantz alone is missing this security policy limitation. Regardless, whether one considers Krantz alone or in combination with Herrmann, specifically required limitations of the Challenged Claims are missing. As such, Ground 2 fails.

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.

Petitioners assert that Krantz has an effective date of December 6, 2002 and Herrmann has an effective date of March 13, 2003.⁵ Pet. at 7, 9. InfoExpress conceived of the claimed invention before that.

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

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

[REDACTED]

[REDACTED]

⁵ 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. EX2056; EX2061; EX2021.

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

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

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

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

December 2002

-

[REDACTED]

-

[REDACTED]

-

[REDACTED]

[REDACTED]

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

January 2003

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

February 2003:

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

○

■

■

■

■

■

■

- 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]

[REDACTED]

May 2003:

- [REDACTED]

[REDACTED]

[REDACTED]

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

June 2003:

- [REDACTED]

- See EX2003, ¶53 (Lum Declaration).

July 2003:

- [REDACTED]
- [REDACTED]

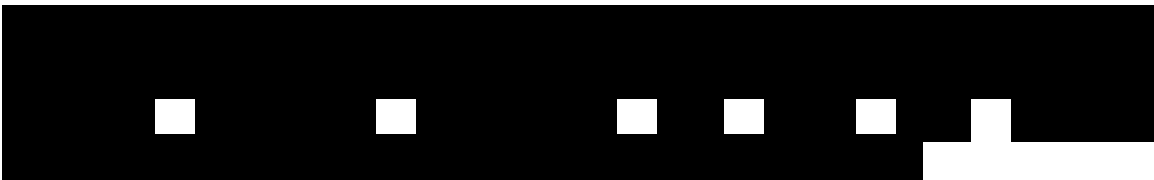
August 2003

- [REDACTED]

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

September 2003

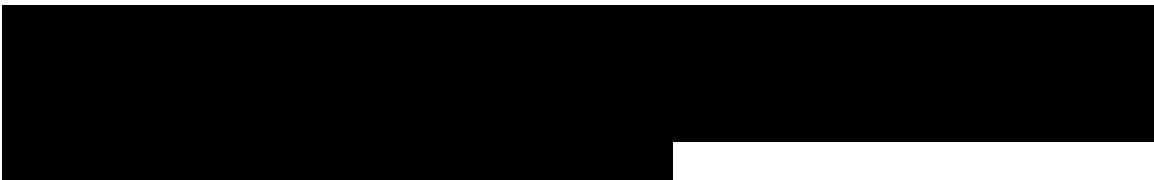
- 
- U.S. Provisional Patent Application Serial No. 60/505,582 was filed on September 24, 2003.

- 

- 

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

October 2003

- 

-  and filing of second provisional application. EX2262-EX2264.

- U.S. Provisional Patent Application Serial No. 60/513,080 was filed on October 21, 2003.

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

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

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

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

VII. Conclusion

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

Respectfully submitted,

Dated: June 26, 2024 Mailing address for all correspondence: Saul Ewing LLP Centre Square West 1500 Market Street, 38th Floor Philadelphia, PA 19102-2186	<i>/s/ Brian R. Michalek</i> Brian R. Michalek (Reg. No. 65,816) Saul Ewing LLP 161 North Clark Street, Suite 4200 Chicago, IL 60601 Tel: (312) 876-7151 brian.michalek@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 13,746 words, excluding the parts of the brief exempted by 37 C.F.R § 42.24(b).

Date: June 26, 2024

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

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

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

Date: June 26, 2024

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