

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,
Petitioner,

v.

NETSKOPE, INC.,
Patent Owner.

Case No. IPR2026-00025

U.S. Patent No. 8,117,639

**PETITION FOR INTER PARTES REVIEW
OF U.S. PATENT NO. 8,117,639**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	REQUIREMENTS FOR <i>INTER PARTES</i> REVIEW	2
	A. Certification.....	2
	B. The Challenged Claims and Relief Requested	2
III.	TECHNOLOGY BACKGROUND.....	3
IV.	THE '639 PATENT	5
	A. Overview of the Specification.....	5
	B. The Challenged Claims	8
	C. Level Ordinary Skill in the Art	8
V.	CLAIM INTERPRETATION.....	9
VI.	PRIOR ART OVERVIEW	9
	A. Overview of Richmond	9
	B. Overview of Wood.....	15
	C. Overview of Teraslinna.....	16
VII.	GROUND 1 & 2 – CLAIMS 1-8, 10-15, 17-20, 22-25 ARE ANTICIPATED OR RENDERED OBVIOUS BY RICHMOND.....	18
	A. Independent Claim 1	18
	B. Dependent Claim 2.....	40
	C. Dependent Claim 3.....	43
	D. Dependent Claim 4 (Ground 2 Only).....	46
	E. Dependent Claim 5.....	48
	F. Dependent Claim 6.....	50
	G. Dependent Claim 7.....	52
	H. Dependent Claim 8.....	54
	I. Dependent Claim 9.....	56
	J. Independent Claim 10	57
	K. Dependent Claim 11	59
	L. Dependent Claim 12.....	59

M.	Dependent Claim 13.....	59
N.	Dependent Claim 14.....	61
O.	Dependent Claim 15.....	61
P.	Dependent Claim 16.....	61
Q.	Independent Claim 17	62
R.	Dependent Claim 18.....	64
S.	Dependent Claim 19.....	64
T.	Dependent Claim 20.....	64
U.	Dependent Claim 22.....	64
V.	Dependent Claim 23.....	65
W.	Dependent Claim 24.....	66
X.	Dependent Claim 25.....	66
Y.	Dependent Claim 26.....	66
Z.	Independent Claim 27	66
VIII.	GROUND 3 – CLAIMS 9, 16, 26, AND 27 ARE RENDERED OBVIOUS BY RICHMOND IN LIGHT OF WOOD.....	68
A.	Dependent Claim 9.....	68
B.	Dependent Claims 16 and 26	72
C.	Independent Claim 27	72
IX.	GROUND 4 – CLAIM 21 IS RENDERED OBVIOUS BY RICHMOND IN LIGHT OF TERASLINNA.....	73
A.	Dependent Claim 21	73
X.	FEES	78
XI.	CONCLUSION	78
XII.	MANDATORY NOTICES	78
A.	Real Party-in-Interest	78
B.	Related Proceedings	78
C.	Counsel Information.....	79
D.	Electronic Service	79

LISTING OF EXHIBITS

Exhibit No.	Document
1001	U.S. Patent No. 8,117,639 ("the '639 Patent")
1002	Declaration of Kevin C. Almeroth.
1003	U.S. Patent Publication No. 2003/0152067 ("Richmond")
1004	WIPO Publication WO 01/11452A2 ("Wood")
1005	U.S. Patent No. 5,623,492 ("Teraslinna")
1006	Enterasys Personalized User Network Whitepaper ("Enterasys Whitepaper")
1007	Excerpts from File History of Richmond
1008	Curriculum Vitae of Kevin Almeroth
1009	Excerpts from A. Tannenbaum, <i>Computer Networks</i> (3d ed., 1996)

All emphasis appearing herein is added unless otherwise noted.

TABLE OF AUTHORITIES

Cases

<i>Arbutus Biopharma Corp. v. ModernaTX, Inc.</i> , 65 F.4th 656 (Fed. Cir. 2023)	57
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	9

Statutes

28 U.S.C. § 102.....	2, 9, 15–16
37 C.F.R. § 42.2.....	2
37 C.F.R. § 42.24.....	80
37 C.F.R. § 42.100(b)	9
37 C.F.R. § 42.104.....	2

I. INTRODUCTION

Petitioner Fortinet, Inc. ("Fortinet") requests *inter partes* review of claims 1-27 ("the Challenged Claims") of U.S. Patent No. 8,117,639 ("the '639 Patent") (Ex1001).

The '639 Patent relates to systems and methods for "provisioning network access" and "provid[ing] access control" for computer networks, based on a user's identity. Ex1001, Abstract. The '639 Patent makes the self-evident observation that, in a shared network, if bandwidth usage is not controlled, "one user connected to a particular router can consume a majority of bandwidth," thereby slowing the network for all other users. *Id.*, 2:1-4. The '639 Patent's solution to this problem is conventional: limit bandwidth usage on a per-user basis. *Id.*, 2:43-51. The Patent acknowledges that it was conventional to require users to authenticate by providing a valid username and password before being allowed access to a computer network. *Id.*, 1:39-44. However, the '639 Patent contends that prior-art access control and provisioning methods were unable to limit bandwidth on a per-user basis, but only on a per-physical-port basis. *Id.*, 1:45-52. But this is incorrect. In fact, prior-art references (*which were not before the examiner during prosecution of the '639 patent*) teach every element of the well-known systems and methods recited in the Challenged Claims. Accordingly, Petitioner respectfully requests cancellation.

II. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Certification

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '639 Patent is available for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the Challenged Claims on the grounds identified herein.

B. The Challenged Claims and Relief Requested

Pursuant to 37 C.F.R. § 42.104(b)(1) and 42.2, Petitioner requests the Board institute IPR and cancel the Challenged Claims. The '639 patent claims priority to a October 10, 2002 provisional application. Without conceding that the '639 Patent is entitled to that priority date, it has been used for the Grounds below. The prior art forming the Grounds are:

Exhibit	Reference	Reference Date	Prior Art Status
Ex1003	U.S. Patent Publication No. 2003/0152067 ("Richmond")	Sept. 20, 2002 (filing date)	§102(e)
Ex1004	WIPO Publication WO 01/11452A2 ("Wood")	Feb. 15, 2001 (publication date)	§102(a), (b)
Ex1005	U.S. Patent No. 5,623,492 ("Teraslinna")	Mar. 24, 1995 (filing date) Apr. 22, 1997 (issue date)	§102(a), (b), (e)
Ex1006	<i>Enterasys User Personalized Whitepaper</i> ("Enterasys Whitepaper"), incorporated by reference into Richmond	Sept. 20, 2002 (filing date of Richmond)	§102(e)

The asserted Grounds of unpatentability are:

Ground	Claims	Basis	Prior Art
1	1-3, 5-20, 22-25	§102	Richmond
2	1-20, 22-25	§103	Richmond
3	9, 16, 26-27	§103	Richmond, Wood
4	21	§103	Richmond, Teraslinna

None of this prior art was considered during the prosecution of the '639 Patent.

This petition is supported by the Expert Declaration of Kevin C. Almeroth (Ex1002).

III. TECHNOLOGY BACKGROUND

The '639 Patent generally relates to controlling users' access to packet-switched computer networks. In a packet-switched network, the stream of data to or from any networked device is broken up into individual short messages, called "packets." Ex1002 ¶47. A networked device transmits a packet to network infrastructure such as a switch or router, which then forwards the packet to the next switch or router, and so on, until the packet reaches its destination. *Id.*

In order for a switch to know the intended destination to which to forward the packet, and in order for the destination to know the source of a received packet, each packet contains a unique address of both the source device and destination device. *Id.* ¶48. This information is placed in fixed locations at the start of the packet, in a region known as the packet's "header," along with other information used in routing a packet. *Id.* The packet also contains the data to be transmitted, known as the "payload." *Id.*

A common packet-based networking protocol is the IEEE 802.3 Ethernet protocol. *Id.* ¶49. Each Ethernet device is assigned a unique 6-byte Media Access Control ("MAC") address. *Id.* When transmitting data, an Ethernet device assembles a packet (sometimes called a "frame") with a header indicating its own MAC address and the intended destination's MAC address. *Id.* The data to be transmitted (generally up to 1500 bytes) is placed in the payload section. *Id.* The packet/frame is then transmitted to a switch, which inspects the header to determine the intended destination and forwards it accordingly.

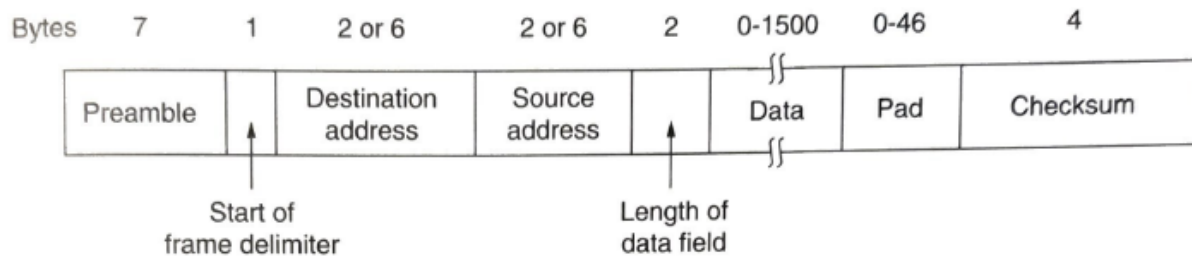


Fig. 4-21. The 802.3 frame format.

Id. (citing Ex1009, 281).

An Ethernet packet's payload can, and typically does, contain a packet of a higher-level protocol. One example is the Internet Protocol ("IP"), on which the Internet is based. Ex1002 ¶50. Each Internet Protocol network device is assigned a 4-byte (or in some cases, 16-byte) IP address. *Id.* Each IP packet includes a header including both source and destination IP addresses. *Id.* The IP payload follows the header. *Id.*

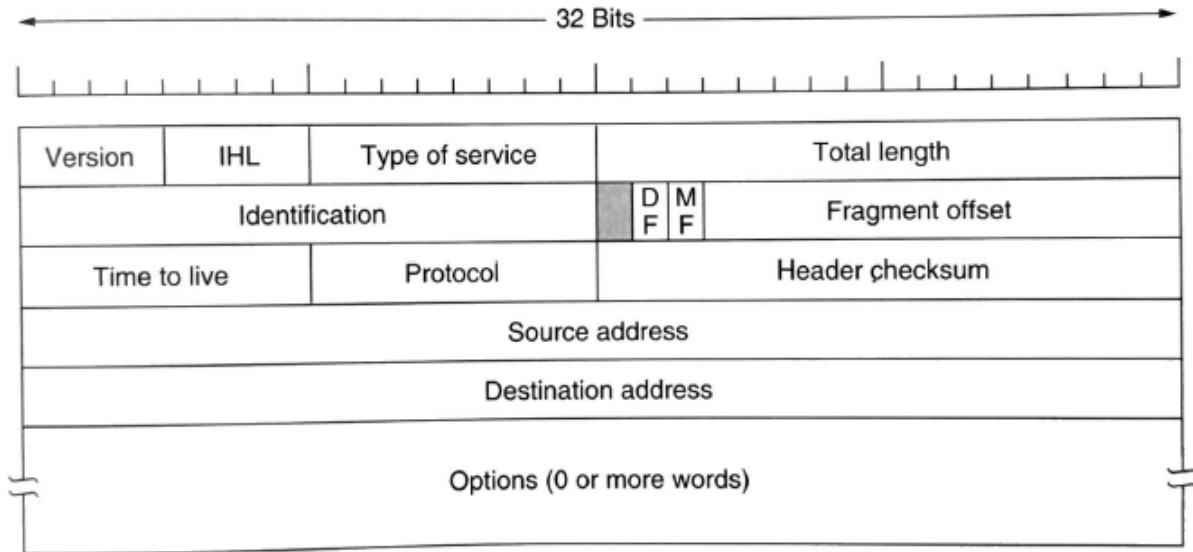


Fig. 5-45. The IP (Internet Protocol) header.

Id. (citing Ex1009, 413). Thus, in a network using IP over Ethernet, each packet received by a device contains both a MAC address and IP address in the Ethernet and IP headers, respectively. *Id.*

IV. THE '639 PATENT

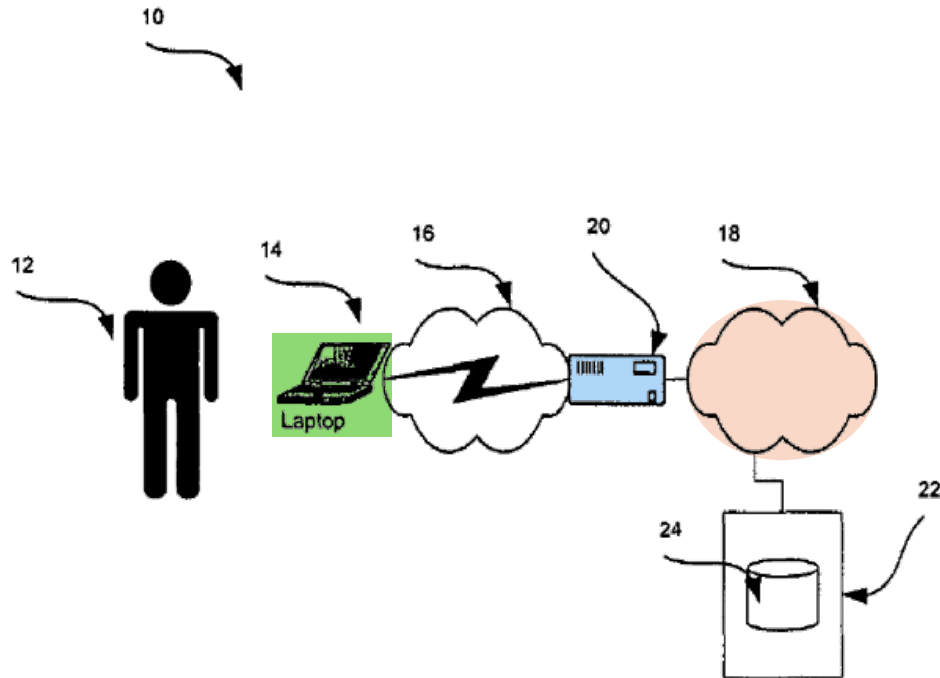
A. Overview of the Specification

The '639 Patent is titled "System and Method for Providing Access Control," and issued on February 14, 2012, from U.S. Patent Application No. 10/683,317, which was filed on October 10, 2003. The '639 Patent claims priority to U.S. Provisional Application No. 60/417,674, filed October 10, 2002. The '639 Patent is thus subject to the pre-AIA Patent Act.

The '639 Patent purports to address the problem of bandwidth overutilization in a shared network. Ex1002 ¶¶52-54. For example, it observes that "many cafes

have public wireless networks to allow patrons to access the Internet," but that if left unchecked, "one user connected to a particular router can consume a majority of the bandwidth (e.g., downloading pictures from the Internet), slowing down the wireless network for other users connected to that router." Ex1001, 1:63-2:4. The '639 Patent acknowledges it was conventional to authenticate users before they are permitted to access a shared network. *See id.*, 1:39-44 ("To access a LAN and, in turn, the Internet, many prior-art access control systems require a user to ... enter a user name and password."). However, the '639 Patent asserts that prior-art access control systems "typically assume that a user is tied to a particular physical port," such that allegedly "provisioning of bandwidth is done on a per port rather than a per user basis." *Id.*, 1:45-52.

To address this purported problem, the '639 Patent discloses a control device 20 that receives network traffic from user device 14 and decides whether and to what extent that user device will be permitted to access controlled network 18. *Id.* 4:13-27. In making access-control decisions, the control device 20 may access authentication database 24, which contains a list of permissible users and the rights associated with each user. *Id.*, 4:28-33.



Ex1001, Fig. 1 (annotated).

Control device 20 operates by inspecting packets received from each user device and extracting fields such as their MAC address and IP address to determine the user identity. *Id.*, 4:54-62. If the addresses do not correspond to a previously authenticated user, the control device requests the user to authenticate themselves, such as by redirecting them to a login webpage. *Id.*, 4:63-5:13, 6:24-56. Once authenticated, the control device stores the user device's MAC address and IP address for future identification. *Id.*, 5:32-35. For an authenticated user, when the control device receives network traffic from the user device, it will manage the user's access to the network based on rules that are associated with that user (*e.g.*, a maximum upload or download bandwidth, or a list of blocked sites or applications). *Id.*, 7:4-21.

B. The Challenged Claims

The '639 Patent contains 27 claims. Claims 1, 10, 17, and 27 are independent. Claim 1 is directed to "[a] method for network access control" performed "at a control device." Independent claims 10 and 17 are directed to a "computer program product" and "control device for network access control," respectively, that are configured to perform steps substantively the same as those of claim 1. Ex1002 ¶55. Independent claim 27 is (like claim 17) directed to a "control device for network access control," further adding that an unauthenticated user is redirected to a login webpage at which to provide credentials. *Id.*

C. Level Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") in the field of the '639 Patent would have had at least a bachelor's degree in computer science, computer engineering, or related field, with two to three years working with computer networking. Ex1002 ¶56. Additional graduate education could substitute for professional experience, while significant experience in the field might substitute for formal education. *Id.* Minor variations of this definition would not have an impact on the conclusions. *Id.* Although this petition assumes that the October 10, 2002 filing date of the provisional application applies as the priority date, the conclusions would not change if the October 10, 2003 non-provisional filing date were applicable. *Id.*

V. CLAIM INTERPRETATION

Claims in IPR are construed according to the plain-and-ordinary meaning standard of *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). *See* 37 C.F.R. § 42.100(b). Petitioner respectfully submits that no claim construction is required for this petition and further submits that the prior art meets all limitations under any reasonable construction. Ex1002 ¶57. In the pending district court proceeding, Patent Owner contends that "global stage" (claims 3, 12, 19) should be construed as "a global stage, distinct from the client discrimination stage and distinct from the user specific stage." Regardless of which construction is adopted, this limitation is disclosed and rendered obvious by the prior art.

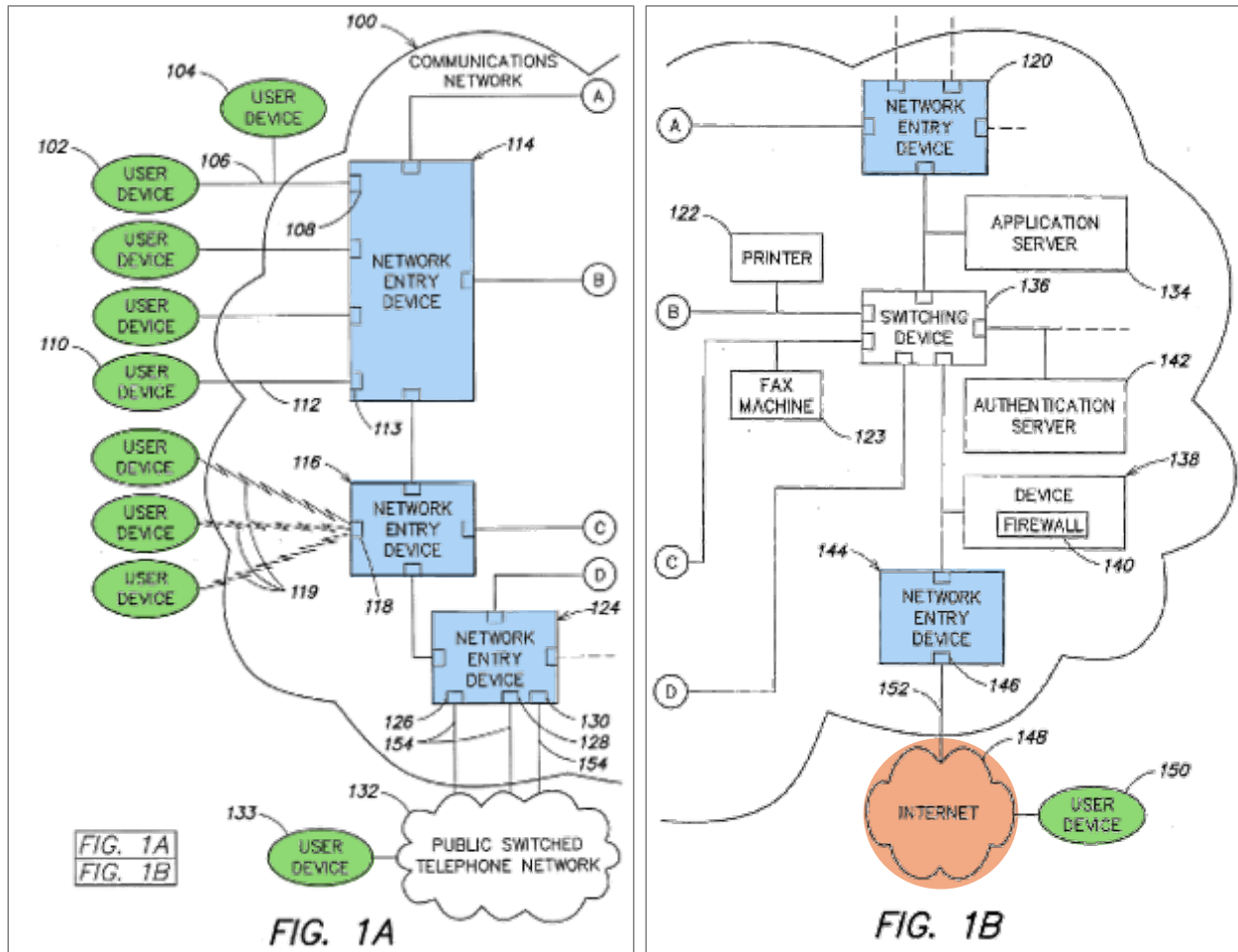
VI. PRIOR ART OVERVIEW

A. Overview of Richmond

U.S. Patent Publication No. 2003/0152067 ("Richmond") is a publication of U.S. Patent Application No. 10/251,140, which was filed on September 20, 2002. Richmond thus predates the October 10, 2002 filing date of the '639 Patent's provisional application, and accordingly is prior art under 35 U.S.C. §102(e). Richmond is a continuation-in-part of U.S. Patent Application No. 10/071,873, filed on February 8, 2002.

Richmond is titled "Controlling Concurrent Usage of Network Resources by Multiple Users at an Entry Point to a Communications Network Based on Identities of the Users." Ex1003, cover. Richmond discloses a system in which **user devices**

connect to a network (including the Internet) through a set of "network entry devices," as shown below in Figure 1.



Ex1002 ¶58; Ex1003, Figs. 1A-1B (annotated).

As is conventional with Internet communications, user devices communicate on the network by sending and receiving packets to and from the network, wherein each packet contains a header with a source and destination address, as well as a data payload. Ex1003, [0010]; *see also* Ex1002 ¶59; Section III, *supra*. The network entry devices impose a set of "packet rules" on the packets that pass through them.

"[E]ach packet rule include[es] a condition and action to be taken if a packet received at a device satisfies the condition." Ex1003, [0082]. For example, the exemplary packet rule definition shown in Figure 5 specifies (in field 508) that "[the] IP addresses of a packet are to be examined," and further specifies (in field 510) that the packet's IP address is compared to the value "10.20.54.0." *Id.*, [0162]-[0163]. If a packet matches, the rule instructs to assign priority 7 (item 516), "representing a Quality of Service (QoS)/Class of Service (CoS)" to apply to the packet. *Id.*, [0156], [0165]. The rule further instructs to not drop the packet (item 581), and to not apply rate limiting (item 520).

NAME	STATUS	TYPE	VALVE	MASK	VLAN	PRIORITY	DENY?	RATE LIMIT	LAYER
CONTAIN SUBNET 54	ENABLED	IP ADDRESS BILATERAL	10.20.54.0	255.255.255.0	5	7	NO	NONE	3

FIG. 5

Id., Fig. 5 (annotated).

Richmond's packet rules may be associated with a higher-level concept called "service abstractions" that group together multiple packet rules to define classes of service for particular applications. *Id.*, [0116]-[0118]. For example, as shown in Figure 2, various packet rules may be assigned to define a "high-priority" class of service (items 208 and 212) that prioritizes traffic for specific applications (*e.g.*, SAP and Citrix). Ex1002 ¶60. Conversely, other classes of service may block certain

applications (e.g., service 210 labelled "NO SNMP" blocks SNMP traffic). Ex1003,

[0141], Fig. 2:

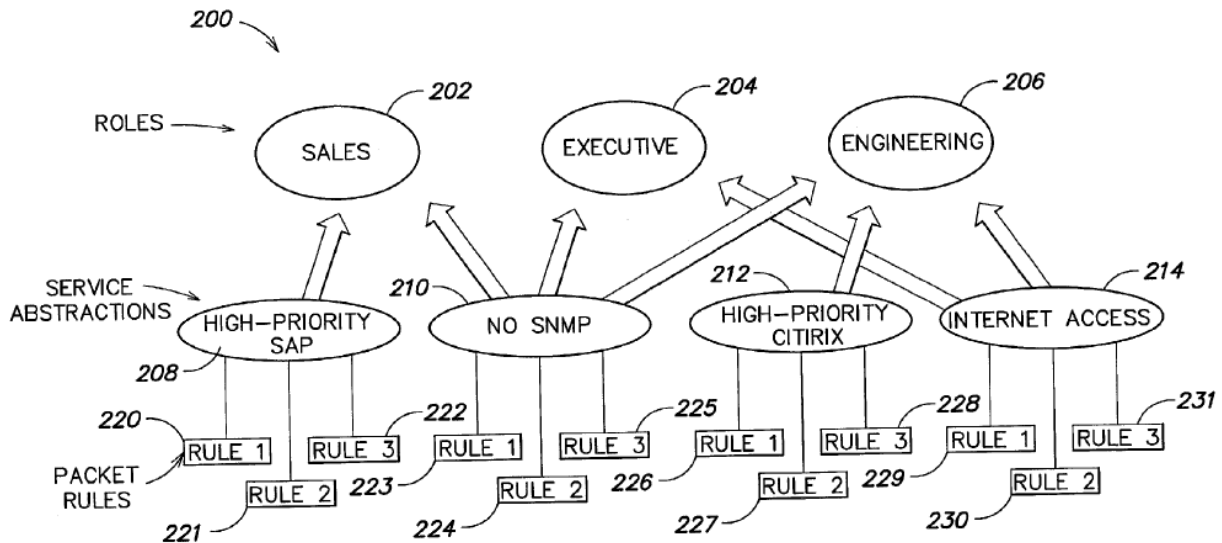
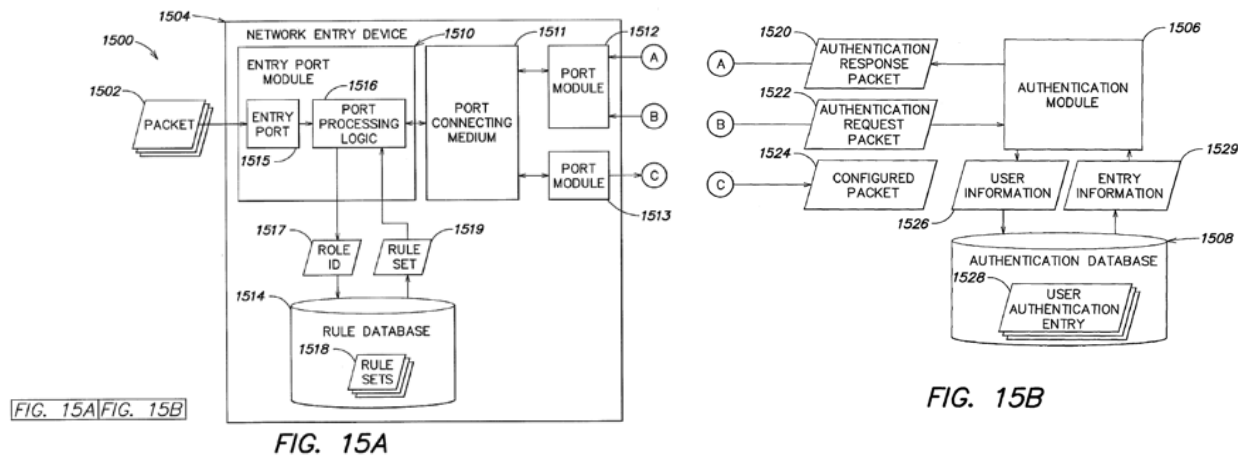


FIG. 2

As also shown in Figure 2, service abstractions (and the packet rules associated with them) may be assigned to classes of users, termed "roles." *Id.*, [0121], [0132], [0139]. For example, the Sales role 202 is given access to "High-Priority SAP" service 208 but not general "Internet Access" 214. Conversely, users in Executive and Engineering roles (items 204 and 206) are given Internet access but not SAP access. *Id.*, [0141], Fig. 2; Ex1002 ¶61. All three roles are barred from using SNMP network management protocol, as a result of being assigned the "NO SNMP" service abstraction 210. Ex1003, [0141].

In Richmond's system, enforcement and application of packet rules (including the determination of which rules apply, based on roles and service abstractions) is

performed by network entry devices, in particular the entry port module of those devices, in conjunction with an authentication module. *Id.*, [0230], [0233], [0238], [0244], [0249]. These are shown in Figures 15A-15B, below:



When a user seeks to access a network controlled by Richmond's network entry devices, they send a login packet to an entry port module 1510 of the network entry device 1504, containing information sufficient to authenticate the user's identity, such as a username and password. *Id.*, [0217], Fig. 13A(2) (act 1310). The network entry device forwards the identity information to an authentication module, which stores a database containing the credentials of each user and their roles. *Id.*, [0273]-[0275]. If the credentials are invalid, the network entry device denies the user access to the network. *Id.*, [0222], Fig. 13A(2) (acts 1314 and 1316). Conversely, if the credentials are valid, the authentication module informs the network entry device of the user's roles, which then configures its entry port modules with the user-based packet rules corresponding to the user's identity and

corresponding roles and service abstractions. *Id.*, [0223], [0277]-[0279]. Subsequently, when the user sends packets to be transmitted on the network, the network entry device processes the packets according to these pre-configured user-based rules. *Id.*, [0280]-[0281], Fig. 13B (act 1327). For example, one type of rule instructs to drop all packets intended for a certain destination, such as to block access to non-work-appropriate sites or applications. *Id.*, [0157]. Another type of rule limits the rate of a user's bandwidth consumption, in order to prevent any one user or small subset of users from monopolizing the available upstream bandwidth. *Id.*, [0158]-[0159].

For simplicity, Richmond does not require each user-based packet rule to specify every field that can be applied to the packet. Ex1002 ¶65. Instead, the administrator may define default rules that will be applied to each packet in the absence of any user-specific rule that sets given packet fields. Ex1003, [0212], [0231], [0252].

Once a packet has been processed by the network entry device (and the rules do not specify dropping the packet), the network entry device forwards that packet on another port module towards its corresponding destination. *Id.*, [0282]. If the user rules specify rate limiting, the network interface device sends the packets at a rate consistent with the limit. *Id.*, [0251], Fig. 14B (act 1430).

B. Overview of Wood

WIPO Publication WO 01/11452A2 to Wood was published February 15, 2001, and thus is prior art under 35 U.S.C. §102(a) and (b). Wood discloses a system in which access to a network is controlled by a "Gatekeeper and entry handler component 110," which "provides an entry point for external client applications requesting access." Ex1004, 5:10-15. The gatekeeper interacts with an authentication component 130 to determine whether a user is authenticated. *Id.*, 6:3-8; Ex1002 ¶¶66-67.

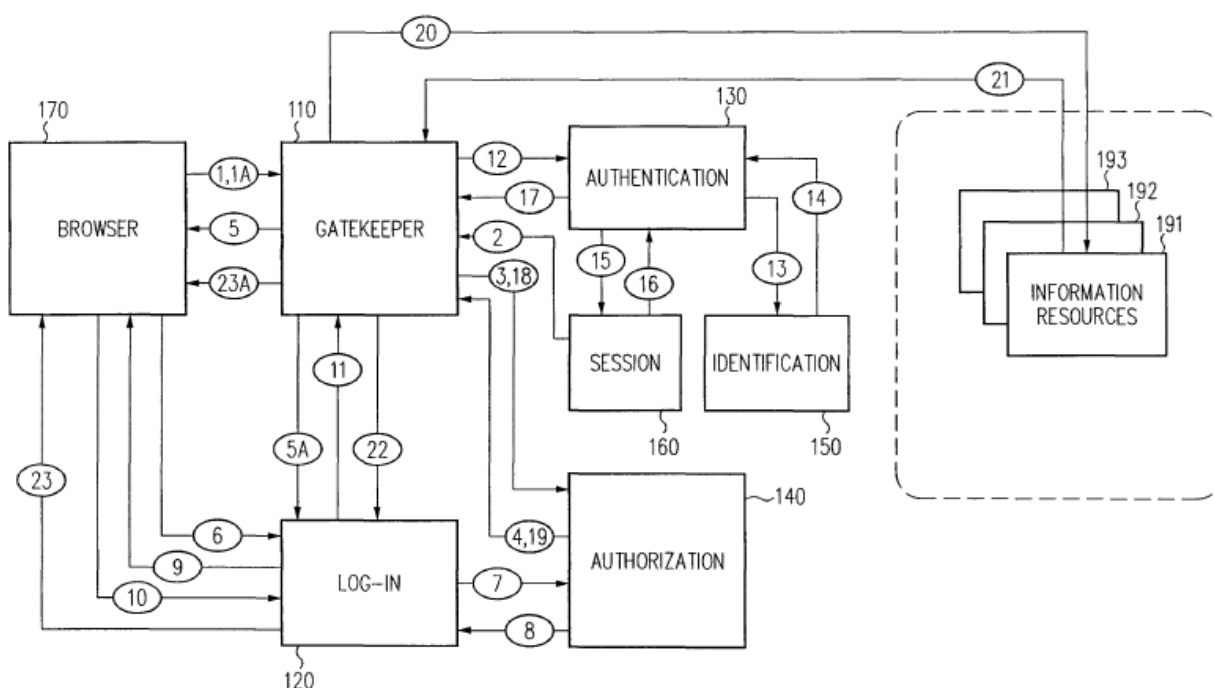


FIG. 1

If the user has not authenticated, the authorization component indicates this to the gatekeeper, which then redirects the user to a login component 120. *Id.*, 6:7-9, 12:1-26. The login component then redirects the user's browser to an authentication

webpage to allow the user to supply his or her credentials. *Id.*, 14:3-10. The system then uses the received credentials to authenticate the user. *Id.*, 14:22-25.

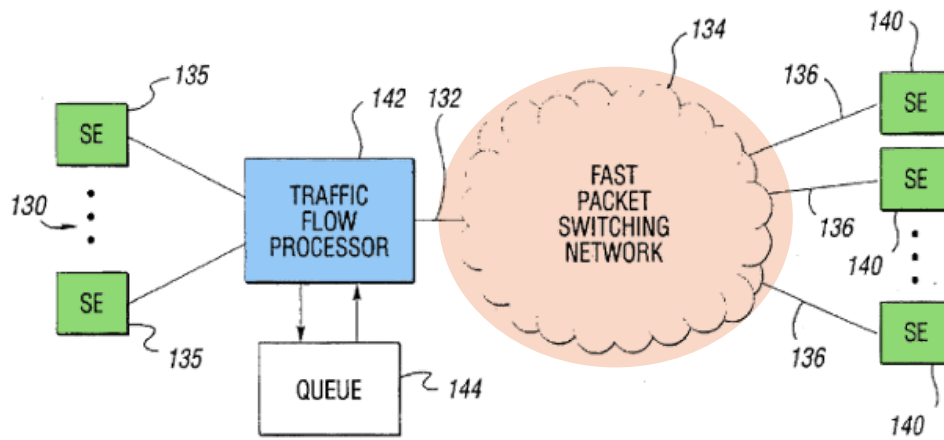
C. Overview of Teraslinna

U.S. Patent No. 5,623,492 ("Teraslinna") was filed on March 24, 1995, and issued on April 22, 1997. Ex1005, cover. Accordingly, it is prior art to the '639 Patent under 35 U.S.C. §102(a), (b), and (e).

Teraslinna is titled "Methods and Systems for Managing Bandwidth Resources in a Fast Packet Switching Network," and relates to "managing bandwidth resources within a switching communication network having at least one fast packet switch." Ex1005, 1:8-13. Teraslinna uses the term "fast packet switching" to refer simply to a packet-switched network, in comparison to slower circuit-switched networks. Ex1002, ¶68; Ex1005, 1:20-25 (defining "fast packet switching" as "a technique wherein a message is communicated between a source endpoint and a destination endpoint of a switching network using a series of information passing elements, i.e. packets, each of which contain both a payload field and an address").

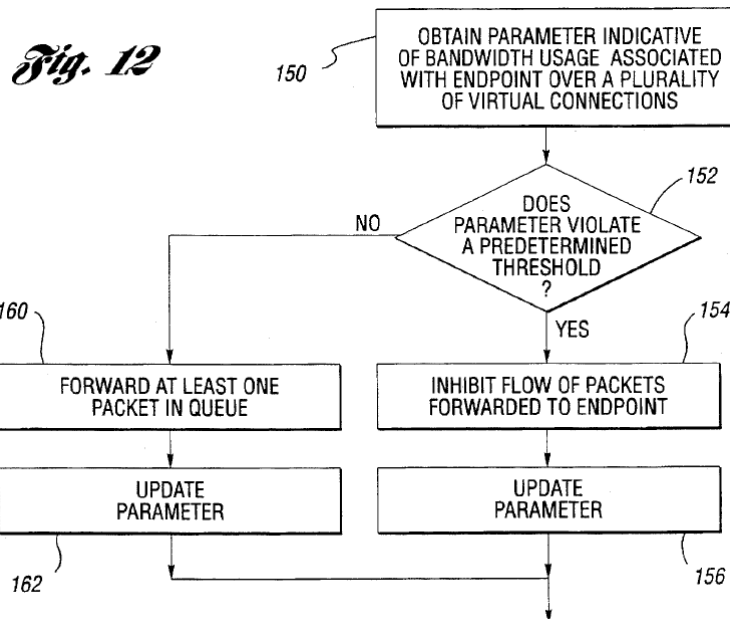
Teraslinna discloses "a system for controlling a flow of packets being forwarded by" user devices ("subscriber equipment 135") from a network of a telecom customer/subscriber ("customer premises equipment (CPE) [130]") through a telecom carrier's network ("fast packet switching network 134") and ultimately to various destination devices ("subscriber equipment 140"). Ex1005, 15:27-39;

Ex1002 ¶69. Teraslinna teaches that it is necessary to control the bandwidth used by subscriber equipment in order to enforce the agreed-upon service contract between the subscriber and the telecom provider. Ex1005, 1:58-2:7. To accomplish bandwidth control, the customer's network is connected to the telecom's network through a "traffic flow processor." *Id.*, 15:40-42, Fig. 11.



Id., Fig. 11 (annotated).

Teraslinna's traffic flow processor 142 is coupled to queue 144, which "queues all incoming packets from the customer premises equipment 130 for traffic shaping by the traffic flow processor." *Id.*, 16:5-8; Ex1002 ¶70. The traffic flow processor then applies an algorithm to determine the rate at which packets should be forwarded from the queue over the network endpoint in order to comply with a set bandwidth limitation. Ex1005, 16:9-17:18, Fig. 12.



Id., Fig. 12.

VII. GROUNDS 1 & 2 – CLAIMS 1-8, 10-15, 17-20, 22-25 ARE ANTICIPATED OR RENDERED OBVIOUS BY RICHMOND

A. Independent Claim 1

Richmond discloses and renders obvious all limitations of claim 1. *See* Ex1002 ¶¶72-111.

1. A method for network access control, comprising

To the extent the preamble is limiting, Richmond discloses a method for network access control. Ex1002, ¶¶72-74. Richmond's "Background" section states that "[a] common issue in [communications] networks is how to control usage of network resources by users," *i.e.*, access control, and its specification as a whole discloses how to address this issue. Ex1003, [0003]. Richmond's Abstract explains that, in its disclosed system, "[e]ach users' usage of [*i.e.*, access to] network

resources is controlled, after such user has been authenticated," by "[a]n entry port module of a network entry device," in which "each packet received from each user may be examined to control usage [*i.e.*, access] of network resources." *Id.*, Abstract.

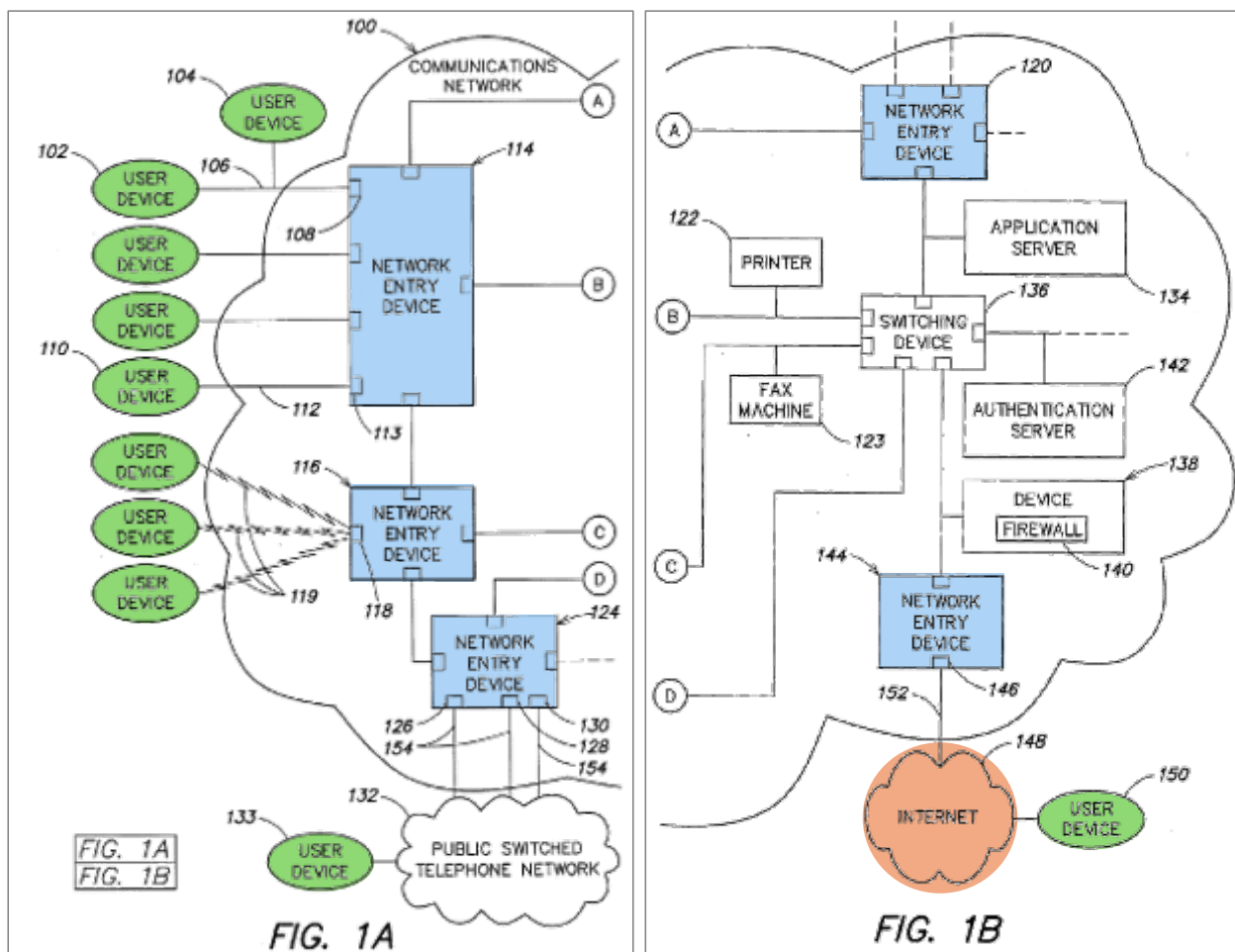
The specific methods performed by the entry port module are disclosed in methods 1300 and 1400, which "configur[e] an entry port module of a network device ... to control usage of network resources." *Id.*, [0206].

2. **at a control device, receiving a packet originating from a user device in a first network, wherein the first network is connected to a second network via the control device, and wherein the user device is associated with a user;**

Richmond discloses, at a control device (*e.g.*, network entry devices 114, 116, 120, 124, 144, and 1504), receiving a packet originating from a user device (*e.g.*, user devices 102, 104, 110, 133, 150, and 1502) in a first network (*e.g.*, Network 100), wherein the first network is connected to a second network (*e.g.*, Internet 148) via the control device, and wherein the user device is associated with a user. Ex1002, ¶¶75-81.

Richmond discloses a "Network 100" (an exemplary first network) that "include[es] ... network entry devices 114, 116, 120, 124, and 144" (exemplary control devices). Ex1003, [0012]. "[A] network entry device serves as an entry point to the network for at least one user." *Id.*, [0016]. "A network entry device ... reside[s] at an edge or boundary of the communications network and provide[s]

connectivity between network resources of the communications network and devices located external to the communications network," such as user devices. *Id.*, [0016].



Id., Figs. 1A-1B (annotated).

The component of the network entry devices to which other devices connect is a "port module." *Id.*, [0013]. A port module "includes a physical port of the device and port processing logic associated with the physical port." *Id.*, [0014]. Such port processing logic "include[s] switching logic, memory, and one or more processors for configuring the port module and for processing packets sent to and received at the port module." *Id.* An "entry port module" is a specific type of port module that "serves as a user's entry point into a network." *Id.*, [0015]. "[T]o communicate with devices on the network, a user's device may transmit one or more packets to an entry port." *Id.*

In Figure 15A, Richmond depicts the structure of its network entry devices (therein identified as item 1504). *Id.*, [0261]-[0262]. Packets 1502 originating from a user device are received by entry port module 1515 of the network entry device. *Id.*, [0265], [0269], [0271]. The network entry device includes additional port modules through which packets from the user device can be forwarded (*e.g.*, item 1513), thereby connecting the user device to the second network. *Id.*, [0270], [0282]. The network entry device acts as an exemplary control device by controlling whether the user device's traffic is able to reach the network.

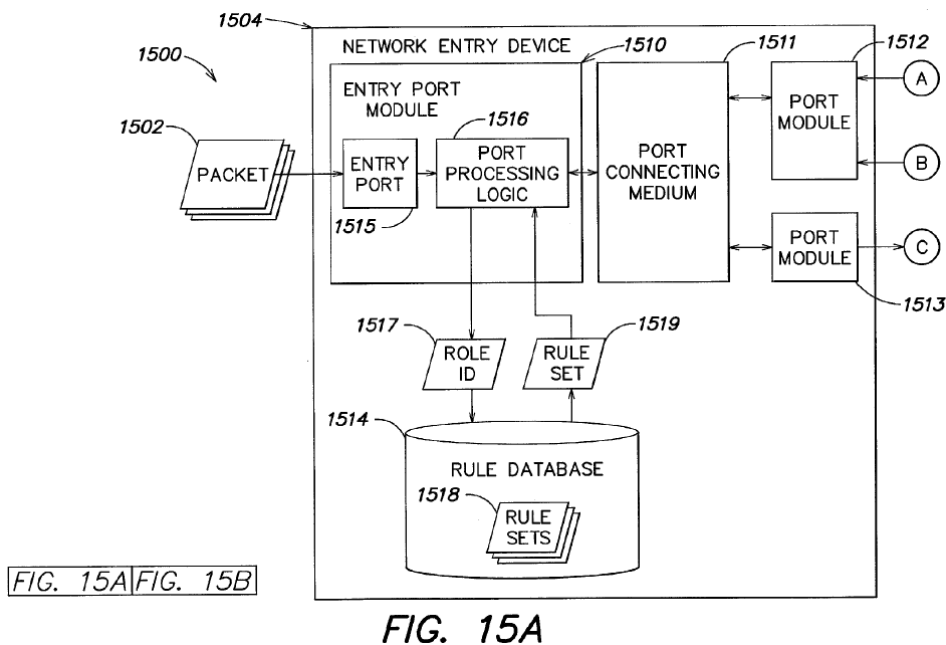


FIG. 15A/FIG. 15B

FIG. 15A

Id., Fig. 15A.

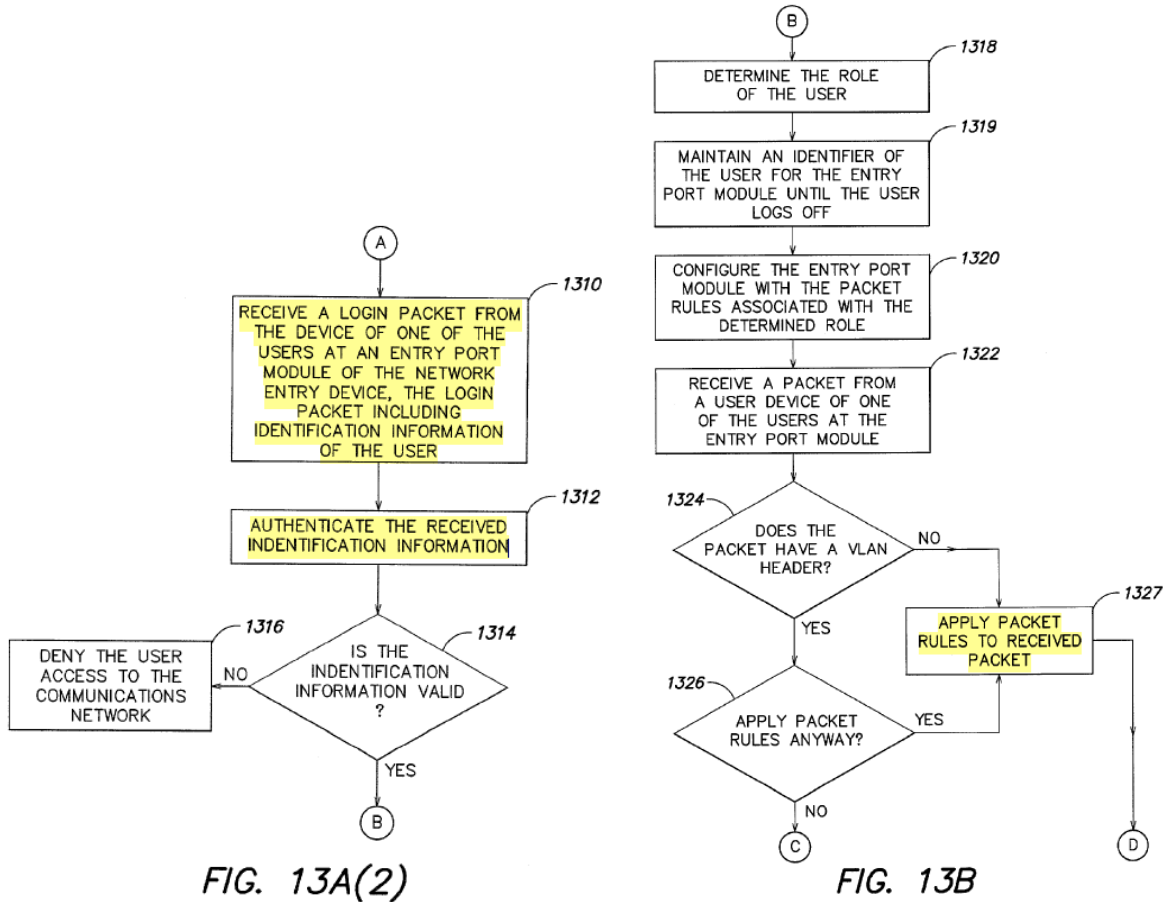
User devices may connect to network entry devices through various connectivity types, such as dedicated or shared wire-based transmission mediums, wireless transmission mediums, or the Internet. *Id.*, [0021]-[0025]. Each user device is "associated with a user" (*i.e.*, the operator or owner of that device). *See, e.g., id.*, [0028], [0035].

As shown in Fig. 1B, the first network (*e.g.*, Network 100) is connected to the Internet 148 (an exemplary second network) via the network entry devices (*e.g.*, item 144, an exemplary control device). Ex1002 ¶81. Alternatively, if Internet 148 is identified as the first network, it is likewise connected to the Network 100 (in this alternate identification, an exemplary second network) via the network entry devices. *Id.*

3. processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;

Richmond discloses the step of processing the packet according to a plurality of stages, including a client discrimination stage (*e.g.*, acts 1310 and 1312 in Fig. 13A(2) and act 1401 in Fig. 14A(1)) and a user-specific rule stage (*e.g.*, acts 1402 and later in method 1400). Ex1002, ¶¶82-87.

Client discrimination stage. As shown in the flow diagram of Figure 13 illustrating method 1300, Richmond teaches that the acts of Richmond's disclosed system proceed in stages. These include numerous steps related to client discrimination, which thus are a "client discrimination stage." For example, the network entry device receives a login packet from the user including "identification information of the user" (act 1310), after which it "authenticate[s] the received identification information" (act 1312). *Id.*, [0217], [0220], Fig. 13A(2). Based on whether "the identification information [is] valid" (act 1314), the network entry device either "den[ies] the user access to the communications network," or otherwise proceeds to determine the user's role (act 1318) and configure the entry port module accordingly (acts 1319 and 1320). *Id.*, [0221]-[0225], Fig. 13B.



Id., Figs. 13A(2) & 13B (annotated).

Method 1400 (an implementation of block 1327 in Fig. 13B, *see id.*, [0243]) further depicts actions involved in client discrimination, which therefore are a client discrimination stage. For example, the first action "determine[s] an identity of a user of the user device from which the packet was received" (act 1401). *Id.*, [0224], Fig. 14A(1).

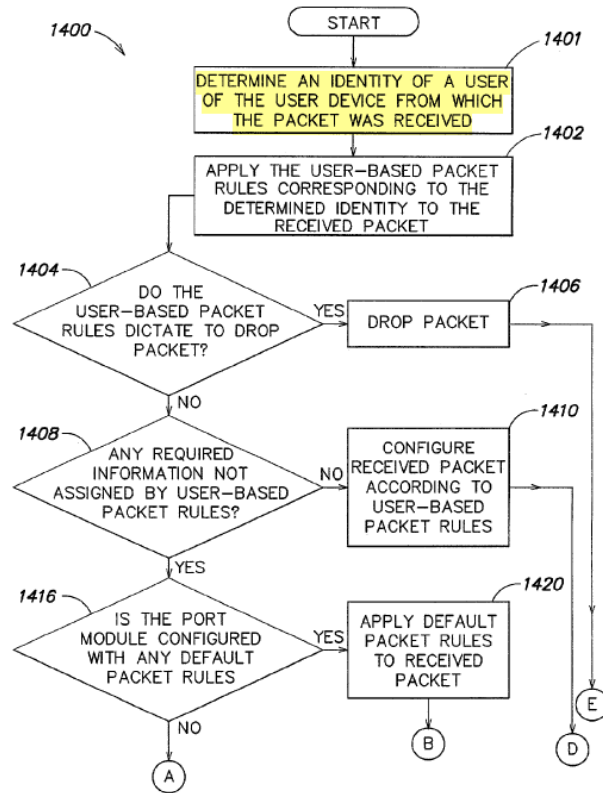


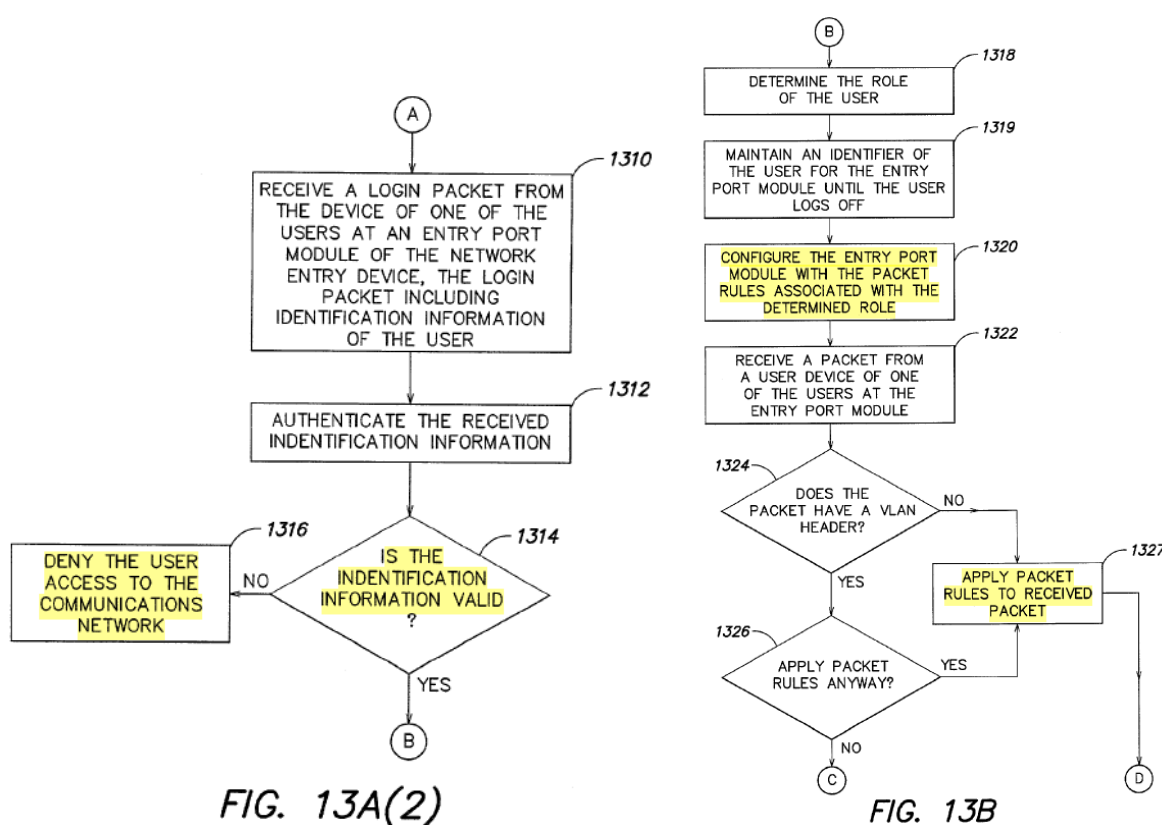
FIG. 14A(1)
 FIG. 14A(2)
 FIG. 14B

FIG. 14A(1)

Id., Fig. 14A(1) (annotated).

User-specific rule stage. As shown in methods 1300 and 1400, Richmond's system also includes numerous steps related to user-specific processing of packets, which thus are a "user specific rule stage." For example, if the result of the client discrimination stage is a determination that the user is not authenticated, the network entry device performs the user-specific rule of "deny[ing] the user access to the communications network" (acts 1314 and 1316). *Id.*, [0222], Fig. 13A(2). Method 1300 further performs user-specific rules by, after determining the identity and role

of the authenticated user, "configur[ing] the entry port module with the packet rules associated with the determined role" (act 1320). *Id.*, [0225], [0227], [0278], Fig. 13B. Finally, the network entry device perform a user-specific rule stage by applying, on packets received at act 1322, "the packet rules corresponding to the user from which the packet was received (i.e., user-based packet rules)." *Id.*, [0231], Fig. 13B.



Id., Figs. 13A(2) & 13B (annotated).

Method 1400 includes additional user-specific actions for processing a packet that are a user-specific rule stage. *Id.*, [0243], Fig. 14A(1)-14A(2), 14B. For example, user-specific rules include a determination of whether "user-based packet

rules dictate to drop [the] packet" (acts 1404 and 1406), whether to configure the "received packet ...according to user-based packet rules" (acts 1408 and 1410) or based on a combination of user-based rules and other rules (acts 1418, 1422, 1424, and 1426), and whether to apply "rate limiting to the received packet" (acts 1428 and 1430). *Id.*, [0247]-[0251]. The user-specific rule stage is discussed further in Section VII.A.5, *infra*.

4. at the client discrimination stage, extracting information associated with the user device from a header of the packet and associating the packet with user specific traffic control rules and user specific firewall rules; and

Richmond discloses, at the client discrimination stage (*e.g.*, acts 1310 and 1312 in Fig. 13A(2) and act 1401 in Fig. 14A(1)), the step of extracting information associated with the user device from a header of the packet (*e.g.*, MAC address or IP address) and associating the packet with user-specific traffic control rules and user-specific firewall rules (*e.g.*, Richmond's user-based packet rules). Ex1002, ¶¶88-102.

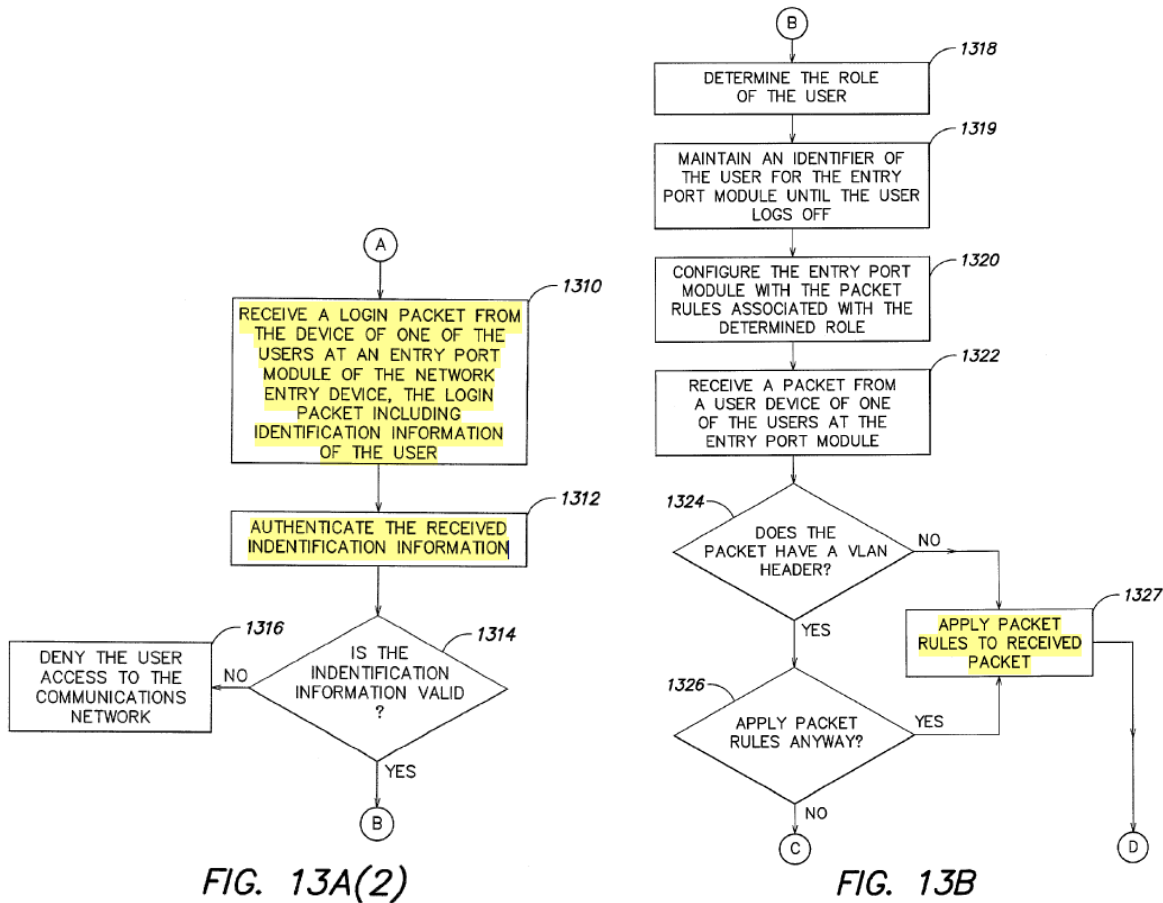
As one example of how Richmond meets this limitation, in acts 1310 and 1312, when a user seeks to access the network controlled by a network entry device, the user's device sends a "login packet" to a port module of the network entry device. Ex1003, [0217]. "[T]he login packet includ[es] identification information of [*i.e.*, associated with] the user" that sent it, such as "a user name, password, and other credential information corresponding to the user." *Id.*, [0215], [0217], [0219]. The

login packet also includes "location identifiers such as a MAC address or IP address or a device identifier." *Id.*, [0224]. These location identifiers are associated with the user device, because they identify the user's device on the network. Ex1002 ¶89.

A POSITA would understand that the portion of the packet that contains the MAC address or IP address is the packet header (either the Ethernet header or IP header, respectively). *Id.* ¶90. As discussed in Section III, *supra*, packet-switched networking protocols such as Ethernet and IP require that a source device include the source and destination addresses at fixed locations in the packet header. *Id.* Accordingly, when Richmond discloses that its network entry devices may "examine the MAC source address and/or IP source address included in each received packet" (Ex1003, [0230]), a POSITA would understand this to disclose that the examined addresses are extracted from a header of the packet. Ex1002, ¶90.

The network entry device extracts this user-identifying information (such as MAC or IP address) from the packet in order to "determine an identity of the user of the user device from which the packet was received." *See* Ex1003, [0224]. The network entry device then sends a request to search "an authentication database 1508 ... for a user authentication entry 1528 corresponding to the identification information received in the login packet" (act 1312). *Id.*, [0220]. If the authentication database indicates that "the identification information [is not] valid" (act 1314), the network entry device will "deny the user access to the

communications network." *Id.*, [0221]-[0222], Fig. 13B. Otherwise, if the information is valid and the user is authenticated, the authentication database retrieves the role ID corresponding to the user and provide this to the network entry device (act 1318). *Id.*, [0223].



Id., Figs. 13A(2) & 13B (annotated).

Once the authentication database has authenticated a user, the network entry device stores a user identifier for that user (act 1319) until the user logs off, so that for later "packet[s] received at the entry port module ... the user identifier may be accessed to determine an identity of the user of the user device from which the packet

was received." *Id.*, [0224]. Richmond teaches that "the user identifier [that is stored by the network entry device] should include information that can be compared against information included in packets received at the entry port module, for example, a location identifier such as a MAC address or IP address or a device identifier." *Id.*, [0224]; *see also id.*, [0244] ("Act 1319 may include storing a MAC address and/or an IP address of a user device of a user, where such information was obtained [*i.e.*, extracted] from an authentication packet received from the user device of the user.").

Given a role ID of a valid user, the network entry device then associates the packet with user-specific traffic control rules and user-specific firewall rules by using the role associated with that user to search for matching user-based rules in a rule database 1514. *Id.*, [0267]. Specifically, "the port configuration logic [of the entry port module 1510] selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs" that are associated with the user. *Id.*, [0278]. "As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly." *Id.*, [0278]. A POSITA would understand that, by configuring port module 1510 according to rule set 1519 based on the received login packet, Richmond's system associates the packet (as well as subsequently received packets at that port module from the user) with the rules in the rule set 1519.

* * *

As a second example of how Richmond meets this limitation, after subsequent packets are received from a user device (act 1322, *see id.*, [0229]-[0230]), the network entry device determines the "identity of a user of the user device from which the packet was received" (act 1401). *Id.*, [0244].

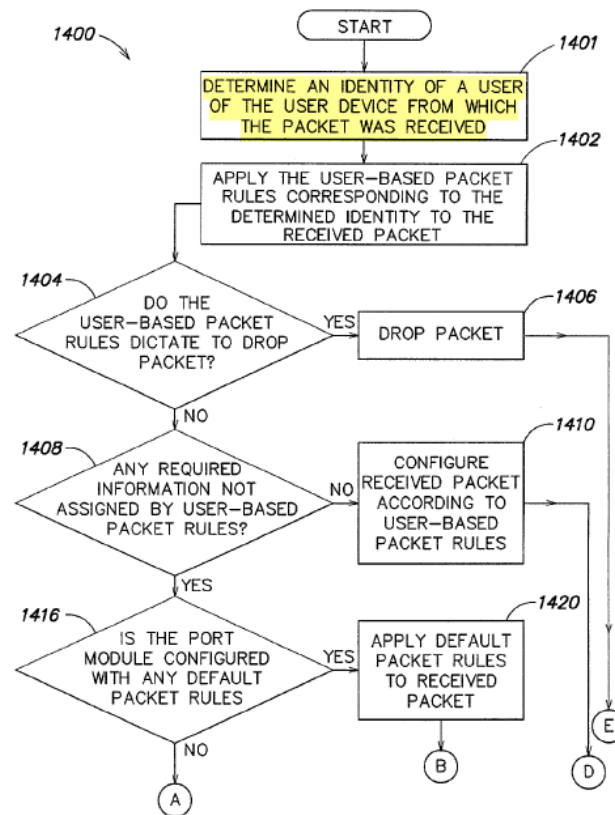


FIG. 14A(1)
FIG. 14A(2)
FIG. 14B

FIG. 14A(1)

Ex1003, Fig. 14A(1) (annotated).

Richmond teaches that a way of doing this is by "extracting the MAC address and/or IP address of the received packet and comparing it to one or more of the MAC

addresses and/or IP addresses maintained on the entry port module." *Id.*, [0244]. A POSITA would understand that such step constitutes extracting information associated with the user device from a header of the packet, because the MAC address and IP address are stored in the header, and because those identify the user device on the Ethernet and IP networks. Ex1002, ¶95.

Moreover, a POSITA would understand that the logical place from which to collect the user-identifying information is from the header, given this is where the MAC and IP addresses are located. *Id.*, ¶96. Accordingly, a POSITA reading Richmond's disclosure would understand that it is a straightforward design choice to extract information associated with the user (*e.g.*, MAC or IP address) from the packet's header. *Id.*

The network entry device then associates the received packet with user-specific traffic control rules and user-specific firewall rules, namely, the user-based rules that correspond to the user's role. *See* Ex1003, [0246] ("The user-based packet rules are packet rules corresponding to an identity of the user, for example, the one or more packet rules associated with the role or one or more service abstractions corresponding to the user."). As discussed further in Section VII.A.5, *infra*, the processing logic will process the packets according to the associated user-based rules.

* * *

A POSITA would understand Richmond's user-based packet rules to include both "user specific traffic control rules" and "user specific firewall rules." Ex1002 ¶¶98-99. The '639 Patent provides, as examples of user-specific traffic control rules, rules that enforce bandwidth rate limitations on users. *See, e.g.*, Ex1001, 8:13-15 ("A traffic rule can include any globally applicable traffic rule: for example, that the total used bandwidth of control device 20 must not exceed a particular amount."), 10:30-37 ("[U]ser specific rule 92 can point to traffic control rule 94 to govern bandwidth provisioning.... As an example, user profile 76 can specify that user 12 is entitled to 128 kbps up and 512 kbps down."), 11:66-67 ("Bandwidth limits can be enforced based on user specific traffic control rules."). Richmond discloses its user-specific rules may enforce bandwidth rate limitations on users. *See* Ex1003, [0010] ("Controlling usage of network resources may include ... **regulating bandwidth** on the network consumed by packets received from the user..."), [0159] ("[A]n entry of [packet rule] data structure 500 may specify a value such as 1 MB/sec... meaning that the number of bytes that may be transmitted ... during one second cannot exceed 1 MB.... The **consumption of bandwidth by a user also may be limited**...."). For example, Richmond discloses that rule entry 502 in rule data structure 500 may contain a "[r]ate limit field 520" that "store[s] a value representing a rate limit to be applied to a packet if it satisfies the rule." *Id.*, [0158]. Such rules are exemplary "user specific traffic rules." Ex1002 ¶¶99-100.

The '639 Patent provides, as examples of user-specific firewall rules, rules that block traffic to or from particular destinations or sources. *See, e.g.*, Ex1001, 8:10-12 ("A firewall rule can include ... for example, that all packets destined for a particular web site will be blocked."). Richmond discloses that its user-specific rules may include firewall rules that block traffic to or from particular destinations or sources. *See, e.g.*, Ex1003, [0010] ("Controlling usage of network resources may include, ... denying one or more packets access to any network resources ... [and] denying access to certain network resources ..."), [0035]-[0036] ("The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet..."), [0112] ("Such distributed firewall reduces use of network resources from users exchanging packets with resources external to the network by applying packet rules at each user's entry point to the network..."), [0230] (disclosing rule that "drop[s] any received packets that are not from a specific user's device"). Richmond discloses that rule data structure 500 may include a "Deny field 518" that "may specify that a packet is to be dropped." *Id.*, [0157]. "For example, a packet rule may specify that if a logical port number identified in the packet corresponds to a particular application, the packet is to be dropped." *Id.*, [0157]. "Using field 518, a network administrator may configure a packet rule to prevent certain users from using particular applications such as sensitive business

applications running on the network or games residing on the network." *Id.*, [0157].

Such rules are exemplary "user specific firewall rules." Ex1002, ¶¶101-102.

5. **at the user specific rule stage, accessing the user specific traffic control rules and user specific firewall rules based on the extracted information associated with the user device and applying the user specific traffic control rules and the user specific firewall rules to the packet as governed by at least one user specific class of service rule associated with the user on the user device in the first network.**

Richmond discloses, at the user specific rule stage (*e.g.*, acts 1402 and later in method 1400), accessing user specific traffic control rules (*e.g.*, Richmond's user-based packet rules that limit a user's bandwidth allocation) and user specific firewall rules (*e.g.*, Richmond's user-based packet rules that limit access to specific websites) based on the extracted information associated with the user device (*e.g.*, MAC or IP address) and applying the user-specific traffic control rules and the user-specific firewall rules to the packet as governed by at least one user-specific class of service rule associated with the user (*e.g.*, service abstraction assigned to the user's role(s)) on the user device in the first network (*e.g.*, Network 100). Ex1002, ¶¶103-111.

As discussed in Section VII.A.4, *supra*, after a user is successfully authenticated, the entry port module is configured with user-based packet rules corresponding to that user's associated roles and service abstractions. Subsequently, the user's device sends additional packets, which are received by the entry port module of the network entry device (act 1322). Ex1003, [0229]. In Richmond's

system, the port modules of the network entry devices (exemplary control devices) contain "processing logic ... for processing packets sent to and received at the port module." *Id.*, [0014]; *see also id.*, [0270]-[0271] (same).

After a packet is received, the port processing logic 1516 of the network entry device accesses those user-based packet rules in order to apply them to the incoming packets. *Id.*, [0270], [0231]. The port processing logic determines which rules to apply by comparing the extracted information associated with the user device (such as the packet's source or destination MAC address or IP address) to fields in the rule. *See, e.g., id.*, [0033], [0224], [0230], [0241]. "For example, one of the packet rules associated with the role of such user may be defined to examine the MAC source address and/or IP source address included in each received packet and to drop the packet if it is not equal to the MAC address and/or IP address, respectively, of the user...." *Id.*, [0230].

As shown in acts 1402 and later in Figures 14A(1), 14A(2), and 14B, the port processing logic applies the user-based packet rules to the incoming packet. As one example of applying a user-based packet rule, the logic determines whether the user-based packet rules dictate to drop the packet (act 1404), and if so, drop the packet (act 1406), with the result that the network traffic is blocked. *Id.*, [0247].

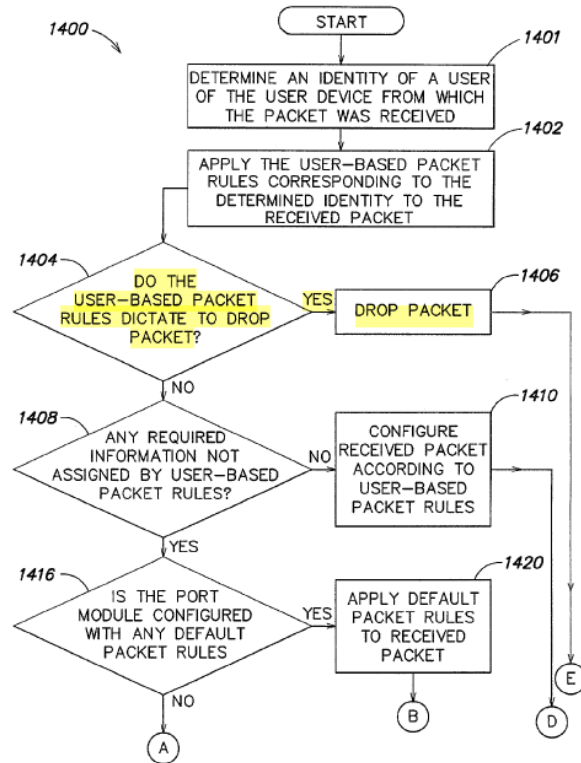


FIG. 14A(1)
 FIG. 14A(2)
 FIG. 14B

FIG. 14A(1)

Id., Fig. 14A(1) (annotated).

A user-based rule that drops packets has its "deny field 518" set to "deny access to the resources of [the] communications network by a packet that satisfies [the] conditions" specified in the rest of the rule, such as the source or destination address or port numbers. *Id.*, [0157]; *see also id.*, [0166]. The deny field can be used to prevent a user from "using particular applications such as sensitive business applications ... or games." *Id.*, [0157]. Such a rule constitutes a "user specific firewall rule." Ex1002 ¶107.

As another example of applying a user-based packet rule, the logic determines if user-based packet rules dictate that rate limiting should be applied to the received packet (act 1428), and if so, applies rate limiting to slow the rate of network traffic (act 1430) instead of immediately forwarding the packet to its next destination (act 1432). Ex1003, [0159], [0249]-[0251].

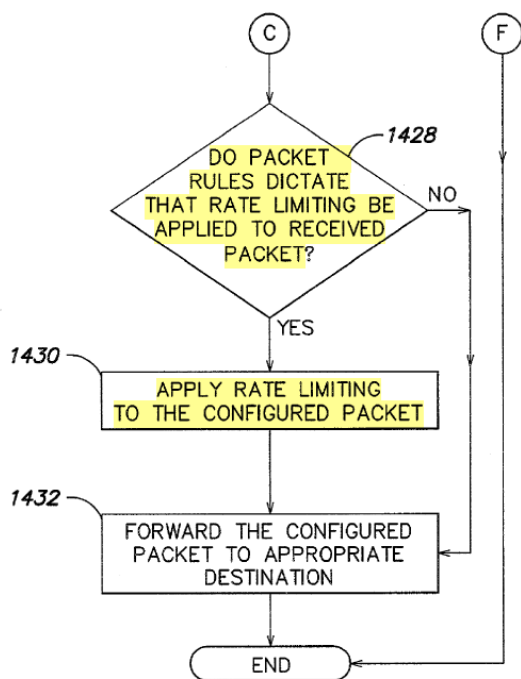


FIG. 14B

Id., 14B (annotated).

Such rules may specify, for example, "a threshold volume of bytes that may be received [from a user device] during a specified temporal interval (*e.g.*, one second)." *Id.*, [0158]; *see also id.*, [0159] (providing exemplary traffic control rule

specifying "the number of bytes that may be transmitted ... during one second cannot exceed 1 MB"). When such rule is active, the network control device may "drop some or all of the bytes of a packet ... that exceeds the threshold amount during the unit interval." *Id.*, [0159]. Such rules constitute user-specific traffic control rules, as they control the amount and rate of traffic that a user may send or receive through the network. Ex1002 ¶109.

Richmond's user-specific rules (both firewall and traffic-control rules) are governed by service abstractions, which are exemplary user-specific class of service rules associated with the user. Ex1002, ¶110. As discussed, Richmond's service abstractions allow a network administrator to define a class of service for applications or users by aggregating a collection of individual packet rules. *Id.*, [0116]-[0118]. For example, as shown in Figure 2, various packet rules may be assigned to define a "high-priority" class of service (items 208 and 212) that prioritizes traffic for specific applications. Conversely, other classes of service may block certain applications (*e.g.*, service 210 labelled "NO SNMP" blocks SNMP traffic). *Id.*, [0141].

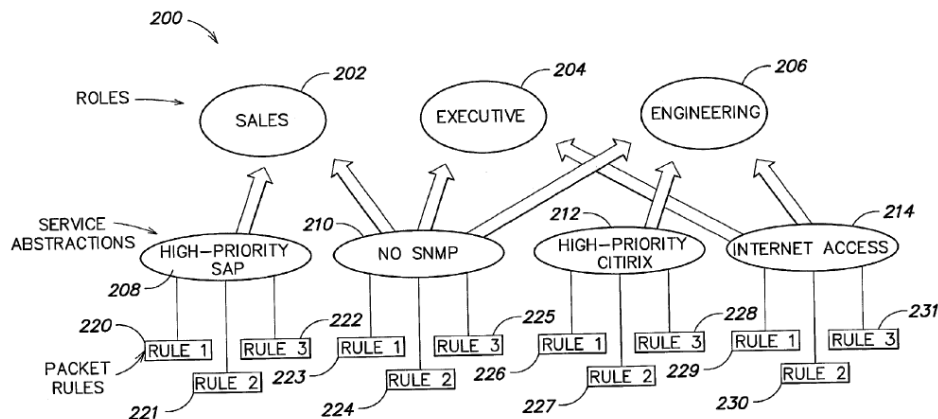


FIG. 2

Id., Fig. 2.

The service abstractions (and thus the packet rules) that are applied at any given time are dependent on the user's role. *See id.*, [0121], [0132], [0139]. Thus, the application of the corresponding rules is user specific.

B. Dependent Claim 2

1. The method according to claim 1, wherein the plurality of stages further comprises an interface specific stage, further comprising: at the interface specific stage, applying interface specific rules to the packet based on a type of a network interface over which the packet is received.

Richmond discloses and renders obvious claim 1, as discussed. Richmond further discloses and renders obvious that the plurality of stages further comprises an interface-specific stage, and that the method further comprises, at the interface-specific stage, applying interface-specific rules (*e.g.*, authentication states, default rules, other rules) to the packet based on a type of network interface over which the packet is received (*e.g.*, dedicated/shared wired or wireless). Ex1002, ¶¶112-118.

In Richmond's system, each network interface is controlled by a "port module" corresponding to that interface. Ex1003, [0014]. Each port module (including "entry port modules" that receive packets from user devices) may be configured individually, to apply a set of rules to traffic through that network interface that is not user-specific. *Id.*, [0014], [0023], [0041]. Such rules are "interface specific rules" instead of "user specific rules." *See id.*, [0231] (contrasting "user-based packet rules" and "default rules"), [0246] ("A user-based packet rule is distinguished from a default packet rule or any other type of rule that is not based on an identity of a user.").

As one example of interface-specific rules, each packet at a port module may also have applied to it "other additional rules with which the entry port module is configured." *Id.*, [0253]; *see also id.*, [0256] (same), [0253] (such rules may include "rules in accordance with ... IEEE 802.1D and/or 802.1Q"), [0257] ("other rules may have applied rate limiting to the packet").

As a second example of interface-specific rules, a port module may be set with a state of "authentication off/port on" state (which applies a rule allowing packets to pass regardless of authentication), "authentication on/port off" state (which applies a rule blocking packets if not authenticated), or "authentication on/port on with default behavior" (which applies a rule allowing unauthenticated packets to pass for "some basic network services, such as access to the Internet or access to a word

processing application," or "assign[ing] a lower priority"). *Id.*, [0208]-[0210]. A POSITA would logically choose this setting according to the interface type, recognizing that different interface types have different security issues, warranting (for example) stricter security for wireless as compared to wired interface types. Ex1002, ¶115.

As a third example of interface-specific rules, a port module may be configured with a "default rule," which applies rules to all packets received at the port module. *See, e.g.*, Ex1003, [0252] (default rule may "assign a default priority to all packets received at the entry port module"), [0254] (act 1416 applying default rules)

For any of the aforementioned interface-specific rules, the stage of processing that applies to them constitutes an "interface specific stage." *See, e.g., id.*, Fig. 14A(1) (act 1420), Fig. 14A(2) (acts 1418, 1424, 1426). Richmond discloses that the particular interface-specific rules to be applied may vary based on the type of network interface, such as a dedicated wired, shared wired, or shared wireless communication media. *See, e.g., id.*, [0021]-[0023] (explaining that port modules for wired media and for wireless media process packets differently), [0207], [0263]-[0264], [0270], [0288].

To the extent that the claim limitation is interpreted to require different rules are to be applied to different interfaces based on the different protocols/media used

for each interface (*e.g.*, different interface-specific rules for dedicated wired interfaces versus shared wireless interfaces), such an implementation would have been obvious to a POSITA. Ex1002, ¶118. A POSITA would have known about the need to deal with different scenarios arising for different network protocols, based on their unique characteristics. *Id.* For example, shared WiFi networks may need greater security because they can be accessed by a person in the vicinity of an access point, whereas dedicated Ethernet networks can only be accessed by individuals with physical access to the network port. *Id.* Indeed, Richmond expressly teaches about the benefits of applying different rules based on the type of network protocol. Ex1003, [0230] (teaching that for a "shared transmission medium," "it may be desirable ... to drop any received packets that are not from a specific user's device").

Thus, a POSITA would understand the need to apply different rules to different types of interfaces in Richmond's system based on the type of media. Ex1002, ¶118. This can be done without modifying Richmond's system, as each port module may be configured individually.

C. Dependent Claim 3.

- 1. The method according to claim 2, wherein the plurality of stages further comprises a global stage, further comprising:**

at the global stage, applying global firewall rules to the packet.

Richmond discloses and renders obvious claim 2, as discussed. Patent Owner has contended in the district-court litigation that "global stage" in this claim should be construed as "a global stage, distinct from the client discrimination stage and distinct from the user specific stage." Whether or not this construction is adopted, Richmond further discloses and renders obvious that the plurality of stages further comprises a global stage, and that the method further comprises, at the global stage, applying global firewall rules to the packet. Ex1002, ¶¶119-122.

Richmond discloses that all packets transiting a network entry device are received at and processed by a port module, which (as discussed for claim 2) applies a set of interface-specific rules to all traffic that is received by that port module (*e.g.*, authentication state, default rules, other rules). *See, e.g.*, Ex1003, [0208]-[0210], [0253]-[0257]. As discussed for claim 1 (*see* Section VII.A.4, *supra*), the rules may include firewall rules, such as blocking certain types of applications or devices for unauthenticated users. *See id.*, [0210], [0212]. A POSITA would understand that where all port modules have been configured with the same firewall rule (*e.g.*, when all port modules have been configured to the "authentication on/port off" blocking traffic for unauthenticated users, *see id.*, [0209]), that constitutes a global firewall rule, and the functionality that applies it to a global stage. Ex1002, ¶120. Moreover, Richmond describes these authentication-stage rules as distinct from user-based

packet rules, such that their application occurs in a stage distinct from the client-discrimination stage (*e.g.*, act 1401) and the user-specific rule stage (*e.g.*, acts 1402 and later), thus meeting the limitation under Patent Owner's construction. *Id.*

Richmond discloses use of a global firewall to apply the same rules to all packets, and that this was conventional in the prior art. Ex1003, [0035] ("Use of a firewall (*e.g.*, firewall 140) is another example of a technique for controlling usage of network resources..."), [0036]-[0037]. A POSITA understands that traditional firewalls apply global rules to each packet, as opposed to user-specific or interface-specific rules. Ex1002, ¶121. A POSITA moreover understands that a firewall includes significant flexibility in the types of rules that can be created, and that such rules would include global rules (*i.e.*, those applied to all packets, as was conventional in the prior art, as opposed to Richmond's user-specific or interface-specific rules). *Id.* A POSITA would further understand that the traditional firewall disclosed in Richmond processes its global rules in a stage distinct from the stages that process Richmond's user-based rules. *Id.*

Further, Richmond renders obvious that its network entry devices have a global stage that applies global firewall rules. *Id.* ¶122. A POSITA would be motivated to use traditional global firewall rules with Richmond's user-specific and interface-specific rules because the use of global rules allows for simpler configuration of the network. *Id.* For example, if a network administrator wants to

block all traffic to certain websites or for certain applications, regardless of which interface it is received on, it would be easier for the administrator to set a global firewall rule once, instead of setting interface-specific firewall rules for each port module. *Id.* Such change would be a combination of prior-art elements (*e.g.*, Richmond's network entry device and traditional firewalls) that yield predictable results. *Id.* Moreover, Richmond discloses that its disclosure is applicable to traditional firewalls, which may co-exist with network entry devices. Ex1003, [0205]-[0206], [0262]. It would also be an obvious implementation detail to process these global rules in a separate stage from the user-specific rules, as such rules do not need to discriminate clients or otherwise access user-specific rules or other user-specific information. Ex1002 ¶122. Such an implementation with distinct stages would be straightforward for a POSITA to implement, with a reasonable expectation of success, as it is the same type of implementation used in traditional firewalls that do not discriminate clients. *Id.*

D. Dependent Claim 4 (Ground 2 Only)

- 1. The method according to claim 1, wherein the packet is processed utilizing a provisioning module running on the control device, wherein the provisioning module comprises a first table for interface specific rules, a second table for global rules, and a third table for user specific rules.**

Richmond discloses and renders obvious claim 1, as discussed. Richmond further renders obvious that the packet is processed utilizing a provisioning module

running on the control device (e.g., network interface device), wherein the provisioning module comprises a first table for interface-specific rules, a second table for global rules, and a third table for user-specific rules. Ex1002, ¶¶123-125.

Richmond discloses that its rules are stored in "packet rule data structure 500," which "may be a table of a relational database." Ex1003, [0150], Fig. 5. A POSITA would understand that a relational database comprises an arbitrary number of tables, each with its own set of columns (individual data fields) and variable number of rows (data entries). *Id.*, Figs. 5-7; Ex1002, ¶124. For example, Richmond discloses that the service abstractions and roles may be stored in separate tables within the relational database. Ex1003, [0170], [0175], Figs. 6-7.

504 NAME	506 STATUS	508 TYPE	510 VALUE	512 MASK	514 VLAN	516 PRIORITY	518 DENY?	520 RATE LIMIT	522 LAYER
CONTAIN SUBNET 54	ENABLED	IP ADDRESS BILATERAL	10.20.54.0	255.255.255.0	5	7	NO	NONE	3

FIG. 5

604 NAME	606 RULE 1	608 RULE 2	610 RULE 3	612 RULE 4
CONTAIN IP ENG SUBNET TRAFFIC	CONTAIN SUBNET 54	CONTAIN SUBNET 55	CONTAIN SUBNET 56	CONTAIN SUBNET 57

FIG. 6

704 NAME	706 DEFAULT VLAN	708 DEFAULT PRIORITY	710 SERVICE 1	712 SERVICE 2	714 SERVICE 3
ENGINEERING	5	NONE	CONTAIN DHCP	CONTAIN ICMP	CONTAIN IP ENG SUBNET TRAFFIC
...					

FIG. 7

It would be obvious in light of Richmond's disclosures to store each type of rule (interface-specific, global, and user-specific) in its own table of a relational database. This would be a routine implementation detail. Ex1002, ¶125. A POSITA would understand that rule sets could be stored in the database in a variety of ways. *Id.* Moreover, a POSITA would understand that it would be more efficient to store such rules in independent tables (as claimed), because not all the rules require the same information; for example, global rules and interface-specific rules do not need to store a user's MAC or IP address (*e.g.*, field 510), and a global rule does not need to store the interface with which it is associated. *Id.* Thus, by using separate tables in a relational database, each table can be optimized to just store the columns/fields appropriate for that rule type. *Id.* This constitutes a simple substitution of known elements (*e.g.*, three relational database tables in place of one table). *Id.* A POSITA would have a reasonable expectation of success, as it is well known to a POSITA how to create and subsequently access additional tables in a relational database (such as that disclosed in Richmond). *Id.*

E. Dependent Claim 5

- 1. The method according to claim 1, wherein the user device is assigned with an Internet Protocol (IP) address in the first network and wherein the at least one user specific rule is associated with the IP address.**

Richmond discloses and renders obvious claim 1, as discussed. Richmond further discloses and renders obvious that the user device is assigned with an Internet

Protocol (IP) address in the first network, wherein the at least one user-specific rule is associated with the IP address. Ex1002, ¶¶126-130.

It is the case in all Internet Protocol-based networks that each networked user device is assigned an IP address, as is well-known to a POSITA (both now and prior to the patent's filing date). *Id.*, ¶127. Each networked device must have an IP address to identify it within that network. *Id.* Each IP packet sent to or received from the networked device thus contains the device's IP address in its destination or source field, in order to properly direct and recognize the packet. *Id.*

Richmond's user devices send and receive packets containing the IP address with which they are assigned, consistent with the POSITA's understanding of what was inherent in all IP-based networks. *See* Ex1003, [0224] (explaining that "information included in packets received at the entry port module" includes "for example, a location identifier such as a MAC address or IP address or a device identifier"), [0230] (disclosing there is a "MAC Source address and/or IP Source address included in each received packet," which can be compared to "the MAC address and/or IP address, respectively, of [*i.e.*, assigned to] the user").

In one embodiment of Richmond's system, user-based packet rules are defined in packet rule data structure 500, which contains entries 502 corresponding to individual rules, each entry containing various fields. *Id.*, [0150]-[0151]. When field 508 of an entry is set to "IPAddress Bilateral," this "specif[ies] that the source

and destination (i.e., bilateral) IP addresses of a packet are to be examined" in order to see if the rule should be applied. *Id.*, [0162]. For example, field 510 shown in Figure 5 "specifies that the value to be compared to the IP addresses of the received packet [in order to determine whether to apply the rule] is '10.20.54.0.'" *Id.*, [0163]; *see also id.*, [0154]. Thus, the rule shown in Figure 5 is associated with a particular IP address.

NAME	STATUS	TYPE	VALVE	MASK	VLAN	PRIORITY	DENY?	RATE LIMIT	LAYER
CONTAIN SUBNET 54	ENABLED	IP ADDRESS BILATERAL	10.20.54.0	255.255.255.0	5	7	NO	NONE	3

FIG. 5

Ex1003, Fig. 5 (annotated).

Richmond provides additional examples of rules associated with a user's IP address; for example "one of the packet rules associated with the role of such user may be defined to examine the MAC Source address and/or IP Source address included in each received packet and to drop the packet if it is not equal to the MAC address and/or IP address, respectively, of the user." *Id.*, [0230]; *see also id.*, [0244] (similar rule comparing address to those previously stored from authentication packet).

F. Dependent Claim 6

- 1. The method according to claim 5, wherein the user device is associated with a media access control (MAC) address and**

wherein the at least one user specific rule is further associated with the MAC address.

Richmond discloses and renders obvious claim 5, as discussed. Richmond further discloses and renders obvious that the user device is associated with a media access control (MAC) address, wherein the at least one user-specific rule is further associated with the MAC address. Ex1002, ¶¶131-134.

It is the case in all Ethernet-based networks that each networked user device is assigned a MAC address, as is well-known to a POSITA (both now and prior to the filing date of the patent). Ex1002, ¶132. It is necessary for each networked device to have a MAC address so that they can be uniquely identified within that network. *Id.* Each Ethernet packet sent to or received from the networked device contains the device's MAC address in its destination or source field, in order to properly direct and recognize the packet. *Id.*

Richmond's user devices send and receive packets containing the MAC address with which they are assigned, consistent with the POSITA's understanding of what was inherent in all Ethernet-based networks. *See* Ex1003, [0224] (explaining that "information included in packets received at the entry port module" includes "for example, a location identifier such as a MAC address or IP address or a device identifier"), [0230] (disclosing that there is a "MAC Source address and/or IP Source address included in each received packet," which can be compared to "the MAC address and/or IP address, respectively, of [*i.e.*, assigned to] the user").

Richmond provides examples of rules associated with a user's MAC address; for example "one of the packet rules associated with the role of such user may be defined to examine the MAC Source address and/or IP Source address included in each received packet and to drop the packet if it is not equal to the MAC address and/or IP address, respectively, of the user." *Id.*, [0230]; *see also id.*, [0244] (similar rule comparing address to those previously stored from authentication packet).

G. Dependent Claim 7

- 1. The method according to claim 1, wherein the user specific traffic control rules and the user specific firewall rules are established for the user based on a user profile that includes parameters that determine an extent of the user's access to the second network, services available to the user, or a combination thereof.**

Richmond discloses and renders obvious claim 1, as discussed. Richmond further discloses and renders obvious that the user specific traffic control rules and the user specific firewall rules are established for the user based on a user profile (*e.g.*, the information in relationship database 410 regarding the user's role and associated service abstractions) that includes parameters that determine an extent of the user's access to the second network, services available to the user, or a combination thereof. Ex1002, ¶¶135-137.

As discussed (Section VI.A, *supra*), users in Richmond's system are assigned to roles, each of which has associated service abstractions. *Id.*, [0116]-[0118]. This information is stored in relationship database 410. *Id.*, [0149]-[0150], [0170],

[0175]. The information stored regarding a user, including the user's roles and service abstractions, is an exemplary user profile. These include parameters that determine a user's access to the second network (*e.g.*, the Internet 148). For example, as shown in Fig. 2, users with sales role 202 may be excluded from the "Internet Access" 214 service abstraction, and therefore blocked from accessing the Internet. However, users in executive role 204 or engineering role 206 are not blocked from accessing the Internet. Even for users whose profile allows them general internet access, their access to that network may be limited by rules that block certain websites or applications, as shown:

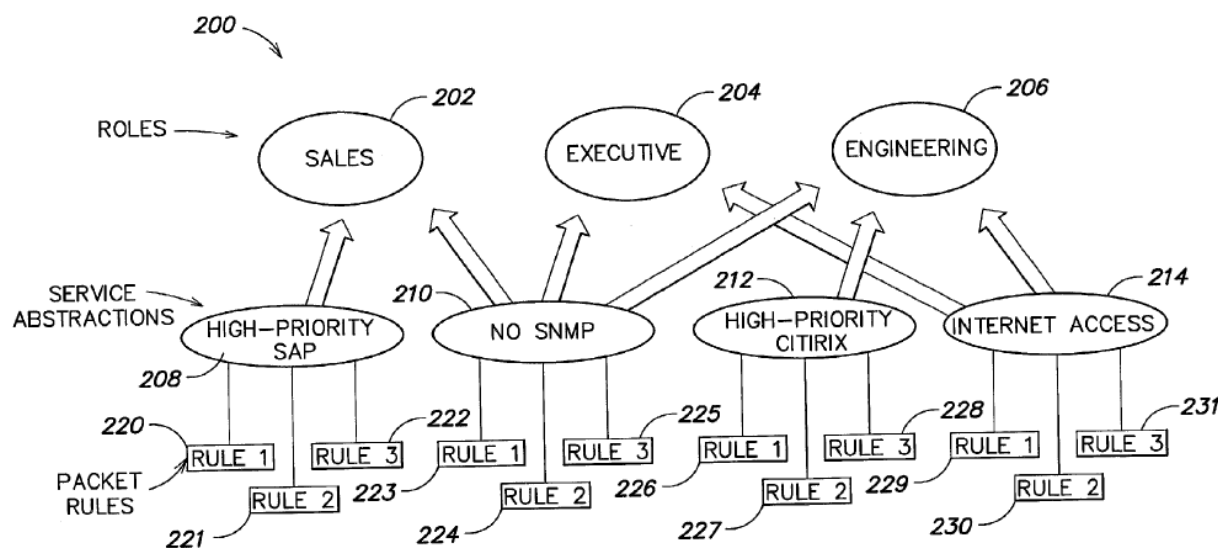


FIG. 2

Ex1003, Fig. 2; Ex1002, ¶136.

The user profiles additionally contain parameters that determine services available to the user. As also shown in Fig. 2, the "High-Priority SAP" service and

"High-Priority Citirix [*sic*]" service may be limited to users in the sales role 202 or engineering role 206, respectively. Similarly, all non-administrators may be blocked from using the SNMP service. Ex1003, [0141], Fig. 2.

H. Dependent Claim 8

1. A method according to claim 1, further comprising determining whether the user has authenticated.

Richmond discloses and renders obvious claim 1, as discussed. Richmond further discloses that its method includes the step of determining whether the user has authenticated. Ex1002, ¶¶138-142.

For example, Richmond discloses its system has an "authentication module 1506," shown in Fig. 15B, which "may be configured to perform authentication in accordance with one or more authentication technologies." Ex1003, [0274].

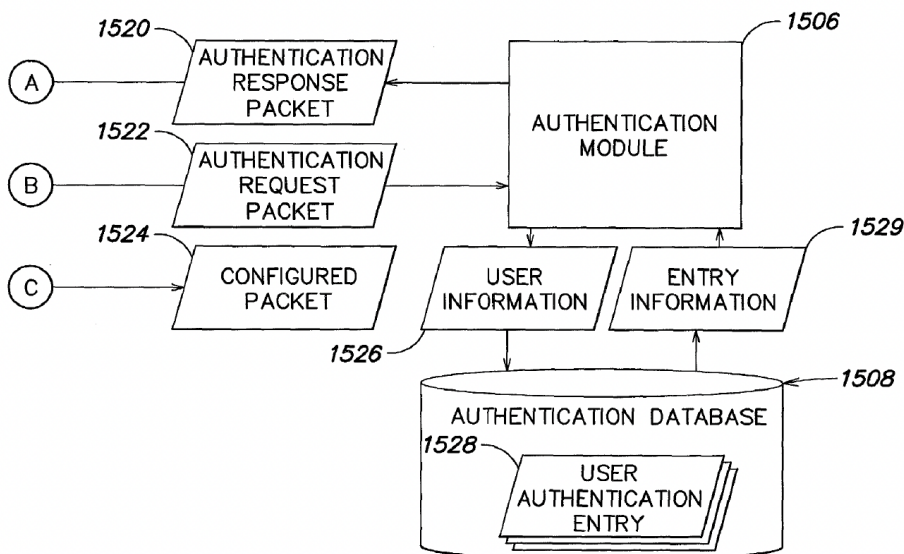


FIG. 15B

The network entry device sends identity information to authentication module 1506, which stores a database containing the credentials of each user and their roles. *Id.*, [0273]-[0275]. If the credentials are invalid, the network entry device denies the user access. *Id.*, [0222], Fig. 13A(2) (acts 1314 and 1316). If the credentials are valid (*i.e.*, the user has authenticated), the authentication module informs the network entry device of the user's roles, which then configures its entry port modules with user-based packet rules corresponding to the user's identity and corresponding roles and service abstractions. *Id.*, [0223], [0277]-[0279]. Subsequently, when the user sends packets, the network entry device processes the packets according to these pre-configured user-based rules. *Id.*, [0280]-[0281], Fig. 13B (act 1327).

Richmond further discloses that "[a] port module may be configured to have a state of 'authentication on/port off,' where a user must authenticate before using any network resources," or alternatively, "a state of 'authentication on/port on with default behavior,' where a user may be allowed to use some network resources before authentication or in the event of a failed authentication." *Id.*, [0209]-[0210]. Thus, the network entry device must determine whether the user has authenticated in order to apply the correct behavior according to these states. Ex1002, ¶141.

Additionally, Richmond discloses a packet rule that filters packets based on whether their MAC address and/or IP address matches those of authenticated users.

Ex1003, [0230]. Such rule acts to determine whether the user has been authenticated and drops packets of those users that are not. Ex1002, ¶142.

I. Dependent Claim 9

- 1. A method according to claim 8, wherein the user has not authenticated, further comprising: redirecting the user to a login web page that requests user credentials; and using the user credentials received from the user to authenticate the user.**

Richmond discloses and renders obvious claim 8, as discussed. Richmond further discloses and renders obvious that wherein the user has not authenticated, redirecting the user to a login web page that requests user credentials and using the user credentials received from the user to authenticate the user. Ex1002, ¶¶143-145.

In Richmond's method 1300, the network entry devices receive "identification information ... includ[ing] a user name, password and other credential information corresponding to the user," and that "the received identification information may be authenticated" using "a variety of authentication techniques." Ex1003, [0219]-[0220]. Richmond further discloses that "[i]n an embodiment of method 1300, various acts ... are performed as described in *Enterasys User Personalized Network*, a white paper available from Enterasys Networks, Inc., available on the filing date of this application at <http://www.enterasys.com/products/whitepapers>, the entire contents of which is hereby incorporated by reference." *Id.*, [0239]. Accordingly, the disclosures of this Enterasys Whitepaper are part of Richmond's disclosure "as

if [they] were explicitly contained therein.” *Arbutus Biopharma Corp. v. ModernaTX, Inc.*, 65 F.4th 656, 662–63 (Fed. Cir. 2023).¹

According to the Enterasys Whitepaper, Richmond's system "provid[es] two primary mechanisms for authenticating users" that have not already authenticated, including "the use of web-based authentication." Ex1007, 15. In such method, "[u]sers who want to receive network [s]ervices access [*i.e.*, are redirected to] a secure web page ... from a browser [and] are asked to provide username and credentials." *Id.* This is an exemplary login webpage that requests user credentials. Ex1002, ¶145. "These credentials are then forwarded on to a RADIUS server, which either authenticates them, or forwards the request to the appropriate authenticator," (Ex1007, 15), thereby using the received user credentials to authenticate the user.

J. Independent Claim 10

Richmond discloses and renders obvious all limitations of claim 10. The limitations of claim 10 are largely identical to those of claim 1, with the only

¹ The Enterasys Whitepaper was submitted to the USPTO on September 20, 2002 with Richmond's application, attached to an Information Disclosure Statement stating the whitepaper was publicly available since February 12, 2001. *See* Ex1007 (excerpt of Richmond's file history), 1-2; *see also* Ex1006 (color copy of Enterasys Whitepaper).

substantive difference being that, whereas claim 1 is directed to a method, claim 10 is directed to a computer program that performs the method when executed on a processor. Ex1002, ¶146. Accordingly, the analysis for this claim primarily incorporates by reference the discussion above for claim 1.

1. A computer program product comprising at least one non-transitory computer-readable storage medium storing computer instructions translatable by a processor of a control device to perform:

To the extent the preamble is limiting, Richmond discloses a computer program product comprising at least one non-transitory computer-readable storage medium storing computer instructions translatable by a processor of a control device to perform the recited steps of claim 10. Ex1002, ¶¶147-148.

Richmond discloses its methods (including methods 1300 and 1400) "may be implemented as a computer program product tangibly embodied as computer-readable signals on a computer-readable medium, for example, a non-volatile recording medium, an integrated circuit memory element, or a combination thereof." *Id.*, [0242]. Such signals may "define instructions, for example, as part of one or more programs, that, as a result of being executed by a computer, instruct the computer to perform one or more of the methods or acts described [in Richmond]." *Id.*, [0242]; *see also id.*, [0260] (disclosing same for Method 1400), [0047], [0147], [0062] & [0085] (disclosing that various embodiments of Richmond's system can be implemented as computer program products consisting of instructions stored on

storage medium). Richmond further specifies that "[t]he computer-readable medium on which such instructions are stored may reside on one or more of the components of network 100 described above in relation to FIG. 1 and/or system 1500 described below in relation to FIG. 15 [*i.e.*, the network entry device], and may be distributed across one or more of such components." *Id.*, [0242].

2. Remaining limitations

See Section VII.A.2-VII.A.5 (corresponding limitations for claim 1).

K. Dependent Claim 11

See Section VII.B.1 (claim 2).

L. Dependent Claim 12

See Section VII.C.1 (claim 3).

M. Dependent Claim 13

- 1. The computer program product of claim 10, wherein the computer instructions are further translatable by the processor to implement a control program on the control device, wherein the control program comprises a provisioning module, wherein the provisioning module comprises a traffic conditioning module for user specific allocation of bandwidth.**

Richmond discloses and renders obvious claim 10, as discussed. Richmond further discloses the computer instructions are further translatable by the processor to implement a control program on the control device, wherein the control program comprises a provisioning module, wherein the provisioning module comprises a

traffic conditioning module for user-specific allocation of bandwidth. Ex1002, ¶¶155-158.

As discussed for claim 10, Richmond's network device (an exemplary control device) may be implemented using a computer program. Ex1003, [0047], [0147], [0062], [0085], [0242], [0260]. Such a program constitutes a control program, as it controls the transmission of packets.

As discussed for claim 1 (*see* Sections VII.A.4 and VII.A.5, *supra*), Richmond's user-based packet rules include rules that enforce bandwidth rate limitations on users, based on the limits to which the user is allocated. *See* Ex1003, [0010], [0158] (disclosing that user-based packet rule has "[r]ate limit field 520 ... [that] store[s] a value representing a rate limit to be applied to a packet"), [0159] ("[A]n entry of [packet rule] data structure 500 may specify a value such as 1 MB/sec, for which a network device may be configured to interpret as meaning that the number of bytes that may be transmitted in packets that satisfy the conditions of 508-512 during one second cannot exceed 1 MB.... Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume....").

The network entry device's control program applies rate limiting according to these user-specific rules. *Id.*, [0158]-[0159], [0249]-[0251].

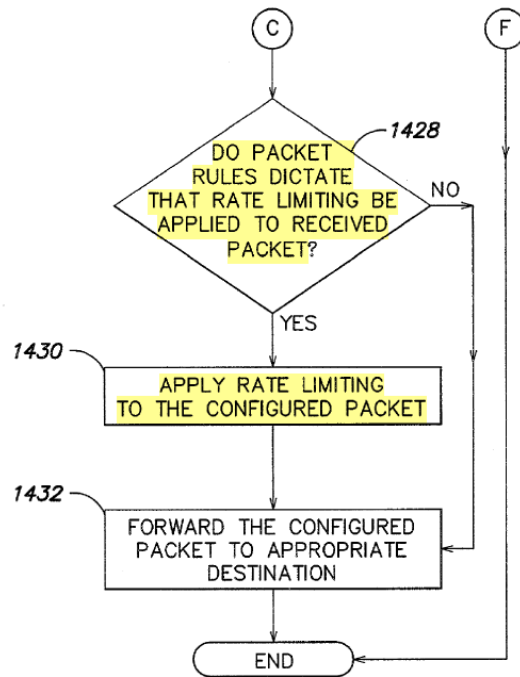


FIG. 14B

The network entry device's hardware, along with the portion of the control program that implements such functionality, constitutes an exemplary provisioning module, including the traffic conditioning module within the provisioning module. Ex1002, ¶158.

N. Dependent Claim 14

See Section VII.G.1 (claim 7).

O. Dependent Claim 15

See Section VII.H.1 (claim 8).

P. Dependent Claim 16

See Section VII.I.1 (claim 9)

Q. Independent Claim 17

Richmond discloses and renders obvious all limitations of claim 17. The limitations of claim 17 are largely identical to those of claim 1, with the only possibly substantive difference being that claim 17 is directed to a control device containing a storage medium that (just as in claim 10) stores computer instructions that, when executed, perform the method of claim 1. Ex1002 ¶162. Accordingly, the analysis for this claim primarily incorporates by reference the discussion above for claims 1 and 10.

1. A control device for network access control, comprising:

To the extent the preamble is limiting, Richmond discloses a control device for network access control (*e.g.*, network entry devices 114, 116, 120, 124, 144, and 1501). Ex1002, ¶163.

Richmond teaches that "[a] network entry device serves as an entry point to the network for at least one user," and that it "reside[s] at an edge or boundary of the communications network and provide[s] connectivity between network resources of the communications network and devices located external to the communications network," such as user devices. Ex1003, [0016]. As discussed above (*see* Sections VII.A.1-2), the network entry device (including its entry port modules) controls the traffic from user devices to the network and therefore acts as a control device for network access control.

2. a processor;

Richmond discloses that its control device (*e.g.*, network access device) comprises a processor. Ex1002, ¶164. For example, network access device 1504 comprises one or more entry port modules 1510, which in turn contain port processing logic 1516. *See, e.g.*, Ex1003, [0014] ("a 'port module' of a switching device includes ... port processing logic associated with the physical port."), [0270].

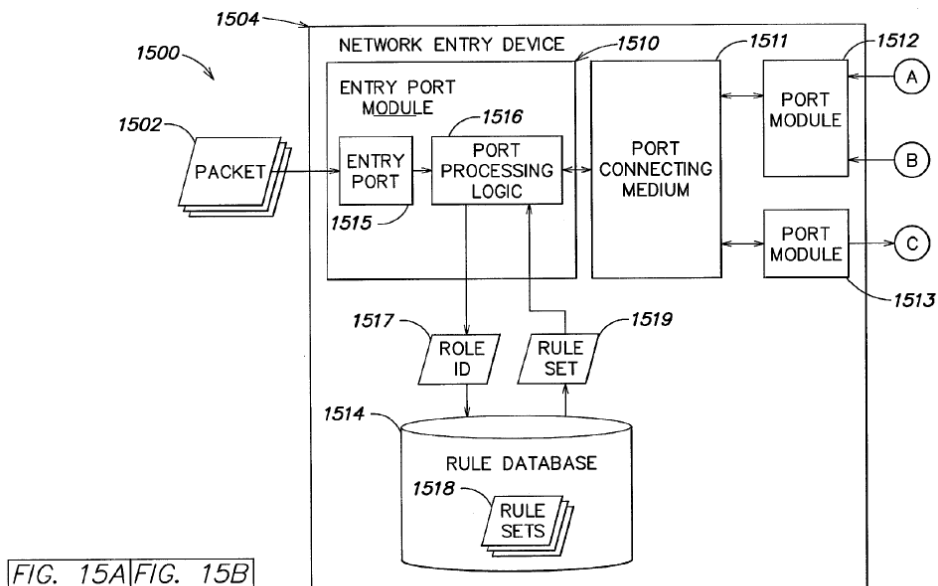


FIG. 15A

"Port processing logic 1516 may include switching logic, memory, and *one or more processors* (not shown) for configuring the port module and for processing packets sent to and received at the port module." *Id.*, [0270].

3. at least one computer-readable storage medium storing computer instructions translatable by the processor to perform:

See Section VII.J.1 (preamble of claim 10).

4. Remaining limitations

See Section VII.A.2-VII.A.5 (corresponding limitations of claim 1).

R. Dependent Claim 18

See Section VII.B.1 (claim 2).

S. Dependent Claim 19

See Section VII.C.1 (claim 3).

T. Dependent Claim 20

See Section VII.M.1 (claim 13).

U. Dependent Claim 22

- 1. The control device of claim 20, wherein the provisioning module further comprises a firewall module for associating the packet with the user specific firewall rules.**

Richmond discloses and renders obvious claim 20, as discussed. Richmond further discloses and renders obvious that the provisioning module further comprises a firewall module for associating the packet with the user-specific firewall rules. Ex1002, ¶¶173-174.

As discussed further for claim 1 (Section VII.A.4, *supra*), the network entry device utilizes an authentication database to authenticate a user (Ex1003, [0224]), and then associates that user with user-specific rules (including firewall rules) by searching in the rule database 1514 for those matching the role of a user (*id.*, [0267], [0278]). The port module is then configured with the rules, and subsequently, all packets received at that port module from the user are associated with the previously

configured rules. *See id.*, [0244], [0246]. The functionality in the port module that applies the firewall rules constitutes a "firewall module."

V. Dependent Claim 23

1. The control device of claim 20, wherein the provisioning module further comprises an authentication module for authenticating the user.

Richmond discloses and renders obvious claim 20, as discussed. Richmond further discloses and renders obvious that the provisioning module further comprises an authentication module for authenticating the user. Ex1002, ¶175.

Richmond discloses its system has an "authentication module 1506," shown in Fig. 15B, which "may be configured to perform authentication in accordance with one or more authentication technologies." Ex1003, [0274].

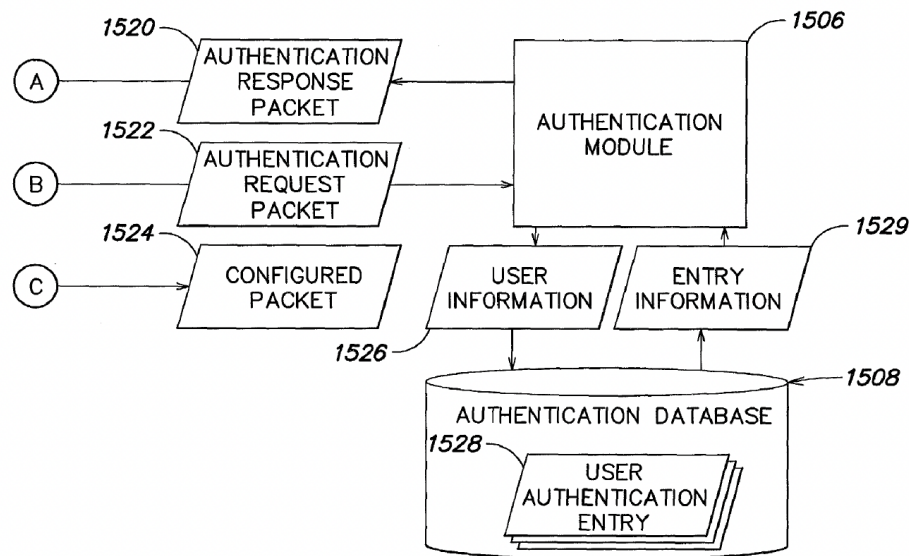


FIG. 15B

As discussed further in connection with claim 8 (*see* Section VII.H), the network entry device sends a user's identity information to the authentication module for authentication. *Id.*, [0273]-[0275].

W. Dependent Claim 24

See Section VII.G.1 (claim 7).

X. Dependent Claim 25

See Section VII.H.1 (claim 8).

Y. Dependent Claim 26

See Section VII.I.1 (claim 9)

Z. Independent Claim 27

Richmond discloses and renders obvious all limitations of claim 27. The limitations of claim 27 are largely identical to those of claim 17 and its dependent claims 25-26, which are apparatus claims that are substantively similar to method claims 1, 8, and 9. Ex1002, ¶179. Accordingly, the analysis for this claim incorporates by reference the discussion above for these claims.

- 1. A control device for network access control, comprising:
a processor;**

See Section VII.Q.1-2 (preamble and corresponding limitations of claim 17),

- 2. at least one computer-readable storage medium storing computer instructions translatable by the processor to perform:**

See Section VII.J.1 (claim 10 preamble).

3. **receiving a packet originating from a user device in a first network, wherein the first network is connected to a second network via the control device, and wherein the user device is associated with a user;**

See Section VII.A.2 (corresponding limitation of claim 1).

4. **determining whether the user has authenticated;**

See Section VII.H.1 (corresponding limitation of claim 8).

5. **if the user has not authenticated: redirecting the user to a login web page that requests user credentials; and using the user credentials received from the user to authenticate the user;**

See Section VII.I.1 (corresponding limitations of claim 9)

6. **processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;**

at the client discrimination stage, extracting information associated with the user device from a header of the packet and associating the packet with user specific traffic control rules and user specific firewall rules; and

at the user specific rule stage, accessing the user specific traffic control rules and user specific firewall rules based on the extracted information associated with the user device and applying the user specific traffic control rules and the user specific firewall rules to the packet as governed by at least one user specific class of service rule associated with the user on the user device in the first network.

See Sections VII.A.3-5 (corresponding limitations of claim 1).

VIII. GROUND 3 – CLAIMS 9, 16, 26, AND 27 ARE RENDERED OBVIOUS BY RICHMOND IN LIGHT OF WOOD

A. Dependent Claim 9

Richmond discloses and renders obvious claim 8, as discussed. Richmond in light of Wood renders obvious that when the user has not authenticated, redirecting the user to a login web page that requests user credentials and using the user credentials received from the user to authenticate the user. Ex1002, ¶¶185-192.

Richmond explains in its Abstract that its focus is on "[c]ontrolling a user's usage of network resources, *after the user has been authenticated*, without using any network resources beyond the user's entry point to the network." Ex1003, cover. Richmond's primary focus is thus on what occurs after authentication, and thus does not mandate a particular method of authentication. A POSITA would understand, in light of Richmond's disclosure of authentication, that they would need to implement some form of authentication in conjunction with Richmond's system. Authentication is a very well known function, and a POSITA would understand that there were many ways of authenticating users.

A POSITA would thus look to other prior-art references to better understand how authentication could be performed. One such reference is Wood which, like Richmond and the '639 Patent, are in the same technical field of controlling access to network resources. Ex1002, ¶187.

In Wood's system, user devices (e.g., "a browser 170 operated by a user") interact with the network via a "Gatekeeper and entry handler component 110," which "provides an entry point for external client applications requesting access." Ex1004, 5:10-15. When gatekeeper/entry handling component 110 receives packets from a user device attempting to access a particular website or application, the "gatekeeper/entry handler component 110 queries authorization component 140 to obtain authorization for access" to that application. *Id.*, 6:3-8.

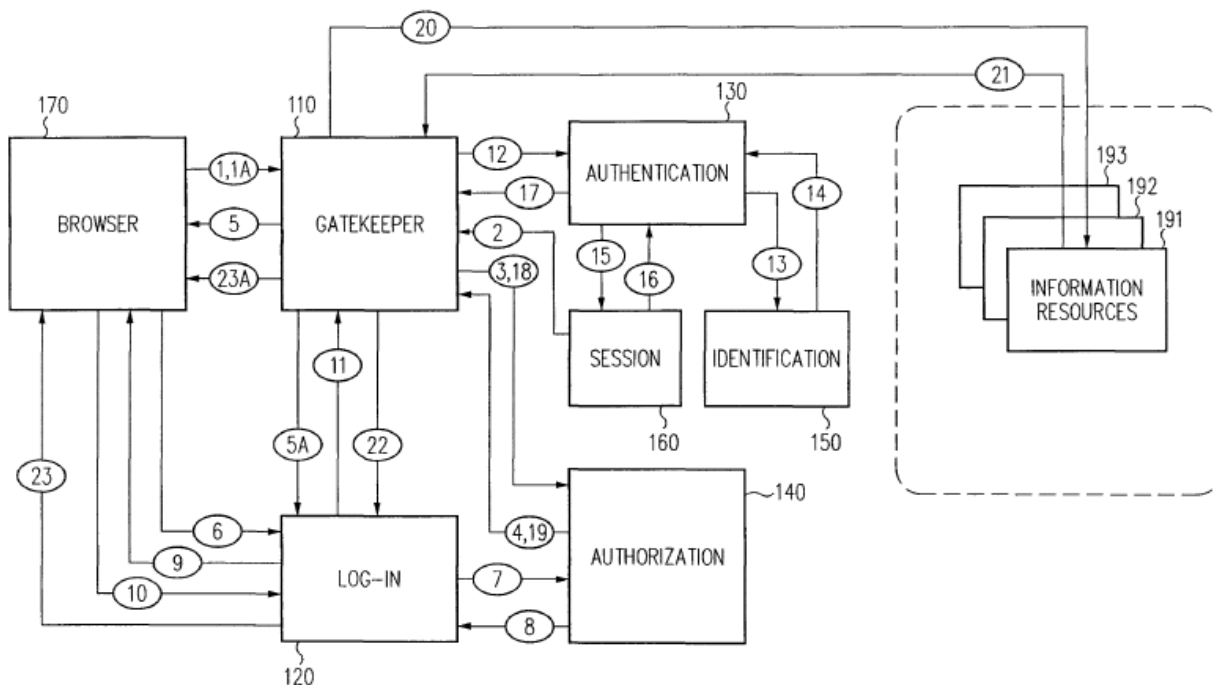


FIG. 1

If the user has not authenticated (or has an insufficient authentication level), "authorization component 140 may indicate that the access request is to be redirected to login component 120 so that login credentials may be obtained and authenticated to a particular trust level." *Id.*, 6:7-9; *see also id.*, 12:1-26 (disclosing that the

authentication module 130 sends a "REDIRECT response" indicating "to forward the access request to login component 120 so that sufficient login credentials may be obtained and authenticated").

Once the gatekeeper/entry handler receives a REDIRECT response, it "redirects (5) browser 170 to login component," such as by "using a client-side redirect via HTTP location directive to forward the request to login component 120." *Id.*, 12:23-29. The login component 120 then "supplies browser 170 with a login page (e.g., HTML) that prompts the user for an application specific user ID and a choice of authentication schemes." *Id.*, 13:37-38:1. This exemplary login webpage then requests user credentials. *See id.*, 14:3-9 (disclosing that "login component 120 may interactively allow a user to select from amongst the credential types (e.g., using any HTML-based dialog)," including "username/password pairs, onetime passwords, enigma challenge, etc.," which a user may supply through "entry into an HTML form"). Subsequently, the credential received from the user are "supplied (11) to gatekeeper/entry handler component 110 for authentication," in order to authenticate the user. *Id.*, 14:22-25.

A POSITA would be motivated to combine Richmond and Wood to achieve the benefits of Richmond's system for user-specific rules controlling network access, along with Wood's user-friendly authentication method. Ex1002, ¶¶191-192. A POSITA would understand that Wood's web-based authentication method is simple

for network administrators to set up, as web pages and web servers were readily available at the time, and a network administrator could use existing tools to design a login page, and existing web servers to provide the page (instead of designing a custom server for accepting user credentials). *Id.*, ¶191. A POSITA would understand that end users would find Wood's web-browser-based system easy to use, given that web browsers were ubiquitous on users' computers at the time (thus avoiding the need to install new software) as were webpage login systems (which thus were familiar to the end user). *Id.* A POSITA would be motivated to use Wood's system to achieve these benefits. *Id.*

The use of Wood's authentication method in Richmond's system would be a combination of prior-art elements according to known methods. Ex1002, ¶192. In the combination, users authenticate with the system (as explained in Wood) and then their traffic is monitored and controlled (as explained in Richmond). *Id.* These functions are discrete: how authentication is performed does not affect Richmond's operation and the functions of Richmond do not dictate a particular type of authentication. *Id.* Any modifications would be straightforward and not involve substantial alteration to Richmond's system, as Richmond's network entry device (as modified) would simply send an HTTP redirect (as in Wood) to the user upon determining (in the steps discussed for claim 9) that the user has not yet

authenticated. *Id.* Accordingly, a POSITA would have a reasonable expectation of success. *Id.*

B. Dependent Claims 16 and 26

Richmond discloses and renders obvious claims 15 and 25 on which these depend, and Richmond in light of Wood render obvious the additional limitations of these claims. *See* Section VIII.A (claim 9).

C. Independent Claim 27

Richmond in light of Wood renders obvious all limitations of claim 27. The limitations of claim 27 are largely identical to those of claim 17 and its dependent claims 25-26, which are apparatus claims that are substantively similar to method claims 1, 8, and 9. Ex1002, ¶195. Accordingly, the analysis for this claim incorporates by reference the discussion above for these claims.

- 1. A control device for network access control, comprising:
a processor;**

See Section VII.Q.1-2 (preamble and corresponding limitations of claim 17),

- 2. at least one computer-readable storage medium storing computer instructions translatable by the processor to perform:**

See Section VII.J.1 (claim 10 preamble).

- 3. receiving a packet originating from a user device in a first network, wherein the first network is connected to a second**

network via the control device, and wherein the user device is associated with a user;

See Section VII.A.2 (corresponding limitation of claim 1).

4. determining whether the user has authenticated;

See Section VII.H.1 (corresponding limitation of claim 8).

5. if the user has not authenticated: redirecting the user to a login web page that requests user credentials; and using the user credentials received from the user to authenticate the user;

See Section VIII.A.1 (corresponding limitation of claim 9).

6. processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;

at the client discrimination stage, extracting information associated with the user device from a header of the packet and associating the packet with user specific traffic control rules and user specific firewall rules; and

at the user specific rule stage, accessing the user specific traffic control rules and user specific firewall rules based on the extracted information associated with the user device and applying the user specific traffic control rules and the user specific firewall rules to the packet as governed by at least one user specific class of service rule associated with the user on the user device in the first network.

See Sections VII.A.3-5 (corresponding limitations of claim 1).

IX. GROUND 4 – CLAIM 21 IS RENDERED OBVIOUS BY RICHMOND IN LIGHT OF TERASLINNA

A. Dependent Claim 21

1. The control device of claim 20, wherein the traffic conditioning module further comprises an interface master

queue for controlling a flow of network traffic over a particular network interface.

Richmond discloses and renders obvious claim 20, as discussed. Richmond in light of Teraslinna renders obvious that the traffic conditioning module further comprises an interface master queue (*e.g.*, Teraslinna's queue 144) for controlling a flow of network traffic over a particular network interface. Ex1002, ¶¶201-208.

Richmond discloses that its user-specific rules include rules that enforce bandwidth rate limitations on users (*i.e.*, traffic shaping). *See* Ex1003, [0010], [0158]-[0159]. Richmond further discloses that the network entry device applies rate limiting (*e.g.*, act 1430) according to these user-specific rules. *Id.*, [0158]-[0159], [0249]-[0251].

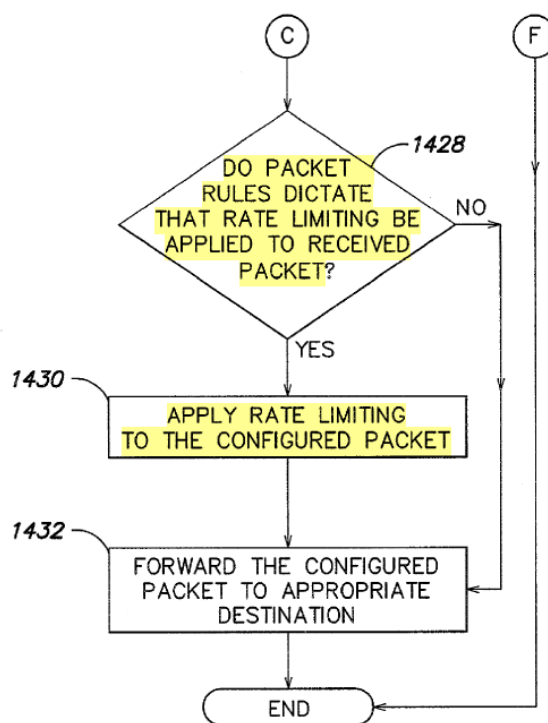
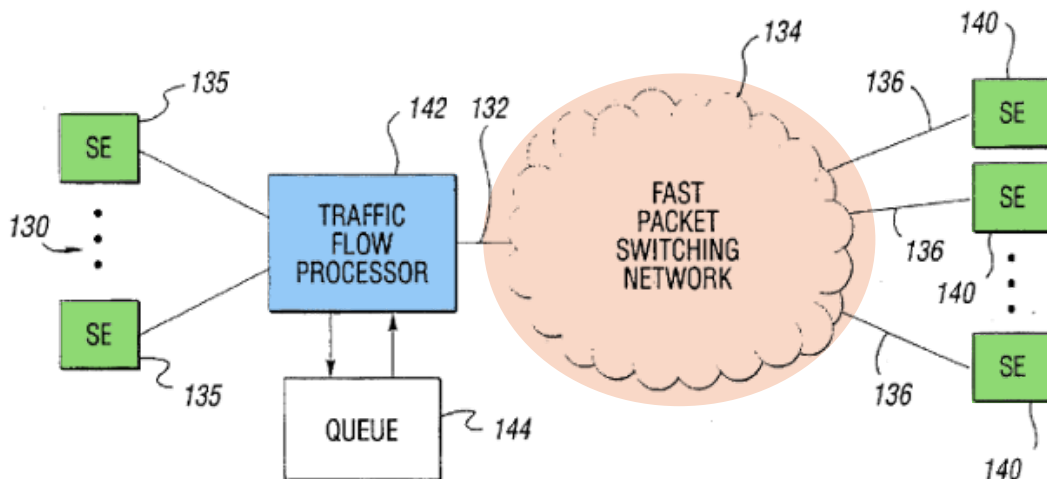


FIG. 14B

A POSITA reading Richmond's disclosure of traffic shaping would naturally look to find a reference that discloses an implementation of traffic shaping, of which there were a variety of known ways. Ex1002, ¶203. One such method is disclosed in Teraslinna, to which a POSITA would look because it is in the same field as Richmond and the '639 Patent, namely, systems for controlling network access, and in particular, systems for controlling bandwidth allocations and performing traffic conditioning in packet-switched networks. *Id.*

Teraslinna discloses that traffic from subscriber equipment 135 (analogous to Richmond's user devices) passes through traffic flow processor 142 (analogous to Richmond's network entry device), in order to reach fast packet switching network

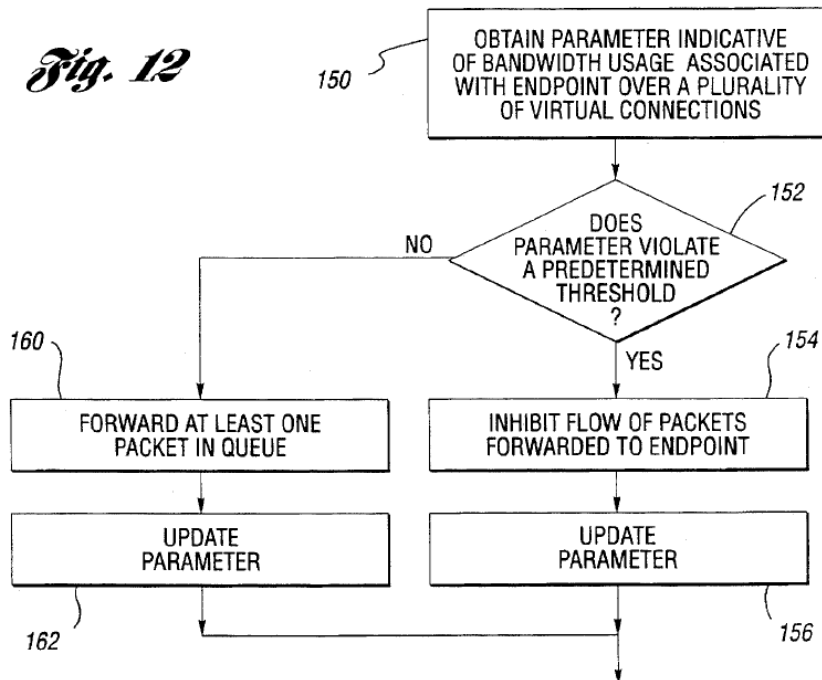
134 (analogous to the Internet in Richmond). Teraslinna further discloses that traffic flow processor 142 is coupled to queue 144, which "queues all incoming packets from the customer premises equipment 130 for traffic shaping by the traffic flow processor." Ex1005, 16:5-8.



Ex1005, Fig. 11 (annotated).

Queue 144 is thus an exemplary interface master queue, as it receives all traffic that is received at the interfaces of traffic flow processor 142 and controls all traffic on the interface to network endpoint 132. Ex1002, ¶205.

The queue 144 is used to control the flow of network traffic across the interface to network endpoint 132, according to the bandwidth limiting algorithm disclosed in Teraslinna. Ex1005, 16:9-17:18, Fig. 12.



Id., Fig. 12.

A POSITA would be motivated to combine Richmond's network entry device with Teraslinna's interface master queue. Ex1002, ¶206. A POSITA would find it desirable that Teraslinna's traffic shaping method (including queue 144 that it is based on) provides for cost-efficient bandwidth allocation, in a way that "reduce[s] bandwidth requirements" and "reduce[s] the cost of implementing a virtual private network." Ex1005, 2:43-48.

A POSITA would understand that combining Teraslinna's queue 144 and traffic shaping method would be a combination of prior-art elements according to known methods to yield predictable results. Ex1002, ¶207. Richmond's and Teraslinna's systems are highly analogous (with Teraslinna's traffic flow processor

142 playing the same role of traffic shaping in its system as Richmond's network entry device), such that a POSITA would be motivated to simply add the traffic-shaping functionality of Teraslinna to Richmond's network entry device. *Id.*, ¶¶207-208. A POSITA would simply add one of Teraslinna's queues to each of Richmond's port modules and then add Teraslinna's algorithm to the port module's port processing logic, in order to process the stream of packets. *Id.*, ¶208. Because of the straightforward nature of this combination, a POSITA would have a reasonable expectation of success. *Id.*

X. FEES

Petition and Post-Institution fees totaling \$61,745.00 have been paid by electronic funds transfer.

XI. CONCLUSION

Petitioner respectfully requests institution and a final written decision cancelling the Challenged Claims.

XII. MANDATORY NOTICES

A. Real Party-in-Interest

Petitioner Fortinet, Inc. is the real party-in-interest.

B. Related Proceedings

The '639 Patent has been asserted by Netskope in the district court proceeding *Netskope, Inc. v. Fortinet, Inc.*, Case No. 3:25-cv-2360-LJC (N.D. Cal., Mar. 7, 2025).

C. Counsel Information

Petitioner designates the following counsel:

Lead Counsel	Back-Up Counsel
Andrew D. Gish (Reg. # 67,562) GISH PLLC 41 Madison Avenue New York, New York 10010 Telephone: (212) 518-7380 andrew@gishpllc.com	Ryan Iwahashi (Reg. # 63,378) GISH PLLC 50 California Street, Suite 1500 San Francisco, CA 94111 Telephone: (415) 630-8960 ryan@gishpllc.com Christopher DeCoro (<i>pro hac vice</i> to be filed) GISH PLLC 41 Madison Avenue New York, New York 10010 Telephone: (212) 518-2890 chris.decoro@gishpllc.com

D. Electronic Service

Petitioner consents to email service at the email addresses above.

Respectfully submitted,

Dated: October 7, 2025

/s/ Andrew D. Gish
Andrew D. Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing Petition with the word count limits set forth in 37 C.F.R. §42.24(a)(1)(i). Excluding the parts of the Petition exempted by 37 C.F.R. §42.24(a)(1), this Petition contains 13,981 words as determined using the word count feature in Microsoft Word, which was used to prepare this Petition.

Dated: October 7, 2025

/s/ Andrew D. Gish
Andrew D. Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER

CERTIFICATE OF SERVICE

The undersigned hereby confirms that on October 7, 2025, the foregoing Petition for *Inter Partes* Review and associated exhibits were caused to be served via overnight courier on the Patent Owner at the correspondence address of record for U.S. Pat. No. 8,117,639.

Gregory Howison
25883 – Munck Wilson Mandala L.L.P.
2000 McKinney Ave, Ste 1900
Dallas, TX 75201

Courtesy copies were also served via email on Patent Owner's counsel of record in a related district court action styled *Netskope, Inc. v. Fortinet, Inc.*, Case No. 3:25-cv-2360-LJC (N.D. Cal.):

Thomas N. Millikan
TMillikan@perkinscoie.com
Joseph P. Reid
JReid@perkinscoie.com
PERKINS COIE LLP
11452 El Camino Real, Suite 300
San Diego, CA 92130-2080
Telephone: 858.720.5700
Facsimile: 858.720.5799

Andrew N. Klein
AKlein@perkinscoie.com
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, CA 94304-1212
Telephone: 650.838.4300
Facsimile: 650.838.4350

Dated: October 7, 2025

/s/ Andrew D. Gish
Andrew D. Gish (Reg. # 67,562)

ATTORNEY FOR PETITIONER