<u>Ex. C-1 - Invalidity of U.S. Patent No. 8,117,639 against U.S. Patent Pub. No. 2003/0152067A1 to Richmond</u>

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

U.S. Patent Publication No. 2003/0152067 to Richmond is a publication of U.S. Patent Application No. 10/251,140, which was filed on September 20, 2002, and published on August 14, 2003, and thus is available as prior art under at least 35 U.S.C. §102(e).

Richmond incorporates by reference the publications *Layer 2/3/4 Frame Classification Primer* (*see* Richmond at [0128]), *Enterasys User Personalized Network* (*see id.* at [0239]), among others. The disclosure of these publications is accordingly part of the disclosure of Richmond, and Fortinet reserves the right to rely on these publications as part of its invalidity arguments based on Richmond, including at least the exemplary citations to these publications included in Ex. C-4.

As illustrated in the chart below, Richmond anticipates the asserted claims of the '639 Patent. To the extent Richmond is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent Richmond is found not to anticipate any asserted claims or claim elements of the '639 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid. The fact that Fortinet has cited evidence for a preamble is not a concession that the preamble is limiting.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

Claim Language	Exemplary Citations from Richmond '067
[1] A method for network access control, comprising:	Richmond discloses: A method for network access control. *See, e.g.*: Richmond '067 at Abstract: Controlling 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. A plurality of users may be connected to an entry point of a network of a network device by a shared transmission medium. Each users' usage of network resources is controlled, after such user has been authenticated, without using any network resources beyond such user's entry point to the network. For each one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. If a plurality of users are connected to an entry point by a shared transmission medium, packet rules associated with the users may be provisioned to the entry point and applied to packets received from the users before any network resources beyond the entry point are used. Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0003]: Communications networks continue to grow and improve in today's world. A common issue in such networks is how to control usage of network resources by users. Richmond '067 at [0010]: Controlling usage of network resources may include, but is not limited to: denying one or more packets access to any network resources beyond a network device (i.e., dropping the packet); regulating bandwidth on the network consumed by packets received from the user, for example, by assigning priorities to received packets or applying rate limiting to received packets; denying access to certain network resources, for example, by assigning a Virtual Local Area Network (VLAN) to the packet; and

	routing the packet. VLANs are described in more detail in IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks , Dec. 8, 1998, the entire contents of which are hereby incorporated by reference. Assigning a VLAN to a packet and/or assigning a priority to a packet, may be referred to herein as “classifying” a packet. As used herein, a “packet” is a unit of communication exchanged between devices. Richmond '067 at [0016]: As used herein, a “network entry device” is a network device that includes at least one entry port module. Thus, from the perspective of other devices, a network entry device serves as an entry point to the network for at least one user. A network entry device may reside at an edge or boundary of the communications network and provide connectivity between network resources of the communications network and devices located external to the communications network. Such network entry device may be any of a variety of types of devices, for example, a switching device. Richmond '067 at [0027]: One technique used to control usage of network resources is to apply user authentication to restrict access to network resources. Technologies that employ user authentication techniques include, among others, network operating systems (NOSs) (e.g., Netware by Novell and Windows NT), Remote Authentication Dial-In User Service (RADIUS) and IEEE 802.1X: Port Based Network Access Control , 2001. RADIUS is described in Request For Comments (RFC) 2138, entitled Remote Authentication Dial In User Service (RADIUS) by C. Rigney et al., promulgated by the Internet Engineering Task Force (IETF), published April, 1997, and available as of the date of this filing at: http://www.ietf.org/rfc/rfc2138.txt? number=2138., the entire contents of which are hereby incorporated by reference. IEEE 802.1X, the entire contents of which are hereby incorporated by reference, defines a standard for providing port-based network access control on a Media Access Control (MAC) bridge. Richmond '067 at [0031]: Another technique for controlling usage of network resources is based on network infrastructure. For example, a network topology may be configured such that there is no possible transmission path between two or more devices. Further, switching devices on the network may be configured to forward packets received at the switching device based on the physical port at which the packet was received. For example, a switching device may be configured not to allow a physical port to receive any packets, or to forward all packets received at one physical port to another physical port on the switching device,

	or to assign or append the same VLAN header to all packets received at a particular physical port. A VLAN header may include a VLAN identifier and a priority, for example, as described in more detail in IEEE 802.1Q. Richmond '067 at [0033]: Another technique for controlling usage of network resources is to analyze information included in packets and forward the received packets based on the information. For example, some switching devices may be configured to examine information included in a received packet, for example, a source Media Access Control (MAC) address, a destination MAC address, or a protocol, and forward the packet or assign a VLAN header to the packet based on this information, for example, as described in more detail in IEEE 802.1Q. A switching device configured as such may serve as an entry point to the network for one or more users. Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0041]: In an embodiment of the invention, a network device of a communications network is used to control usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The port module is configured with one

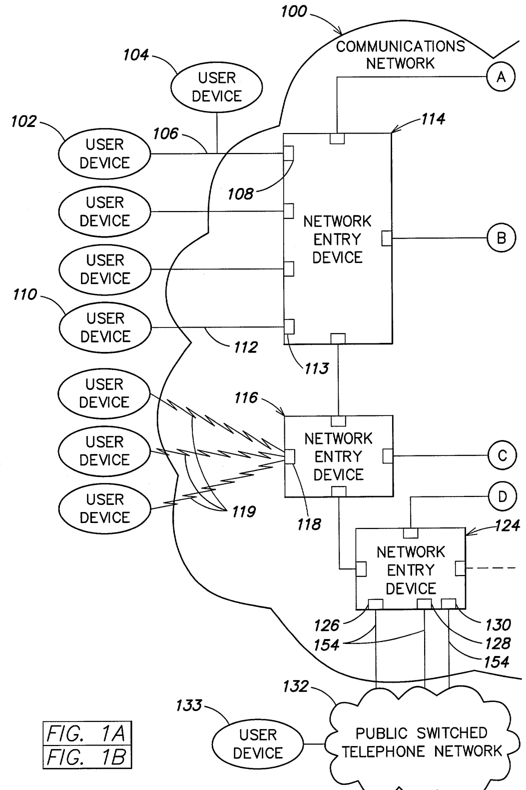
	or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the packet rules is associated with the identity of the second user. Richmond '067 at [0042]: In an aspect of this embodiment, a first packet is received at the port module from a user device, and an identity of a user of the user device is determined. If the determined identity is the identity of the first user, then, before using any of the network resources beyond the network device in response to processing the first packet, at least the first rule is applied to the first packet. This process may be repeated for all packets received at the port module from the first user device until the first user logs off of the communications network. Richmond '067 at [0048]: In another embodiment of the invention, a network device of a communications network is provided for controlling usage of network resources of the communications network by a plurality of users. The network device serves as an entry point to the communications network for the plurality of users and includes a port module, where the port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The system comprises port configuration logic to configure the port module with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the one or more packet rules is associated with the identity of the second user. Richmond '067 at [0056]: In another embodiment of the invention, a network device of a communications network is provided for controlling usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network, and the port module is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The network device comprises means for configuring the port module with one or more packet rules associated with an identity of the first user and an identity of the second user, where at least a first of the one or more packet rules is associated with the identity of the first user.

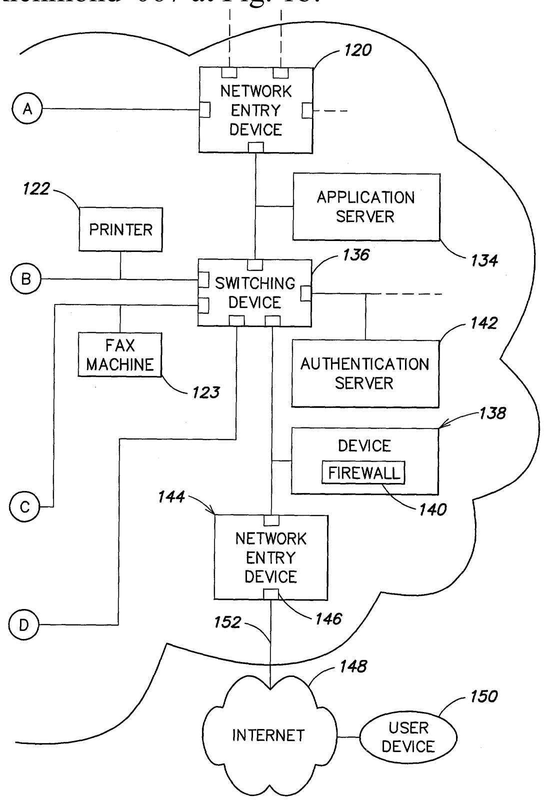
	Richmond '067 at [0057]: In another embodiment of the invention, usage of network resources of a communications network by a user beyond a network device of the communications network that serves as the user's entry point to the communications network is controlled. The port module of the network device is configured with one or more packet rules corresponding to an identity of the user. A packet is received from a device used by the user at the port module, and, before using any of the network resources beyond the network device, the one or more packet rules are applied to the received packet. Richmond '067 at [0069]: In another embodiment, a network device of a communications network is provided for controlling usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network, and the port module is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The network device comprises means for configuring the port module with one or more packet rules associated with an identity of the first user and an identity of the second user, where at least a first of the one or more packet rules is associated with the identity of the first user. Richmond '067 at [0076]: In another embodiment of the invention, provided is a network device serving as an entry point to a communications network for a user. The network device operative to control usage of network resources beyond the network device by the user and includes a port module including a physical port to receive a packet from a device used by the user and rule application logic to apply one or more packet rules to the received packet before using any of the network resources beyond the network device, and means for configuring the port module with the one or more packet rules based on an identity of the user. Richmond '067 at [0082]: In another embodiment of the invention, usage of network resources of a communications network by a user is controlled. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. A packet including identification information of the user is received from a device of the user at a port module of a network

	device. The assigned role of the user is determined based on the identification information, and the port module is configured with the one or more packet rules associated with the assigned role of the user. Richmond '067 at [0086]: In yet another embodiment of the invention, provided is a system for controlling usage of network resources of a communications network by a user. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. The system includes a port module including a physical port to receive a packet including identification information of the user from a device of the user and port configuration logic to configure the port module with the one or more packet rules associated with the assigned role of the user, and an authentication module to determine the assigned role of the user based on the identification information. Richmond '067 at [0089]: In another embodiment of the invention, provided is a system for controlling usage of network resources of a communications network by a user. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, where each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. The system includes a port module including a physical port to receive a packet including identification information of the user from a device of the user and port configuration logic to configure the port module with the one or more packet rules associated with the assigned role of the user, and means for determining the assigned role of the user based on the identification information. Richmond '067 at [0093]: FIG. 1 is a block diagram illustrating an example of a communications network; Richmond '067 at [0105]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method of controlling usage of network resources by one or more users at such users' entry point to a communications network; Richmond '067 at [0106]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method of applying packet rules to a packet received at an entry port module of a network device of a communications network to control usage of network resources by a user; and

	Richmond '067 at [0107]: FIG. 15 is a block diagram illustrating an example of a system for controlling usage of network resources by one or more users at such users' entry point to a communications network. Richmond '067 at [0108]: Described below is a system and method that control 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. Richmond '067 at [0109]: In an embodiment, a plurality of users are connected to an entry point of a network of a network device by a shared transmission medium. In such embodiment, each users' usage of network resources is controlled after such user has been authenticated without using any network resources beyond such user's entry point to the network. Richmond '067 at [0114]: An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules.

	Richmond '067 at [0243]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method 1400 for performing Act 1327 . Richmond '067 at [0257]: Thus, application of method 1400 to a received packet may result in a packet being configured based on user-based packet rules, default packet rules, and other additional rules with which the entry port module is configured. For example, the user-based packet rules may have assigned a VLAN to the received packet, the default packet rules may have assigned a priority to the received packet, and other rules may have applied rate limiting to the packet. Richmond '067 at [0261]: FIG. 15 is a block diagram illustrating an example of a system 1500 for controlling usage of network resources by one or more users beyond such users' entry point to a communications network based on the respective identities of one or more users. The system 1500 may include a network entry device 1504 , a authentication module 1506 and an authentication database 1508 . Although authentication module 1506 and authentication database 1508 are shown as not being part of network entry device 1504 in FIG. 15, module 1506 or database 1508 or both may be part of network entry device 1504 . Richmond '067 at [0280]: For each packet received at the entry port module, except login packets, the user identification logic may be configured to identify the user of the user device that transmitted the packet, for example, as described above in relation to act 1401 of method 1400 . For example, network entry device may include logic that creates a user identification list as described above in relation to act 1319 . Such list may be stored on network entry device 1504 or on any other network element of FIG. 15 accessible by network entry device 1504 . The determined user identity dictates the packet rules applied to the received packet by the rule application logic. Richmond '067 at [0281]: The rule application logic of port processing logic 1516 may be configured to apply, in response to receiving a packet 1502 at port module 1510 after a user has been authenticated, the rule set 1519 to the packet 1502 . The application of the rule set may be performed as described above in relation to method 1400 of FIGS. 14A and 14B. Thus, the rule application logic may be configured to apply one or more user-based packet rules, one or more default packet rules, and one or more other types of rules to the

	received packet. It should be noted that multiple rules may specify that a certain value be assigned to a parameter of the received packet that is to be configured. For example, two user-based packet rules, a default packet rule and another type of rule all may specify a different VLAN value to be applied to the received packet. Accordingly, the rule application logic may be configured to give precedence to certain rules over other rules. Richmond '067 at Fig. 1a:  FIG. 1A

	Richmond '067 at Fig. 1b:  FIG. 1B

Richmond '067 at Fig. 13b:

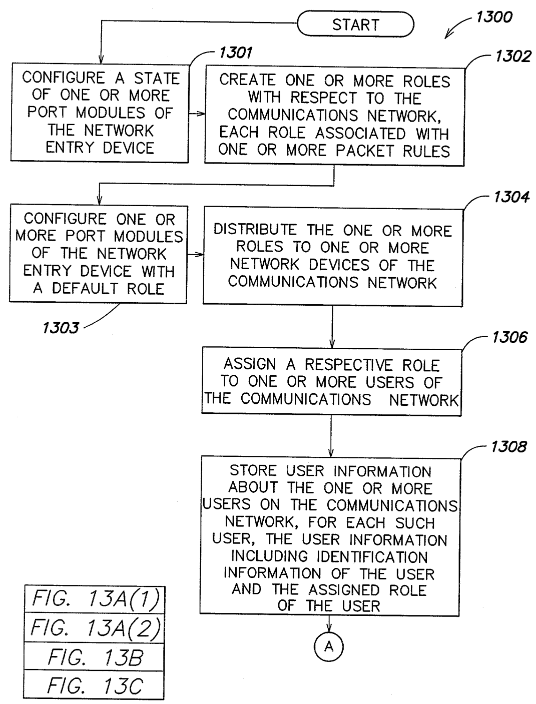


FIG. 13A(1)

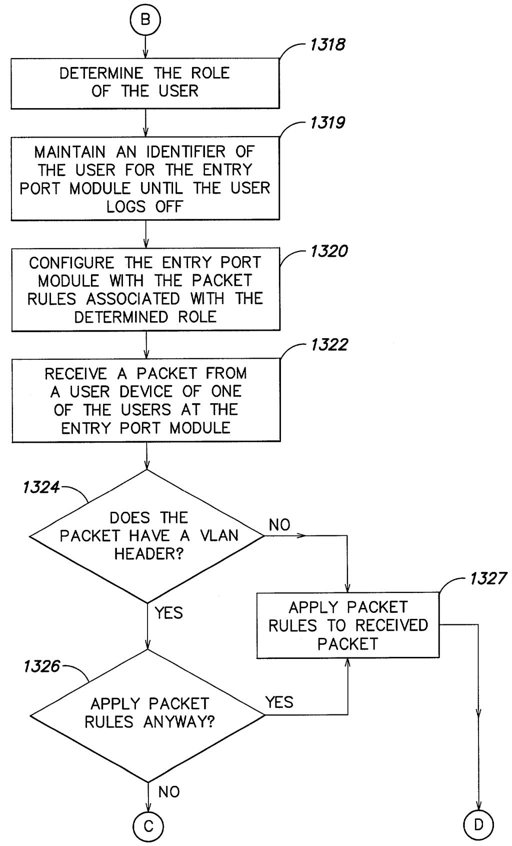
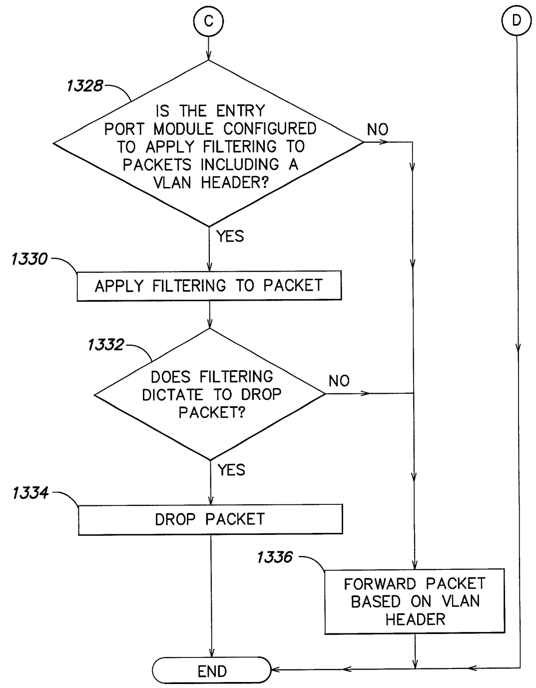
	Richmond '067 at Fig. 13b: 

FIG. 13B

	Richmond '067 at Fig. 13c:  FIG. 13C

	Richmond '067 at Fig. 14b:

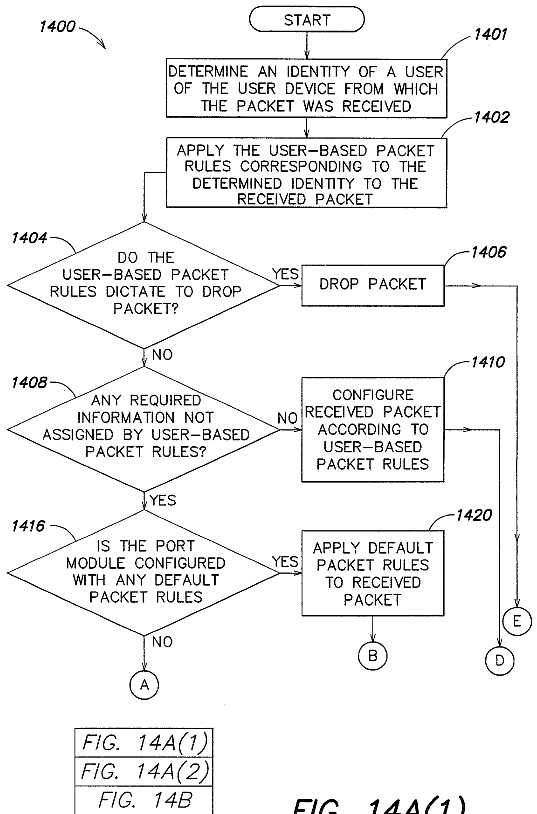
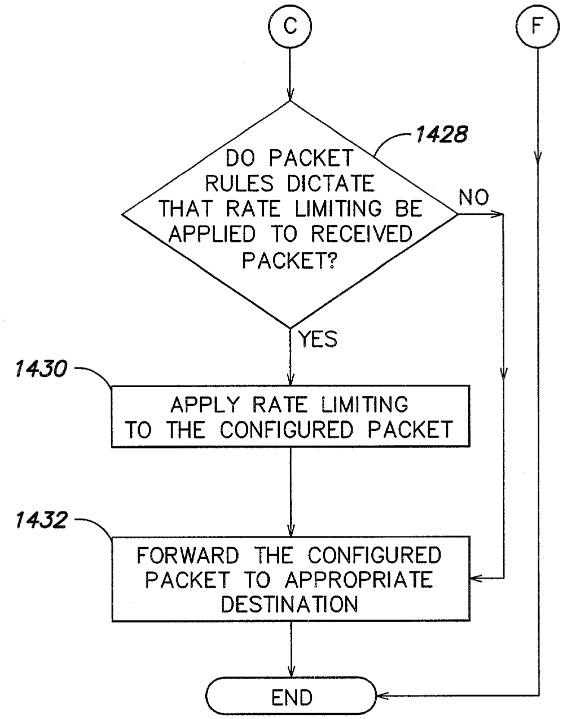


FIG. 14A(1)

	Richmond '067 at Fig. 14b:  *FIG. 14B* The evidence cited above is exemplary; further exemplary evidence that Richmond discloses a method for network access control is provided for the following limitations of this claim.
[1.1] 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	Richmond discloses: 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. *See, e.g.*:

device, and wherein the user device is associated with a user;	Richmond '067 at Abstract: Controlling 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. A plurality of users may be connected to an entry point of a network of a network device by a shared transmission medium. Each users' usage of network resources is controlled, after such user has been authenticated, without using any network resources beyond such user's entry point to the network. For each one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. If a plurality of users are connected to an entry point by a shared transmission medium, packet rules associated with the users may be provisioned to the entry point and applied to packets received from the users before any network resources beyond the entry point are used. Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0011]: FIG. 1 is a block diagram illustrating an example of a communications network 100 . Network 100 may include one or more interconnected Local Area Networks (LANs), Metropolitan Area Networks (MANs), or combinations thereof. Further, network 100 may serve as a communications network for a business organization or other type of enterprise, and as such may be considered an "enterprise" network. Richmond '067 at [0012]: Network 100 may include a plurality of devices of varying type, including any of network entry devices 114 , 116 , 120 , 124 and 144 , printer 122 , fax machine 123 , application server 134 , switching device 136 , device 138 and authentication server 142 . Switching device 136 may be configured as a core switching device that serves as a more centralized switching device for network 100 than the network entry devices.

	Richmond '067 at [0013]: A network entry device may include one or more port modules, and one or more of these port modules may be an entry port module. Richmond '067 at [0014]: As used herein, a “port module” of a switching device includes a physical port of the device and port processing logic associated with the physical port. Such port processing logic may include 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. Such port processing logic may be divided into one or more virtual ports, each virtual port corresponding to a communication channel of the physical port. The port processing logic may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of a port module may be shared with several other port modules. A port module may be implemented as part of a port interface card (PIC), which may include one or more port modules. Richmond '067 at [0015]: As used herein, an “entry port” is a physical port of a network device that serves as a user's entry point into a network. Thus, to communicate with devices on the network, a user's device may transmit one or more packets to an entry port. Further, as used herein, an “entry port module” is a port module of a network device that includes an entry port. Richmond '067 at [0016]: As used herein, a “network entry device” is a network device that includes at least one entry port module. Thus, from the perspective of other devices, a network entry device serves as an entry point to the network for at least one user. A network entry device may reside at an edge or boundary of the communications network and provide connectivity between network resources of the communications network and devices located external to the communications network. Such network entry device may be any of a variety of types of devices, for example, a switching device. Richmond '067 at [0017]: As used herein, a “user device” is a device used by a user of a communications network to perform at least one of the following: receive a packet from the network and send a packet to the network. Types of user devices may include, but are not limited to, workstations, terminals, personal computers, laptops, telephones, pagers, BlackBerry™ brand devices, and personal digital assistants (PDAs).

	Richmond '067 at [0018]: An entry port module may be coupled to a user device by a shared transmission medium or a dedicated transmission medium. As used herein, a "shared transmission medium" is a transmission medium connected to a port module of a first device and over which multiple other devices may exchange packets with the first device. For example, a gateway server for an enterprise network may have a port module connected to the Internet by a T-3 cable, over which several users of the enterprise network may exchange packets with the Internet. Another example is an Ethernet cable connected to multiple user devices of a LAN. Richmond '067 at [0021]: Referring to FIG. 1, network entry device 114 may include an entry port module 108 that is connected to user devices 102 and 104 by a shared wire-based transmission medium 106 . As used herein, a "wire-based transmission medium" is a transmission medium that is not a wireless transmission medium (e.g., air), for example, an optical cable or an electrical wire or cable. Accordingly, a "shared wire-based transmission medium" is a wire-based transmission medium that connects two or more devices. Richmond '067 at [0024]: Entry port module 146 of network entry device 144 is connected to user device 150 by the Internet 148 and shared transmission medium 152 . Richmond '067 at [0025]: Entry port modules 126 , 128 and 130 of network entry device 124 may be connected to user device 133 by a Public Switched Telephone Network (PSTN) 132 and by shared transmission mediums 154 . Although transmission mediums 154 are shared, any of ports 126 , 128 and 130 may be configured along with devices to which they are coupled on the PSTN to make any of transmission mediums 154 dedicated to user device 133 for the duration of a session, such as a telephone call during which data is exchanged. Richmond '067 at [0028]: Typically, such authentication technologies require a user to initially log-in to a network, for example, by entering a username, password and possibly other credentials, before having access to information stored on the network. Logging in may include exchanging packets between a device of the user (e.g., user device 102 , 104 , 110 , 133 or 150) and one or more network devices (e.g., switching device 136

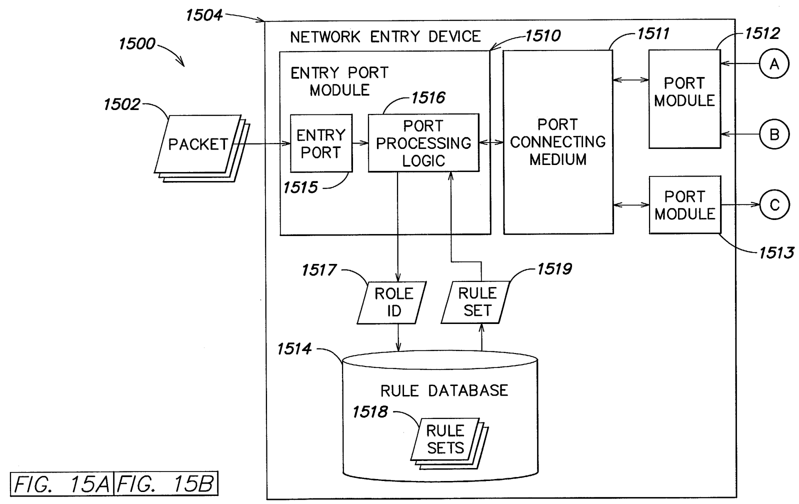
	and authentication server 142), and these packets may be transmitted through a network device (e.g., 114 , 116 , 124 or 144) serving as the user's entry point in to the network. Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0041]: In an embodiment of the invention, a network device of a communications network is used to control usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The port module is configured with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the packet rules is associated with the identity of the second user. Richmond '067 at [0042]: In an aspect of this embodiment, a first packet is received at the port module from a user device, and an identity of a user of the user device is determined. If the determined identity is the identity of the first user, then, before using any of the network resources beyond the network device in response to processing the first packet, at least the first rule is applied to the first packet. This process may be repeated for all packets received at the port module from the first user device until the first user logs off of the communications network.

	Richmond '067 at [0048]: In another embodiment of the invention, a network device of a communications network is provided for controlling usage of network resources of the communications network by a plurality of users. The network device serves as an entry point to the communications network for the plurality of users and includes a port module, where the port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The system comprises port configuration logic to configure the port module with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the one or more packet rules is associated with the identity of the second user. Richmond '067 at [0049]: In an aspect of this embodiment, the port module further comprises a physical port to receive a first packet from a user device and user identification logic to determine an identity of a user of the user device. The port module further comprises rule application logic to apply at least the first rule to the first packet, before using any of the network resources beyond the network device in response to processing packet, if the determined identity is the identity of the first user. Richmond '067 at [0059]: In another aspect of this embodiment, the one or more packet rules are applied to all packets received at the port module until the user logs off of the communications network. Richmond '067 at [0065]: In another aspect of this embodiment, the rule application logic is operative to apply the one or more packet rules to all packets received from the device of the user at the port module until the user logs off of the communications network. Richmond '067 at [0070]: In an aspect of this embodiment, the system comprises: means for receiving a first packet at the port module from a user device, means for determining an identity of a user of the user device, and means for applying at least the first rule to the first packet if the determined identity is the identity of the first user before using any of the network resources beyond the network device in response to processing the first packet. In another aspect of this embodiment, the system further comprises means for determining

	the identity and applying the packet rules for all packets received at the port module from the first user device until the first user logs off of the communications network. Richmond '067 at [0076]: In another embodiment of the invention, provided is a network device serving as an entry point to a communications network for a user. The network device operative to control usage of network resources beyond the network device by the user and includes a port module including a physical port to receive a packet from a device used by the user and rule application logic to apply one or more packet rules to the received packet before using any of the network resources beyond the network device, and means for configuring the port module with the one or more packet rules based on an identity of the user. Richmond '067 at [0110]: For each of the one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. Richmond '067 at [0114]: An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0126]: Each of the packet rules define a rule to be applied to a packet received at a device, for example, a device of the communications network 100 . Each packet rule may be defined to examine information included in a packet and to perform actions based on such information. The information to be examined may be any information that may be included in a packet.

	Richmond '067 at [0229]: In Act 1322 , a packet may be received from a user device of one of the users at the entry port module, for example, to initiate an application between the user device and a device of the communications network in accordance with an application already being executed. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0261]: FIG. 15 is a block diagram illustrating an example of a system 1500 for controlling usage of network resources by one or more users beyond such users' entry point to a communications network based on the respective identities of one or more users. The system 1500 may include a network entry device 1504 , a authentication module 1506 and an authentication database 1508 . Although authentication module 1506 and authentication database 1508 are shown as not being part of network entry device 1504 in FIG. 15, module 1506 or database 1508 or both may be part of network entry device 1504 . Richmond '067 at [0270]: Entry port module 1510 may include an entry port 1515 and port processing logic 1516 . 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. Port processing logic 1516 may be divided into one or more virtual ports (not shown), each virtual port corresponding to a communication channel of the entry port 1515 (e.g., if entry port 1515 is connected to a shared wireless transmission medium). Port processing logic 1516 may include separate switching

	logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of port processing logic 1516 may be shared with port processing logic of other port modules (e.g., 1512 and 1513). Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for configuring port module 1510 , for example, in accordance with the respective identities of one or more users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 . Richmond '067 at [0280]: For each packet received at the entry port module, except login packets, the user identification logic may be configured to identify the user of the user device that transmitted the packet, for example, as described above in relation to act 1401 of method 1400 . For example, network entry device may include logic that creates a user identification list as described above in relation to act 1319 . Such list may be stored on network entry device 1504 or on any other network element of FIG. 15 accessible by network entry device 1504 . The determined user identity dictates the packet rules applied to the received packet by the rule application logic. Richmond '067 at [0282]: The port processing logic 1516 may be configured to forward configured packet 1524 through the port connecting medium 1511 and port module 1513 to another destination on the network, where such packet may be configured and forwarded as described above in relation to methods 1300 and 1400 described above in relation to FIGS. 13 A13 C, 14 A and 14 B.

	Richmond '067 at Fig. 15a:  FIG. 15A Furthermore, the publication *Layer 2/3/4 Frame Classification Primer*, incorporated into Richmond by reference (*see* Richmond at [0128]), provides further disclosure of this limitation. *See, e.g.*, *Layer 2/3/4 Frame Classification Primer* at 3 (disclosing classification of packets according to "MAC address," "Protocol," "Layer 3 network address (e.g., their individual IP address, IP subnet, or Novell Network Number)"). Further exemplary citations have been provided in Ex. C-4.
[1.2] processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;	Richmond discloses: processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;. *See, e.g.*: Richmond '067 at [0041]: In an embodiment of the invention, a network device of a communications network is used to control usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module

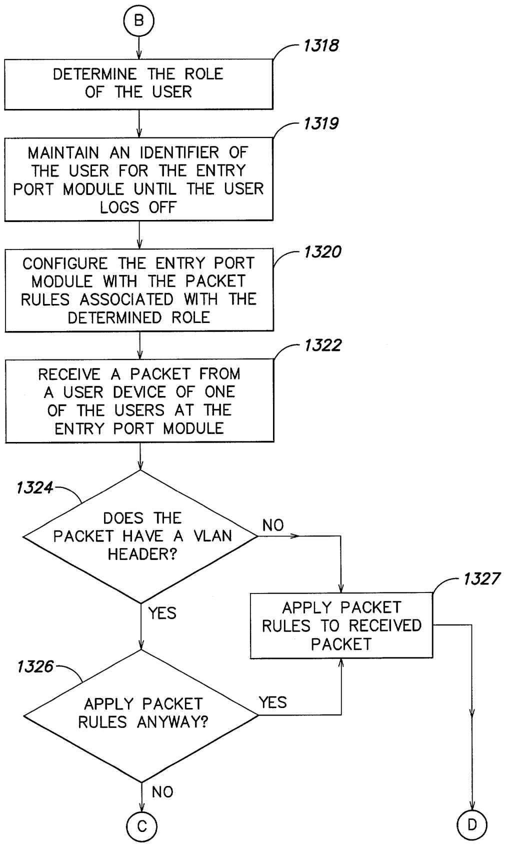
	also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The port module is configured with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the packet rules is associated with the identity of the second user. Richmond '067 at [0042]: In an aspect of this embodiment, a first packet is received at the port module from a user device, and an identity of a user of the user device is determined. If the determined identity is the identity of the first user, then, before using any of the network resources beyond the network device in response to processing the first packet, at least the first rule is applied to the first packet. This process may be repeated for all packets received at the port module from the first user device until the first user logs off of the communications network. Richmond '067 at [0049]: In an aspect of this embodiment, the port module further comprises a physical port to receive a first packet from a user device and user identification logic to determine an identity of a user of the user device. The port module further comprises rule application logic to apply at least the first rule to the first packet, before using any of the network resources beyond the network device in response to processing packet, if the determined identity is the identity of the first user. Richmond '067 at [0075]: In yet another aspect of this embodiment, the identity of the first user is associated with a role assigned to the first user, and the role is associated with at least the first packet rule, and the system further comprises means for selecting the first packet rule based on the role. Richmond '067 at [0082]: In another embodiment of the invention, usage of network resources of a communications network by a user is controlled. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. A packet including identification information of the user is received from a device of the user at a port module of a network device. The assigned role of the user is determined based on the identification information, and the port module is configured with the one or more packet rules associated with the assigned role of the user.

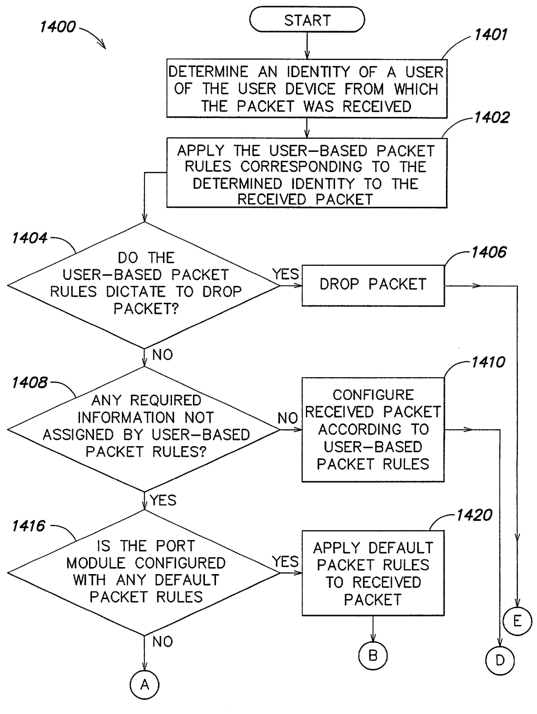
	Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0159]: For example, an entry of 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. Further, a network device may be configured to drop some or all of the bytes of a packet that contains an amount of packets that exceeds the threshold amount during the unit interval. Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume in sending packets to a particular network device specified by conditions 508 512 , or limit the amount of bandwidth that a user consumes on the network in sending packets corresponding to a particular application specified by conditions 508 512 . The consumption of bandwidth by a user also may be limited by the priority specified in field 516 . Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules. Richmond '067 at [0222]: If in Act 1314 it is determined that the identification information is invalid (e.g., it does not match any entry of an authentication database), then in Act 1316 , the user may be denied access to the communications network. Whether or not the user is denied access may depend on the state defined for the entry port module in Act 1301 . Richmond '067 at [0224]: In Act 1319 , an identifier of the user is maintained (e.g., stored) for the entry port module until the user logs off. Such user identifier may be stored in a list along with other user identifiers for other users that

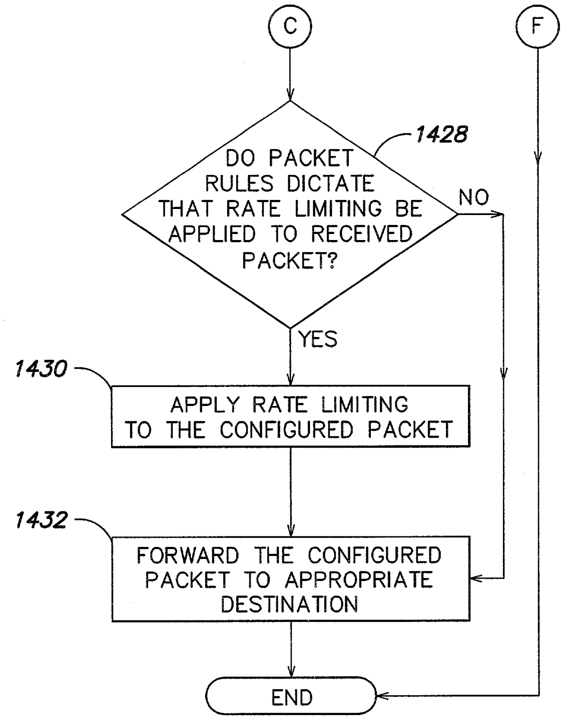
	have been authenticated and are currently logged on to the port module. Such user identifier may be stored on a computer-readable medium accessible by the entry port module. The user identifier may be any information that was included in a login packet received from the user or any information included in the entry information retrieved from the authentication database for the user as described above in relation to Act 1314 . The user identifier 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. As will be described in more detail below in relation to Act 1401 of method 1400 , for each packet received at the entry port module after performance of Act 1319 , the user identifier may be accessed to determine an identity of the user of the user device from which the packet was received. Richmond '067 at [0227]: As described above in relation to 1304 , one or more roles (and/or service abstractions) may have been distributed to the network entry device. Accordingly, Act 1320 may include configuring the entry port module with the one or more packet rules corresponding to one or more of the roles and/or service abstractions that were distributed to the network entry device in Act 1304 . Richmond '067 at [0228]: In addition to or as an alternative to Acts 1318 and 1320 , one or more service abstractions corresponding to a user may be determined, and the entry port module may be configured with the packet rules associated with the one or more determined service abstractions. As described above in relation to distribution module 408 of FIG. 4, in addition to or as an alternative to distributing roles 432 to devices of a network, one or more relationship hierarchies and/or service abstractions also may be distributed. Thus, entries of authentication database 1508 or another database accessible by the authentication module 1506 may specify the one or more service abstractions assigned to a user, and this information may be used to determine the one or more service abstractions assigned to a user and to configure the entry port module with the packet rules associated with these one or more service abstractions, as similarly described in relation to Acts 1318 and 1320 with respect to the assigned role of a user. Richmond '067 at [0239]: In an embodiment of method 1300 , various acts of method 1300 and/or part thereof are performed as described in Enterasys User Personalized Network , a white paper available from Enterasys Networks,

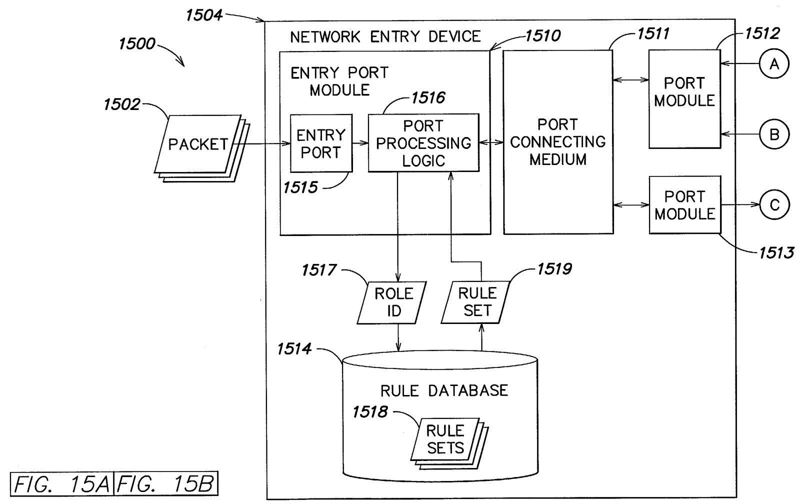
	Inc., available on the filing date of this application at http://www.enterasys.com/products/whitepapers, the entire contents of which is hereby incorporated by reference. Richmond '067 at [0243]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method 1400 for performing Act 1327 . Richmond '067 at [0244]: In Act 1401 , an identity of a user of the user device from which the packet was received is determined. For example, information from the received packet may be compared against a list of user identifiers maintained by the entry port module as a result of performing Act 1319 . For example, 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 from an authentication packet received from the user device of the user, and Act 1319 may be repeated for a plurality of users. Accordingly, Act 1401 may include 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. Richmond '067 at [0246]: In Act 1402 , the user-based packet rules are applied to the received packet. 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. 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. Richmond '067 at [0247]: In Act 1404 , it may be determined whether the user-based packet rules dictate to drop the received packet. If the user-based packet rules dictate to drop the packet, then in Act 1406 , the packet is dropped and the method ends. Richmond '067 at [0249]: In a following Act 1428 , it may be determined whether the packet rules dictate that rate limiting is to be applied to the received packet. An entry port module may be configured to apply one or more rate limiting techniques, known now or later developed. Rate limiting is described above in more detail in relation to rate limit field 520 of packet rule data structure 500 of FIG. 5.

	Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for configuring port module 1510 , for example, in accordance with the respective identities of one or more users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 . Richmond '067 at [0276]: System 1500 may include logic (not shown) for entering entry information in an entry 1528 , including assigning logic to assign a role identifier and/or one or more service abstraction identifiers to a user. Such logic may reside on any of one or more network devices of the network on which the system 1500 is implemented, including on network entry device 1504 , a user device, or the device on which the authentication module resides. A device on which at least a portion of such logic resides may include a user interface to enable a user to enter the entry information. Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 . Richmond '067 at [0280]: For each packet received at the entry port module, except login packets, the user identification logic may be configured to identify the user of the user device that transmitted the packet, for example, as

	described above in relation to act 1401 of method 1400 . For example, network entry device may include logic that creates a user identification list as described above in relation to act 1319 . Such list may be stored on network entry device 1504 or on any other network element of FIG. 15 accessible by network entry device 1504 . The determined user identity dictates the packet rules applied to the received packet by the rule application logic. Richmond '067 at Fig. 13b:  FIG. 13B

	Richmond '067 at Fig. 14b:  FIG. 14A(1) FIG. 14A(2) FIG. 14B FIG. 14A(1)

	Richmond '067 at Fig. 14b:  FIG. 14B

	Richmond '067 at Fig. 15a:  FIG. 15A Further exemplary evidence regarding the processing of the packet in the client-discrimination stage is provided in connection with limitation [1.3]. Further exemplary evidence regarding the processing of the packet in the user-specific rule stage is provided in connection with limitation [1.4].
[1.3] 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, 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. *See, e.g.*: Richmond '067 at [0010]: Controlling usage of network resources may include, but is not limited to: denying one or more packets access to any network resources beyond a network device (i.e., dropping the packet); regulating bandwidth on the network consumed by packets received from the user, for example, by assigning priorities to received packets or applying rate limiting to received packets; denying access to certain network resources, for example, by assigning a Virtual Local Area Network (VLAN) to the packet; and routing the packet. VLANs are described in more detail in IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks , Dec. 8, 1998, the entire contents

	of which are hereby incorporated by reference. Assigning a VLAN to a packet and/or assigning a priority to a packet, may be referred to herein as “classifying” a packet. As used herein, a “packet” is a unit of communication exchanged between devices. Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0041]: In an embodiment of the invention, a network device of a communications network is used to control usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The port module is configured with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the packet rules is associated with the identity of the second user. Richmond '067 at [0042]: In an aspect of this embodiment, a first packet is received at the port module from a user device, and an identity of a user of the user device is determined. If the determined identity is the identity of the first user, then, before using any of the network resources beyond the network device in response to processing the first packet, at least the first rule is applied to the first packet. This process may be repeated for all packets received at the port module from the first user device until the first user logs off of the communications network.

	Richmond '067 at [0049]: In an aspect of this embodiment, the port module further comprises a physical port to receive a first packet from a user device and user identification logic to determine an identity of a user of the user device. The port module further comprises rule application logic to apply at least the first rule to the first packet, before using any of the network resources beyond the network device in response to processing packet, if the determined identity is the identity of the first user. Richmond '067 at [0058]: In an aspect of this embodiment, the identity of the user is authenticated and the configuring of the port module is based on the authentication. Richmond '067 at [0075]: In yet another aspect of this embodiment, the identity of the first user is associated with a role assigned to the first user, and the role is associated with at least the first packet rule, and the system further comprises means for selecting the first packet rule based on the role. Richmond '067 at [0082]: In another embodiment of the invention, usage of network resources of a communications network by a user is controlled. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. A packet including identification information of the user is received from a device of the user at a port module of a network device. The assigned role of the user is determined based on the identification information, and the port module is configured with the one or more packet rules associated with the assigned role of the user. Richmond '067 at [0112]: Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. 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, as opposed to applying the rules after the user has already consumed bandwidth and processing resources as is typical on a network with a more centralized firewall.

	Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0154]: Value field 510 may store a value to be compared against information included in a packet to determine if the information matches the value. Mask field 512 may store a value representing a mask to be applied to the information in the packet to be compared to the value field 510 . For example, a bit-wise logical AND operation may be performed between the value stored in mask field 512 and the value of the information included in the packet specified by type field 508 . The result of this comparison then may be compared to the value specified in value field 510 . The mask field 512 may be used only for certain packet rules, for example, rules that specify an IP subnetwork address. Richmond '067 at [0158]: Rate limit field 520 may store a value representing a rate limit to be applied to a packet if it satisfies the rule. Some rules may be defined such that if the condition of the rule is satisfied by a packet, then rate limiting will be applied to a packet. In such case, rate limit field 520 may specify a threshold value (e.g., 1 megabyte (MB)). This threshold value may specify a threshold volume of bytes that may be received during a specified temporal interval (e.g., one second) in packets that satisfy a particular rule. The temporal interval may be specified in field 520 itself or in another field. Richmond '067 at [0159]: For example, an entry of 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. Further, a network device may be configured to drop some or all of the bytes of a packet that contains an amount of packets that exceeds the threshold amount during the unit interval. Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume in sending packets to a particular network device specified by conditions 508 512 , or limit the amount of bandwidth that a user consumes on the network in sending packets corresponding to a particular application specified by conditions 508 512 . The consumption of bandwidth by a user also may be limited by the priority specified in field 516 .

	Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules. Richmond '067 at [0215]: In Act 1308 , user information about the one or more users to which the respective roles are assigned may be stored on the communications network. This user information may include identification information of the user and the assigned role of the user. The identification information may include a user name, password, and other credentials of the user, for example, personal information about the user such as the user's social security number, birth date, or other piece of information. The user information may be stored in an authentication database, for example, authentication database 1508 described below in relation to FIG. 15. Richmond '067 at [0217]: In Act 1310 , a login packet may be received from a device of one of the users at an entry port module of the network entry device, the login packet including identification information of the user. The login packet may be received in response to the user's device sending a signaling packet to the network entry device and the network entry device requesting login information. Richmond '067 at [0219]: The identification information included in the login packet may be similar to the identification information described above in relation to 1308 , and may include a user name, password and other credential information corresponding to the user. Richmond '067 at [0222]: If in Act 1314 it is determined that the identification information is invalid (e.g., it does not match any entry of an authentication database), then in Act 1316 , the user may be denied access to the communications network. Whether or not the user is denied access may depend on the state defined for the entry port module in Act 1301 .

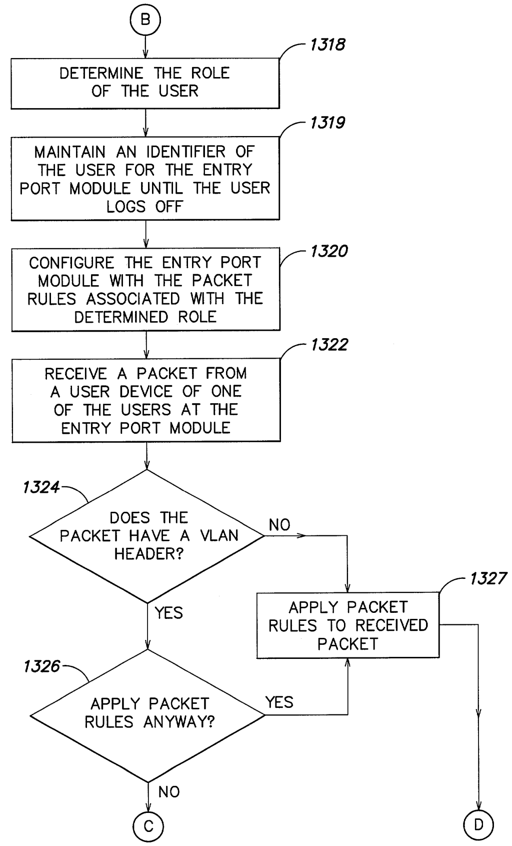
	Richmond '067 at [0223]: If it is determined in Act 1314 that the identification information is valid, then in Act 1318 , the role of the user may be determined. For example, the entry information 1529 extracted from authentication database 1508 may include a role identifier (ID) corresponding to the user, from which the authentication module may determine the role of the user. Alternatively, the authentication module may access another database that includes a plurality of entries, where each entry corresponds to a user and includes a role assigned to the user, from which the authentication module 1506 may determine the role of a user. Richmond '067 at [0224]: In Act 1319 , an identifier of the user is maintained (e.g., stored) for the entry port module until the user logs off. Such user identifier may be stored in a list along with other user identifiers for other users that have been authenticated and are currently logged on to the port module. Such user identifier may be stored on a computer-readable medium accessible by the entry port module. The user identifier may be any information that was included in a login packet received from the user or any information included in the entry information retrieved from the authentication database for the user as described above in relation to Act 1314 . The user identifier 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. As will be described in more detail below in relation to Act 1401 of method 1400 , for each packet received at the entry port module after performance of Act 1319 , the user identifier may be accessed to determine an identity of the user of the user device from which the packet was received. Richmond '067 at [0227]: As described above in relation to 1304 , one or more roles (and/or service abstractions) may have been distributed to the network entry device. Accordingly, Act 1320 may include configuring the entry port module with the one or more packet rules corresponding to one or more of the roles and/or service abstractions that were distributed to the network entry device in Act 1304 . Richmond '067 at [0228]: In addition to or as an alternative to Acts 1318 and 1320 , one or more service abstractions corresponding to a user may be determined, and the entry port module may be configured with the packet rules associated with the one or more determined service abstractions. As described above in relation to distribution module 408 of FIG. 4, in addition to or as an alternative to distributing roles 432

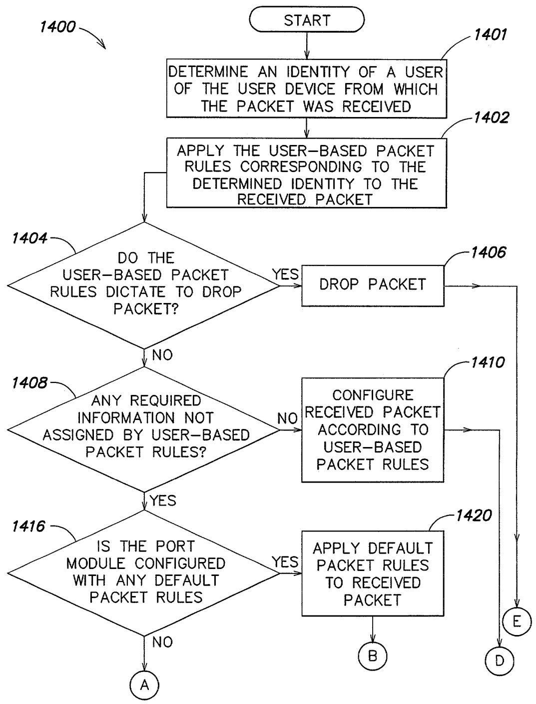
	to devices of a network, one or more relationship hierarchies and/or service abstractions also may be distributed. Thus, entries of authentication database 1508 or another database accessible by the authentication module 1506 may specify the one or more service abstractions assigned to a user, and this information may be used to determine the one or more service abstractions assigned to a user and to configure the entry port module with the packet rules associated with these one or more service abstractions, as similarly described in relation to Acts 1318 and 1320 with respect to the assigned role of a user. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0239]: In an embodiment of method 1300 , various acts of method 1300 and/or part thereof 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. Richmond '067 at [0243]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method 1400 for performing Act 1327.

	Richmond '067 at [0244]: In Act 1401 , an identity of a user of the user device from which the packet was received is determined. For example, information from the received packet may be compared against a list of user identifiers maintained by the entry port module as a result of performing Act 1319 . For example, 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 from an authentication packet received from the user device of the user, and Act 1319 may be repeated for a plurality of users. Accordingly, Act 1401 may include 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. Richmond '067 at [0246]: In Act 1402 , the user-based packet rules are applied to the received packet. 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. 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. Richmond '067 at [0267]: Rule database 1514 may include a plurality of rule sets 1518 , which may be indexed using a role identifier 1517 (and/or a service abstraction identifier-not shown). The storage of the rule sets 1518 and rule database 1514 may result from Act 1304 of method 1300 described above in relation to FIG. 13A. As described above, although a relationship hierarchy may have at least three levels, including packet rules, roles and service abstractions, a network entry device or other device of a network may not be configured with service abstractions, as such devices may only be concerned with the packet rules associated with a role. Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for configuring port module 1510 , for example, in accordance with the respective identities of one or more

	users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 . Richmond '067 at [0276]: System 1500 may include logic (not shown) for entering entry information in an entry 1528 , including assigning logic to assign a role identifier and/or one or more service abstraction identifiers to a user. Such logic may reside on any of one or more network devices of the network on which the system 1500 is implemented, including on network entry device 1504 , a user device, or the device on which the authentication module resides. A device on which at least a portion of such logic resides may include a user interface to enable a user to enter the entry information. Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 . Richmond '067 at [0280]: For each packet received at the entry port module, except login packets, the user identification logic may be configured to identify the user of the user device that transmitted the packet, for example, as described above in relation to act 1401 of method 1400 . For example, network entry device may include logic that creates a user identification list as described above in relation to act 1319 . Such list may be stored on network entry device 1504 or on any other network element of FIG. 15 accessible by network entry device 1504 . The determined user identity dictates the packet rules applied to the received packet by the rule application logic.

	Richmond '067 at [0281]: The rule application logic of port processing logic 1516 may be configured to apply, in response to receiving a packet 1502 at port module 1510 after a user has been authenticated, the rule set 1519 to the packet 1502 . The application of the rule set may be performed as described above in relation to method 1400 of FIGS. 14A and 14B. Thus, the rule application logic may be configured to apply one or more user-based packet rules, one or more default packet rules, and one or more other types of rules to the received packet. It should be noted that multiple rules may specify that a certain value be assigned to a parameter of the received packet that is to be configured. For example, two user-based packet rules, a default packet rule and another type of rule all may specify a different VLAN value to be applied to the received packet. Accordingly, the rule application logic may be configured to give precedence to certain rules over other rules.

	Richmond '067 at Fig. 13b:  FIG. 13B

	Richmond '067 at Fig. 14b:  FIG. 14A(1) FIG. 14A(2) FIG. 14B FIG. 14A(1)

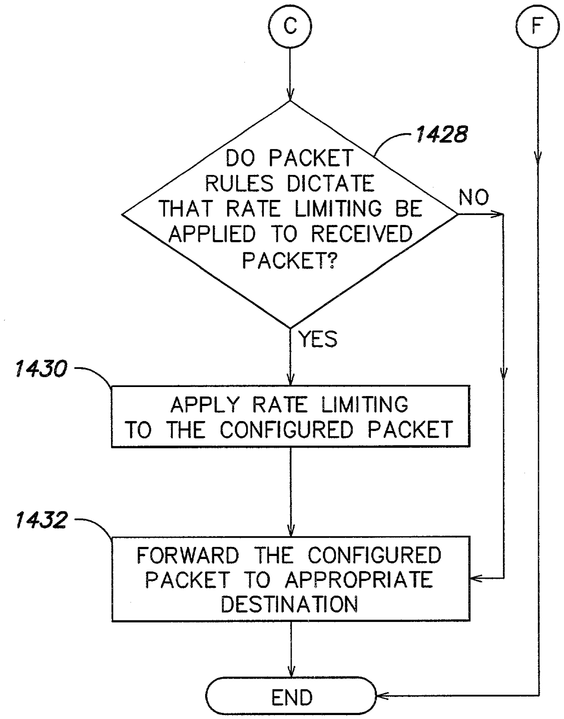
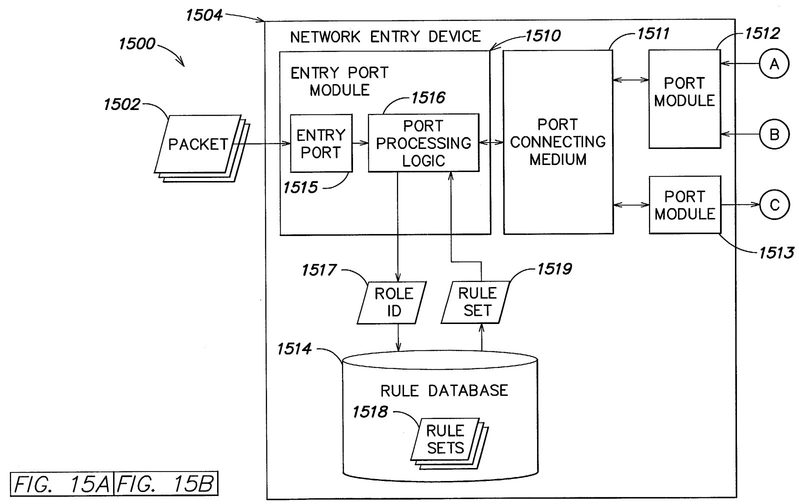
	Richmond '067 at Fig. 14b: 

FIG. 14B

	Richmond '067 at Fig. 15a:  FIG. 15A
[1.4] 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, 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, e.g.*: Richmond '067 at [0010]: Controlling usage of network resources may include, but is not limited to: denying one or more packets access to any network resources beyond a network device (i.e., dropping the packet); regulating bandwidth on the network consumed by packets received from the user, for example, by assigning priorities to received packets or applying rate limiting to received packets; denying access to certain network resources, for example, by assigning a Virtual Local Area Network (VLAN) to the packet; and routing the packet. VLANs are described in more detail in IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks , Dec. 8, 1998, the entire contents

	of which are hereby incorporated by reference. Assigning a VLAN to a packet and/or assigning a priority to a packet, may be referred to herein as "classifying" a packet. As used herein, a "packet" is a unit of communication exchanged between devices. Richmond '067 at [0014]: As used herein, a "port module" of a switching device includes a physical port of the device and port processing logic associated with the physical port. Such port processing logic may include 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. Such port processing logic may be divided into one or more virtual ports, each virtual port corresponding to a communication channel of the physical port. The port processing logic may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of a port module may be shared with several other port modules. A port module may be implemented as part of a port interface card (PIC), which may include one or more port modules. Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0042]: In an aspect of this embodiment, a first packet is received at the port module from a user device, and an identity of a user of the user device is determined. If the determined identity is the identity of the first user, then, before using any of the network resources beyond the network device in response to processing the first packet, at least the first rule is applied to the first packet. This process may be repeated for all packets received at the port module from the first user device until the first user logs off of the communications network.

	Richmond '067 at [0049]: In an aspect of this embodiment, the port module further comprises a physical port to receive a first packet from a user device and user identification logic to determine an identity of a user of the user device. The port module further comprises rule application logic to apply at least the first rule to the first packet, before using any of the network resources beyond the network device in response to processing packet, if the determined identity is the identity of the first user. Richmond '067 at [0054]: In yet another aspect of this embodiment, the port configuration logic is operative to select the first packet rule based on the identity of the first user and to select the at least one packet rule based on the identity of the second user. Richmond '067 at [0055]: In another aspect of this embodiment, the identity of the first user is associated with a role assigned to the first user. The role is associated with at least the first packet rule, and the port configuration logic is operative to select at least the first packet rule based on the role. Richmond '067 at [0061]: In another aspect of this embodiment, the one or more packet rules are selected based on the identity of the user. Richmond '067 at [0075]: In yet another aspect of this embodiment, the identity of the first user is associated with a role assigned to the first user, and the role is associated with at least the first packet rule, and the system further comprises means for selecting the first packet rule based on the role. Richmond '067 at [0082]: In another embodiment of the invention, usage of network resources of a communications network by a user is controlled. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. A packet including identification information of the user is received from a device of the user at a port module of a network device. The assigned role of the user is determined based on the identification information, and the port module is configured with the one or more packet rules associated with the assigned role of the user.

	Richmond '067 at [0106]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method of applying packet rules to a packet received at an entry port module of a network device of a communications network to control usage of network resources by a user; and Richmond '067 at [0112]: Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. 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, as opposed to applying the rules after the user has already consumed bandwidth and processing resources as is typical on a network with a more centralized firewall. Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0127]: Each rule may include a condition and an action to be taken if the condition is satisfied. Actions defined by packet rules may include, but are not limited to, assigning a VLAN to the packet, assigning priority to the packet, applying rate limiting to the packet, routing the packet, and dropping the packet. Richmond '067 at [0141]: For example, it may be determined that users that are assigned an executive role 204 should have Internet access, but should not be able to transmit packets on the network for managing devices on the network. This may lead to the creation of the Internet Access service abstraction 214 and the inclusion of this service abstraction in an executive role 204 , and the creation of the NO SNMP service abstraction 210 and the inclusion of this service abstraction in the executive role 204 . The Simple Network Management Protocol (SNMP) is a set of protocols for managing a network. Richmond '067 at [0156]: Priority field 516 may store a value representing a priority to be assigned to a packet that satisfies the conditions specified by fields 508 512 of an entry. For example, priority field 516 may store a value

	representing a Quality of Service (QoS)/Class of Service (CoS) as described in IEEE 802.1D, 1998 edition, accessible as of the filing date of this application at http://standards.ieee.org/getieee802/802.1.html, the entire contents of which is hereby incorporated by reference. Richmond '067 at [0157]: Deny field 518 may store a value (e.g., a flag) indicating whether or not to deny access to the resources of a communications network by a packet that satisfies conditions specified by fields 508 512 of an entry. Some packet rules may specify that a packet is to be dropped if the condition of the rule is satisfied. 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. 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. Richmond '067 at [0158]: Rate limit field 520 may store a value representing a rate limit to be applied to a packet if it satisfies the rule. Some rules may be defined such that if the condition of the rule is satisfied by a packet, then rate limiting will be applied to a packet. In such case, rate limit field 520 may specify a threshold value (e.g., 1 megabyte (MB)). This threshold value may specify a threshold volume of bytes that may be received during a specified temporal interval (e.g., one second) in packets that satisfy a particular rule. The temporal interval may be specified in field 520 itself or in another field. Richmond '067 at [0159]: For example, an entry of 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. Further, a network device may be configured to drop some or all of the bytes of a packet that contains an amount of packets that exceeds the threshold amount during the unit interval. Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume in sending packets to a particular network device specified by conditions 508 512 , or limit the amount of bandwidth that a user consumes on the network in sending packets corresponding to a particular application specified by conditions 508 512 . The consumption of bandwidth by a user also may be limited by the priority specified in field 516 .

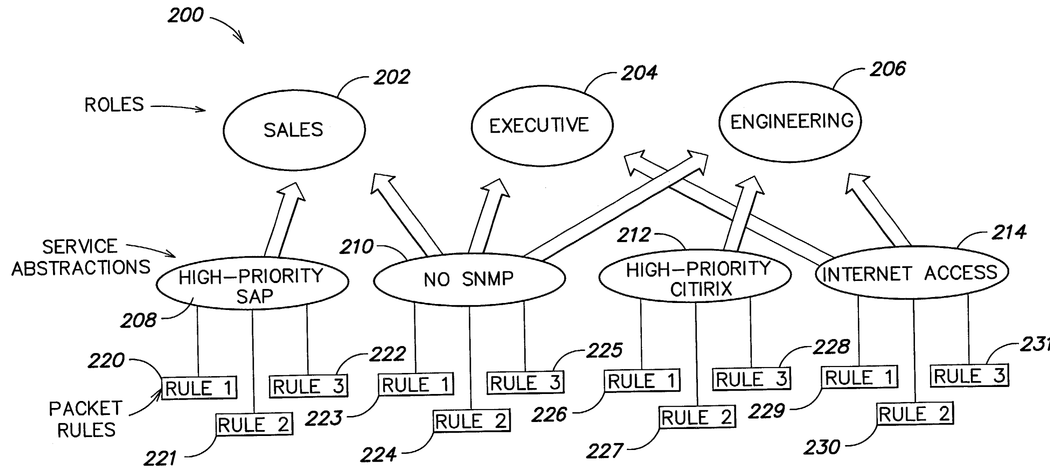
	Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules. Richmond '067 at [0222]: If in Act 1314 it is determined that the identification information is invalid (e.g., it does not match any entry of an authentication database), then in Act 1316 , the user may be denied access to the communications network. Whether or not the user is denied access may depend on the state defined for the entry port module in Act 1301 . Richmond '067 at [0225]: In a following Act 1320 , the entry port module may be configured with the packet rules associated with the determined role. The entry port module may remain configured as such until the user logs off. The entry port module may be dedicated to the user such that any packets received at the entry port module from a device other than the user device is dropped, until the user logs off. This is described in more detail below in relation to Act 1322 . Richmond '067 at [0227]: As described above in relation to 1304 , one or more roles (and/or service abstractions) may have been distributed to the network entry device. Accordingly, Act 1320 may include configuring the entry port module with the one or more packet rules corresponding to one or more of the roles and/or service abstractions that were distributed to the network entry device in Act 1304 . Richmond '067 at [0228]: In addition to or as an alternative to Acts 1318 and 1320 , one or more service abstractions corresponding to a user may be determined, and the entry port module may be configured with the packet rules associated with the one or more determined service abstractions. As described above in relation to distribution module 408 of FIG. 4, in addition to or as an alternative to distributing roles 432 to devices of a network, one or more relationship hierarchies and/or service abstractions also may be

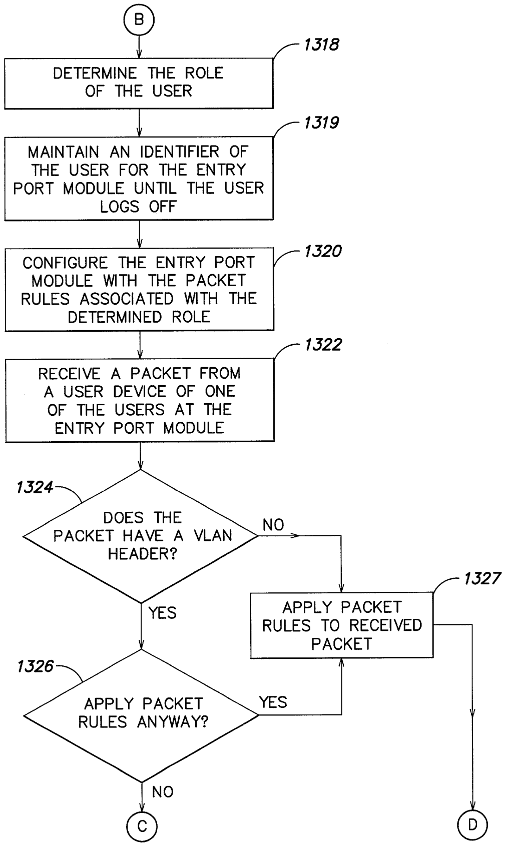
	distributed. Thus, entries of authentication database 1508 or another database accessible by the authentication module 1506 may specify the one or more service abstractions assigned to a user, and this information may be used to determine the one or more service abstractions assigned to a user and to configure the entry port module with the packet rules associated with these one or more service abstractions, as similarly described in relation to Acts 1318 and 1320 with respect to the assigned role of a user. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0231]: In an embodiment of method 1300 , following Act 1322 , packet rules, including the packet rules corresponding to the user from which the packet was received (i.e., user-based packet rules) and default rules, may be applied to the received packet in Act 1327 as described below in relation to FIG. 14. Richmond '067 at [0239]: In an embodiment of method 1300 , various acts of method 1300 and/or part thereof 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.

	Richmond '067 at [0243]: FIGS. 14A and 14B comprise a flow chart illustrating an example of a method 1400 for performing Act 1327 . Richmond '067 at [0246]: In Act 1402 , the user-based packet rules are applied to the received packet. 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. 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. Richmond '067 at [0247]: In Act 1404 , it may be determined whether the user-based packet rules dictate to drop the received packet. If the user-based packet rules dictate to drop the packet, then in Act 1406 , the packet is dropped and the method ends. Richmond '067 at [0248]: If in Act 1404 it is determined that the user-based packet rules do not dictate to drop the packet, then in Act 1408 it may be determined whether there is any required information that is not assigned by the user-based packet rules. For example, the entry port module may be configured such that certain information is required, for example, a VLAN and/or a priority. If it is determined in Act 1408 that there is not any required information that has not been assigned by the user-based packet rules, then in Act 1410 , the received packet may be configured according to the user-based packet rules. For example, a VLAN header may be configured to include a specific VLAN and/or priority based on the packet rules. Richmond '067 at [0249]: In a following Act 1428 , it may be determined whether the packet rules dictate that rate limiting is to be applied to the received packet. An entry port module may be configured to apply one or more rate limiting techniques, known now or later developed. Rate limiting is described above in more detail in relation to rate limit field 520 of packet rule data structure 500 of FIG. 5.

	Richmond '067 at [0251]: If it is determined in Act 1428 that the packet rules dictate that rate limiting be applied to the received packet, then in Act 1430 rate limiting may be applied to the received packet. Richmond '067 at [0267]: Rule database 1514 may include a plurality of rule sets 1518 , which may be indexed using a role identifier 1517 (and/or a service abstraction identifier-not shown). The storage of the rule sets 1518 and rule database 1514 may result from Act 1304 of method 1300 described above in relation to FIG. 13A. As described above, although a relationship hierarchy may have at least three levels, including packet rules, roles and service abstractions, a network entry device or other device of a network may not be configured with service abstractions, as such devices may only be concerned with the packet rules associated with a role. Richmond '067 at [0270]: Entry port module 1510 may include an entry port 1515 and port processing logic 1516 . 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. Port processing logic 1516 may be divided into one or more virtual ports (not shown), each virtual port corresponding to a communication channel of the entry port 1515 (e.g., if entry port 1515 is connected to a shared wireless transmission medium). Port processing logic 1516 may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of port processing logic 1516 may be shared with port processing logic of other port modules (e.g., 1512 and 1513). Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for configuring port module 1510 , for example, in accordance with the respective identities of one or more users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 .

	Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 . Richmond '067 at [0280]: For each packet received at the entry port module, except login packets, the user identification logic may be configured to identify the user of the user device that transmitted the packet, for example, as described above in relation to act 1401 of method 1400 . For example, network entry device may include logic that creates a user identification list as described above in relation to act 1319 . Such list may be stored on network entry device 1504 or on any other network element of FIG. 15 accessible by network entry device 1504 . The determined user identity dictates the packet rules applied to the received packet by the rule application logic. Richmond '067 at [0281]: The rule application logic of port processing logic 1516 may be configured to apply, in response to receiving a packet 1502 at port module 1510 after a user has been authenticated, the rule set 1519 to the packet 1502 . The application of the rule set may be performed as described above in relation to method 1400 of FIGS. 14A and 14B. Thus, the rule application logic may be configured to apply one or more user-based packet rules, one or more default packet rules, and one or more other types of rules to the received packet. It should be noted that multiple rules may specify that a certain value be assigned to a parameter of the received packet that is to be configured. For example, two user-based packet rules, a default packet rule and another type of rule all may specify a different VLAN value to be applied to the received packet. Accordingly, the rule application logic may be configured to give precedence to certain rules over other rules.

	Richmond '067 at Fig. 2:  FIG. 2

	Richmond '067 at Fig. 13b:  FIG. 13B

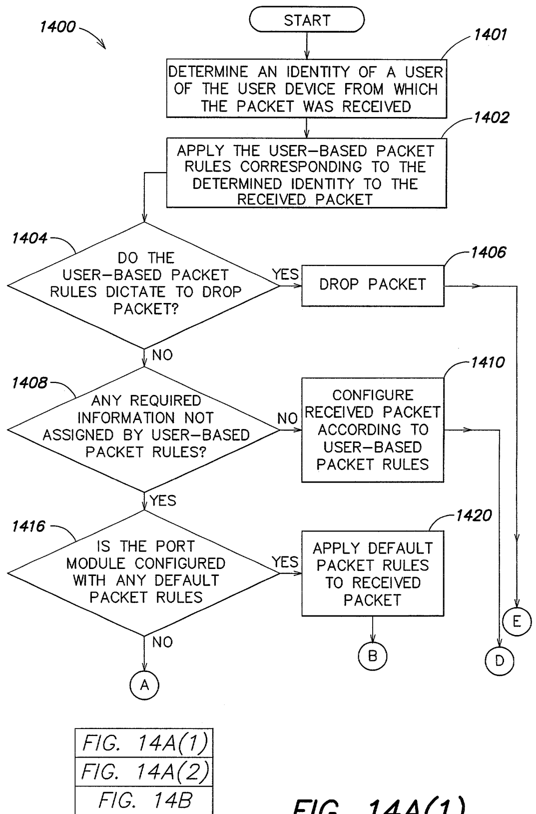
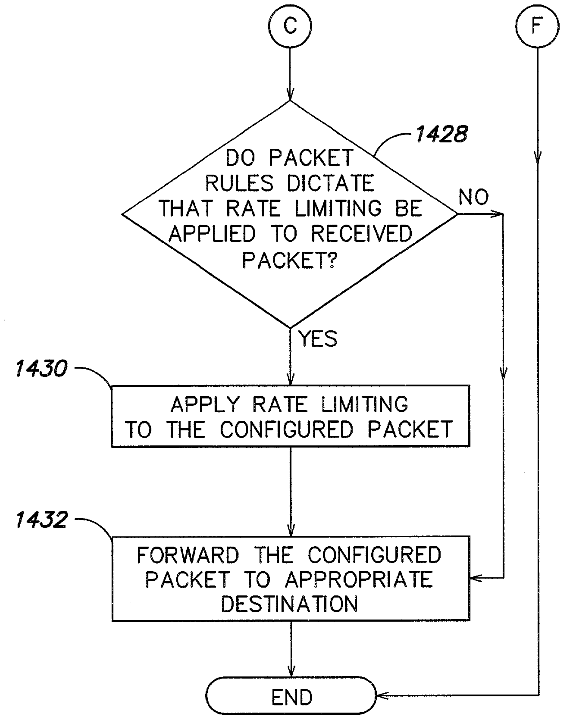
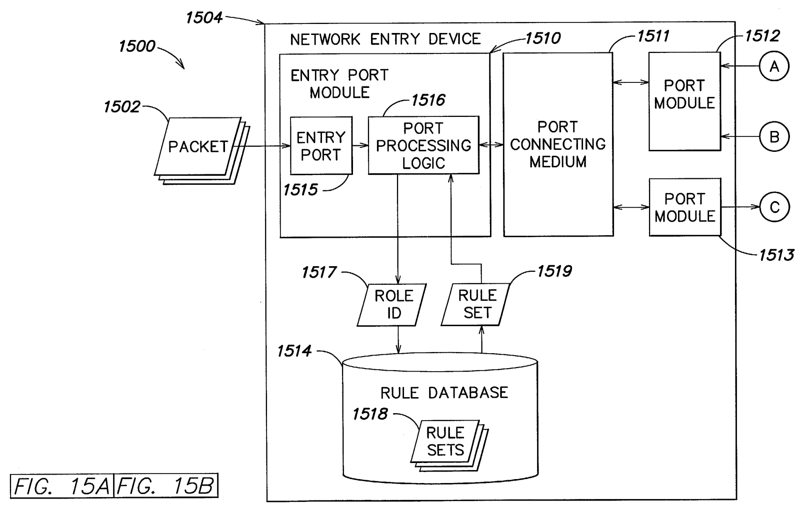
	Richmond '067 at Fig. 14b: 

FIG. 14A(1)

	Richmond '067 at Fig. 14b:  FIG. 14B

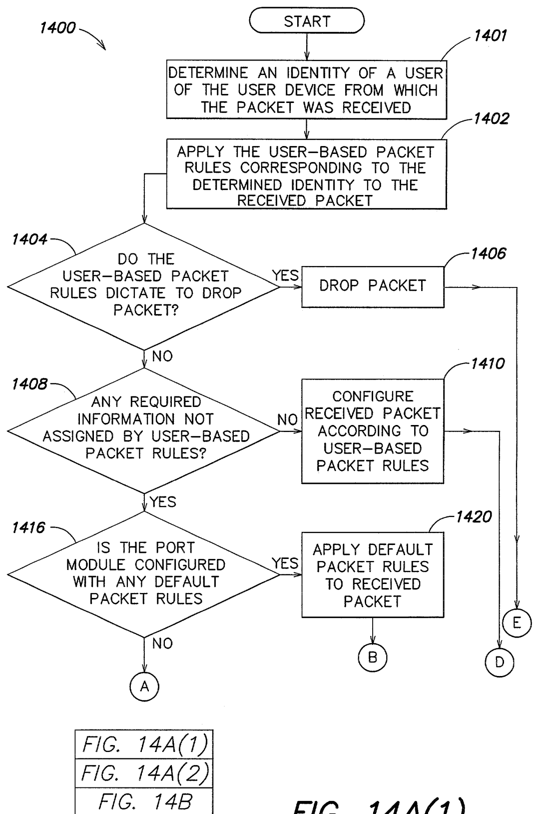
	Richmond '067 at Fig. 15a:  FIG. 15A
[2] The method according to claim 1, wherein the plurality of stages further comprises an interface specific stage, further comprising: at the interface specific stage, applying interface specific rules to the packet based on a type of a network interface over which the packet is received.	Richmond discloses: 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. *See, e.g.*: Richmond '067 at [0014]: As used herein, a "port module" of a switching device includes a physical port of the device and port processing logic associated with the physical port. Such port processing logic may include 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. Such port processing logic may be divided into one or more virtual ports, each virtual port corresponding to a communication channel of the physical port. The port processing logic may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of a port module may be shared with several other port modules. A port module may be implemented as part of a port interface card (PIC), which may include one or more port modules.

	Richmond '067 at [0015]: As used herein, an “entry port” is a physical port of a network device that serves as a user's entry point into a network. Thus, to communicate with devices on the network, a user's device may transmit one or more packets to an entry port. Further, as used herein, an “entry port module” is a port module of a network device that includes an entry port. Richmond '067 at [0023]: Entry port module 118 of network entry device 116 is connected to user devices by a shared wireless (i.e., air) transmission medium 119 , which by nature is a shared transmission medium. Multiple user devices may concurrently exchange packets with the entry port module 118 , using communication channels that share the transmission medium using known or later developed multiplexing schemes (e.g., time division, frequency division, code division, or combinations thereof). Accordingly, port module 118 may include a plurality of virtual ports, each virtual port corresponding to one of the communication channels. It should be noted that such multiplexing schemes, as well as others such as space division multiplexing, may be used on any port module (e.g., 108 , 118 and 146) on which multiple users share a transmission medium. Richmond '067 at [0207]: Further, it should be understood that methods 1300 and 1400 may be applied to configure individual virtual ports of a port module according to an identity of a user, for example, if the physical port of the port module of a wireless switching device (described below in more detail in relation to system 1500 of FIG. 15) and is connected to multiple user devices by a shared wireless transmission medium. Thus, multiple virtual ports of a port module may be configured differently, and may be configured according to different user identities. Richmond '067 at [0208]: In Act 1301 , a state of one or more port modules of a network entry device may be configured. For example, a port module may be configured to have an “authentication off/port on” state, where authentication is not required for a user to transmit packets onto the network and use the network resources. For a port module configured as such, Acts 1310 1336 of method 1300 may not be performed.

	Richmond '067 at [0209]: 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. Thus, a user cannot send any packets onto the network or receive any packets from the network until the user has successfully authenticated. Richmond '067 at [0210]: A port module of the network entry device may be configured with 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. For example, a network administrator may decide that all users should have access to some basic network services, such as access to the Internet or access to a word processing application, but not access to other network resources. Further, this state may be defined such that a port module that does not have an authenticated user attached thereto may be restricted such that all packets received at the port module and/or transmitted from the port module are assigned a lower priority, until a user is authenticated on the port module. Richmond '067 at [0231]: In an embodiment of method 1300 , following Act 1322 , packet rules, including the packet rules corresponding to the user from which the packet was received (i.e., user-based packet rules) and default rules, may be applied to the received packet in Act 1327 as described below in relation to FIG. 14. Richmond '067 at [0238]: Depending on the configuration of the entry port module, for example, as described above in relation to Acts 1301 and 1303 , after all users connected to the entry port module have logged off, the entry port module then may apply packet rules corresponding to a default role or one or more default services, and may apply other rules to all received packets, until another user authenticates at the entry port module. Alternatively, all packets may be denied access (e.g., dropped) to the communications network until another user authenticates at the entry port module. Richmond '067 at [0246]: In Act 1402 , the user-based packet rules are applied to the received packet. 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. 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.

	Richmond '067 at [0252]: Returning to Act 1408 , if it is determined that there is required information that has not been assigned by the user-based packet rules, then in Act 1416 it may be determined whether the entry port module is configured with any default packet rule. Default packet rules are described above in more detail in relation to Act 1303 of method 1300 of FIG. 13A. For example, an entry port module may be configured to assign a default priority to all packets received at the entry port module. Richmond '067 at [0253]: If it is determined in Act 1416 that the entry port module is not configured with any default packet rules, then, in Act 1418 , the packet may be configured based on user-based packet rules and possibly other additional rules with which the entry port module is configured. For example, even though an entry port module may not be configured with default packet rules, the entry port module may be configured to apply rules in accordance with known or later developed technologies, for example, IEEE 802.1D and/or 802.1Q. The method then may proceed to Act 1428 , which is described above. Richmond '067 at [0254]: If in Act 1416 it is determined that the entry port module is configured with default packet rules, then the default packet rules may be applied to the received packet in Act 1420 . Richmond '067 at [0257]: Thus, application of method 1400 to a received packet may result in a packet being configured based on user-based packet rules, default packet rules, and other additional rules with which the entry port module is configured. For example, the user-based packet rules may have assigned a VLAN to the received packet, the default packet rules may have assigned a priority to the received packet, and other rules may have applied rate limiting to the packet. Richmond '067 at [0263]: Further, it should be understood that system 1500 may be operative to configure individual virtual ports of a port module according to an identity of a user, for example, if the physical port of the port module is connected to multiple user devices by a shared, wireless transmission medium. Thus, multiple virtual ports of a port module may be configured differently, and may be configured according to different user identities.

	Richmond '067 at [0264]: Virtual ports may be used by a wireless switching device that aggregates and provides connectivity to the communications network for a plurality of mobile user devices. For example, network entry device 1504 may be a wireless switching device. A wireless switching device may include a wireless access module (e.g., a transceiver) and a switching module (e.g., an Ethernet router). The wireless access module may be configured to apply radio-based protocols (e.g., RF protocols) to transmit, receive, modulate, demodulate, multiplex, de-multiplex and authenticate wireless transmissions to/from user devices. Such wireless access module, possibly in combination with the switching module may build a virtual port for each communication channel, where each communication channel corresponds to a user transmitting/receiving at a particular predefined frequency (or a plurality of frequencies in sequence in accordance with a code division multiplexing scheme) during certain predefined timeslots. Thus each virtual port may be dedicated to a particular user and user device, and methods 1300 and 1400 may be performed for each virtual port. Richmond '067 at [0270]: Entry port module 1510 may include an entry port 1515 and port processing logic 1516 . 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. Port processing logic 1516 may be divided into one or more virtual ports (not shown), each virtual port corresponding to a communication channel of the entry port 1515 (e.g., if entry port 1515 is connected to a shared wireless transmission medium). Port processing logic 1516 may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of port processing logic 1516 may be shared with port processing logic of other port modules (e.g., 1512 and 1513). Richmond '067 at [0281]: The rule application logic of port processing logic 1516 may be configured to apply, in response to receiving a packet 1502 at port module 1510 after a user has been authenticated, the rule set 1519 to the packet 1502 . The application of the rule set may be performed as described above in relation to method 1400 of FIGS. 14A and 14B. Thus, the rule application logic may be configured to apply one or more user-based packet rules, one or more default packet rules, and one or more other types of rules to the received packet. It should be noted that multiple rules may specify that a certain value be assigned to a parameter of the received packet that is to be configured. For example, two user-based packet rules, a

	default packet rule and another type of rule all may specify a different VLAN value to be applied to the received packet. Accordingly, the rule application logic may be configured to give precedence to certain rules over other rules. Richmond '067 at Fig. 14b:  FIG. 14A(1)
[3] The method according to claim 2, wherein the plurality of stages further comprises a global stage,	Richmond discloses: 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. *See, e.g.*:

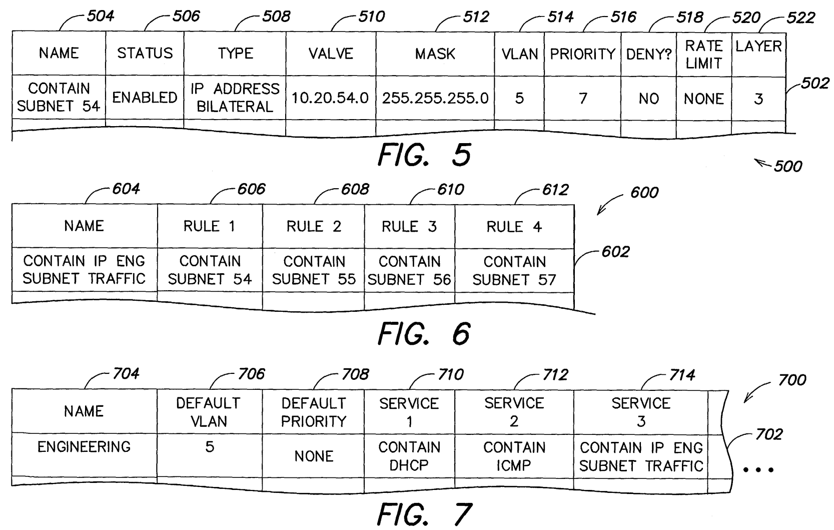
further comprising: at the global stage, applying global firewall rules to the packet.	Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0036]: Such firewall may perform similar analysis to incoming packets from users (e.g., user 150) outside of the private network to control usage of resources of the private network. For example, the firewall may be configured to prevent unauthorized users from accessing network resources (e.g., screening emails from an outside user), and may be configured to establish a Virtual Private Network (VPN) across one or more publicly-accessible networks (e.g., the Internet) with a user device. Richmond '067 at [0037]: Similar to as described above for applications employing user authentication, a problem with typical firewalls is that users are allowed to use network resources beyond their respective entry points to the network before the firewall is ever enforced. Specifically, for each packet transmitted by a user, the user consumes bandwidth on transmission media between the network device serving as the user's entry point and the network device on which the firewall resides, consumes processing power on switching devices between the user device and the network device, and consumes processing power on the network device on which the firewall resides while executing the programs of the firewall. Richmond '067 at [0194]: Returning to FIG. 4, the distribution module 408 may be configured to access one or more roles 430 from relationship database 410 and distribute one or more roles 432 to one or more devices of a network. For example, system 400 may reside on a user device, for example, one of the user devices of network 100 , and distribution module 408 may be configured to distribute the roles 432 to any of the devices

	described above in relation to FIG. 1. Roles 432 then may be used to configure a component of a network device, for example, a port module or a firewall, as described below in more detail. Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules. Richmond '067 at [0208]: In Act 1301 , a state of one or more port modules of a network entry device may be configured. For example, a port module may be configured to have an "authentication off/port on" state, where authentication is not required for a user to transmit packets onto the network and use the network resources. For a port module configured as such, Acts 1310 1336 of method 1300 may not be performed. Richmond '067 at [0209]: 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. Thus, a user cannot send any packets onto the network or receive any packets from the network until the user has successfully authenticated. Richmond '067 at [0210]: A port module of the network entry device may be configured with 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. For example, a network administrator may decide that all users should have access to some basic network services, such as access to the Internet or access to a word processing application, but not access to other network resources. Further, this state may be defined such that a port module that does not have an authenticated user attached thereto may be restricted such that all packets received at the port module and/or transmitted from the port module are assigned a lower priority, until a user is authenticated on the port module.

	Richmond '067 at [0212]: In Act 1303 , one or more port modules of the network entry device may be configured with a default role (i.e., one or more default packet rules) that define default behavior for the port module. For example, a port module may be configured to assign a certain priority or VLAN to all packets received at the port module until the port module has been configured based on the respective identities of one or more users. Further, a default role may be configured for a port module for which authentication capability has not been enabled. Such default role configuring may be desirable for network devices that do not require authentication or are incapable of authentication, for example, printers, fax machines, and legacy devices such as software-based routers and shared hubs. Richmond '067 at [0252]: Returning to Act 1408 , if it is determined that there is required information that has not been assigned by the user-based packet rules, then in Act 1416 it may be determined whether the entry port module is configured with any default packet rule. Default packet rules are described above in more detail in relation to Act 1303 of method 1300 of FIG. 13A. For example, an entry port module may be configured to assign a default priority to all packets received at the entry port module. Richmond '067 at [0253]: If it is determined in Act 1416 that the entry port module is not configured with any default packet rules, then, in Act 1418 , the packet may be configured based on user-based packet rules and possibly other additional rules with which the entry port module is configured. For example, even though an entry port module may not be configured with default packet rules, the entry port module may be configured to apply rules in accordance with known or later developed technologies, for example, IEEE 802.1D and/or 802.1Q. The method then may proceed to Act 1428 , which is described above. Richmond '067 at [0256]: If it is determined in Act 1422 that there is still required information not yet assigned, then in Act 1424 , the packet will be configured based on the user-based packet rules and default packet rules applied in Acts 1402 and 1420 , respectively, and any other additional rules with which the entry port module is configured. The method then may proceed to act 1428 . Richmond '067 at [0262]: Although system 1500 illustrates an entry port module 1510 of a network entry device 1504 configured to control usage of network resources by one or more users based on the respective identities of such

	users, other port modules of the network entry device (e.g., port modules 1512 and 1513) may be configured as such. Further other components of the network entry device 1504 or components (e.g., a firewall) of other devices of the network may be configured as such.
[4] 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: 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. *See, e.g.*: Richmond '067 at [0143]: Returning to FIG. 3, in Act 308 , the relationship hierarchy may be stored for later use, for example, on a computer-readable medium such as relationship database 410 described below in relation to FIG. 4. Richmond '067 at [0150]: FIG. 5 is a block diagram illustrating an example of a packet rule data structure 500 for storing one or more packet rules. Such data structure 500 may be a table of a relational database, an object of an object-oriented database, a record of a flat file, a combination thereof, or other type of data structure. Data structure 500 may be included as part of relationship database 410 and may store one or more of the packet rules 428 . Richmond '067 at [0170]: FIG. 6 is a block diagram illustrating an example of a service data structure 600 for storing one or more service abstractions. Such data structure 600 may be a table of a relational database, an object of an object-oriented database, a record of a file, a combination thereof, or other type of data structure. Data structure 600 may be included as part of relationship database 410 and may include one or more of the service abstractions 426 . The data structure may include a plurality of entries, including entry 602 . Each entry may include a plurality of fields including, but not limited to, name field 604 and rule fields 606 612 . Richmond '067 at [0175]: FIG. 7 is a block diagram illustrating an example of a role data structure 700 for storing one or more roles. Such role data structure 700 may be a table of a relational database, an object of an object-oriented database, a record of a file, a combination thereof or other type of data structure. Data structure 700 may be included as part of relationship database 410 and may include one or more of the roles 424 .

	Richmond '067 at [0267]: Rule database 1514 may include a plurality of rule sets 1518 , which may be indexed using a role identifier 1517 (and/or a service abstraction identifier-not shown). The storage of the rule sets 1518 and rule database 1514 may result from Act 1304 of method 1300 described above in relation to FIG. 13A. As described above, although a relationship hierarchy may have at least three levels, including packet rules, roles and service abstractions, a network entry device or other device of a network may not be configured with service abstractions, as such devices may only be concerned with the packet rules associated with a role. Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 . Richmond '067 at [0281]: The rule application logic of port processing logic 1516 may be configured to apply, in response to receiving a packet 1502 at port module 1510 after a user has been authenticated, the rule set 1519 to the packet 1502 . The application of the rule set may be performed as described above in relation to method 1400 of FIGS. 14A and 14B. Thus, the rule application logic may be configured to apply one or more user-based packet rules, one or more default packet rules, and one or more other types of rules to the received packet. It should be noted that multiple rules may specify that a certain value be assigned to a parameter of the received packet that is to be configured. For example, two user-based packet rules, a default packet rule and another type of rule all may specify a different VLAN value to be applied to the received packet. Accordingly, the rule application logic may be configured to give precedence to certain rules over other rules.

	Richmond '067 at Fig. 5: 
[5] 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: 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. *See, e.g.*: Richmond '067 at [0150]: FIG. 5 is a block diagram illustrating an example of a packet rule data structure 500 for storing one or more packet rules. Such data structure 500 may be a table of a relational database, an object of an object-oriented database, a record of a flat file, a combination thereof, or other type of data structure. Data structure 500 may be included as part of relationship database 410 and may store one or more of the packet rules 428 . Richmond '067 at [0151]: The data structure 500 may include a plurality of entries, including entry 502 . Each entry may include a plurality of fields, including, but not limited to, name field 504 , status field 506 , type field 508 ,

	value field 510 , mask field 512 , VLAN field 515 , priority field 516 , deny field 518 , rate limit field 520 and layer field 522 . Richmond '067 at [0154]: Value field 510 may store a value to be compared against information included in a packet to determine if the information matches the value. Mask field 512 may store a value representing a mask to be applied to the information in the packet to be compared to the value field 510 . For example, a bit-wise logical AND operation may be performed between the value stored in mask field 512 and the value of the information included in the packet specified by type field 508 . The result of this comparison then may be compared to the value specified in value field 510 . The mask field 512 may be used only for certain packet rules, for example, rules that specify an IP subnetwork address. Richmond '067 at [0162]: Field 508 of entry 502 specifies that the type of the packet rule is “IP Address Bilateral.” This type of packet rule may specify that the source and destination (i.e., bilateral) IP addresses of a packet are to be examined. Richmond '067 at [0163]: Field 510 of entry 502 specifies that the value to be compared to the IP addresses of the received packet is “10.20.54.0,” where each decimal value represents an 8-bit binary value. Further, mask field 412 specifies that a mask of “255.255.255.0” (which represents 3 octets of binary “1”s followed by an octet of all “0”s) is to be ANDed to both the IP source address and the IP destination address before comparing these addresses to the binary equivalent of “10.20.54.0” (i.e., “00110110.00010000.00001010.00000000”). Richmond '067 at [0164]: VLAN field 514 of entry 502 has a value of “5”, specifying that should the IP source address or IP destination address match the value stored in value field 510 after applying the mask 512 , then the received packet shall be assigned a VLAN value of 5, where the value of 5 may correspond to a particular VLAN such as an engineering VLAN. Thus, a device configured with the packet rule represented by entry 502 may be configured to append a VLAN header to a received packet, where the VLAN header includes a field specifying VLAN 5 . Further, such device may be configured to change the VLAN header to specify VLAN 5 if the received packet already includes a VLAN header.

	Richmond '067 at [0173]: Field 606 of entry 602 specifies that the packet rule entitled "Contain Subnet 54" is included as part of this service abstraction. This value may be used to index entry 502 of the packet rule data structure 500 . Each of fields 608 612 of entry 602 specifies another packet rule included as part of this service. The names stored in these fields in FIG. 6 imply that these rules may specify similar conditions and actions for packets that include a destination or source IP address corresponding to subnetworks 55 , 56 or 57 , respectively. Richmond '067 at [0224]: In Act 1319 , an identifier of the user is maintained (e.g., stored) for the entry port module until the user logs off. Such user identifier may be stored in a list along with other user identifiers for other users that have been authenticated and are currently logged on to the port module. Such user identifier may be stored on a computer-readable medium accessible by the entry port module. The user identifier may be any information that was included in a login packet received from the user or any information included in the entry information retrieved from the authentication database for the user as described above in relation to Act 1314 . The user identifier 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. As will be described in more detail below in relation to Act 1401 of method 1400 , for each packet received at the entry port module after performance of Act 1319 , the user identifier may be accessed to determine an identity of the user of the user device from which the packet was received. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged

<table>
<tr>
<td></td>
<td>

on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off.

Richmond '067 at [0244]:
In Act 1401 , an identity of a user of the user device from which the packet was received is determined. For example, information from the received packet may be compared against a list of user identifiers maintained by the entry port module as a result of performing Act 1319 . For example, 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 from an authentication packet received from the user device of the user, and Act 1319 may be repeated for a plurality of users. Accordingly, Act 1401 may include 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.

Richmond '067 at Fig. 5:

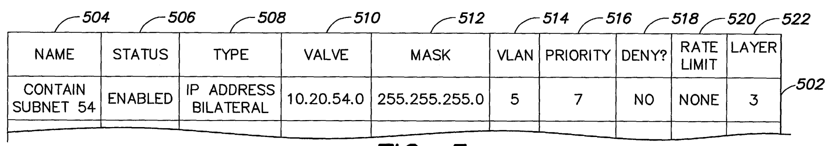


FIG. 5

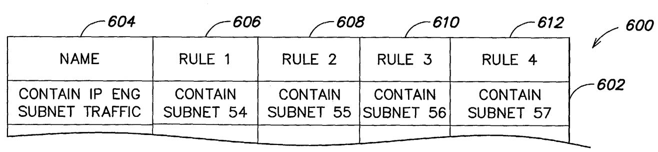


FIG. 6

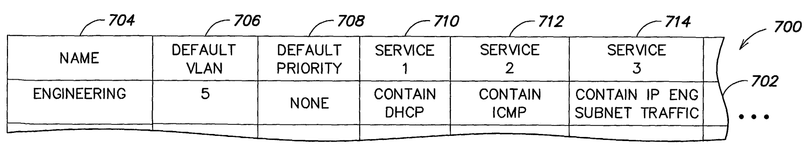


FIG. 7

</td>
</tr>
<tr>
<td>[6] The method according to claim 5, wherein the user device is associated with a</td>
<td>Richmond discloses: 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.</td>
</tr>
</table>

media access control (MAC) address and wherein the at least one user specific rule is further associated with the MAC address.	*See, e.g.*: Richmond '067 at [0033]: Another technique for controlling usage of network resources is to analyze information included in packets and forward the received packets based on the information. For example, some switching devices may be configured to examine information included in a received packet, for example, a source Media Access Control (MAC) address, a destination MAC address, or a protocol, and forward the packet or assign a VLAN header to the packet based on this information, for example, as described in more detail in IEEE 802.1Q. A switching device configured as such may serve as an entry point to the network for one or more users. Richmond '067 at [0128]: Packet rules may be configured to examine any information included in a packet. As is known in the field of network communications, different portions of a packet may include information pertaining to different protocol layers. These layers may include an application layer, presentation layer, session layer, transport layer, network layer and data link layer, which correspond to layers seven through two, respectively, of the Open System Interconnection (OSI) networking framework model. A packet rule may be defined to examine any portion of a packet, and thereby examine information pertaining to any protocol layer. For example, a packet rule may be configured to examine information in a packet as described in Layer 2/3/4 Frame Classification Primer , a white paper made available from Enterasys Networks, Inc., accessible as of the date of the filing of this application at http://www.enterasys.com/products/whitepapers/switching/layer-primer/index.html, the entire contents of which are hereby incorporated by reference. Richmond '067 at [0224]: In Act 1319 , an identifier of the user is maintained (e.g., stored) for the entry port module until the user logs off. Such user identifier may be stored in a list along with other user identifiers for other users that have been authenticated and are currently logged on to the port module. Such user identifier may be stored on a computer-readable medium accessible by the entry port module. The user identifier may be any information that was included in a login packet received from the user or any information included in the entry information retrieved from the authentication database for the user as described above in relation to Act 1314 . The user identifier 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. As will be described in more detail below

	in relation to Act 1401 of method 1400 , for each packet received at the entry port module after performance of Act 1319 , the user identifier may be accessed to determine an identity of the user of the user device from which the packet was received. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0244]: In Act 1401 , an identity of a user of the user device from which the packet was received is determined. For example, information from the received packet may be compared against a list of user identifiers maintained by the entry port module as a result of performing Act 1319 . For example, 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 from an authentication packet received from the user device of the user, and Act 1319 may be repeated for a plurality of users. Accordingly, Act 1401 may include 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. Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for

	configuring port module 1510 , for example, in accordance with the respective identities of one or more users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 .
[7] 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: 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. *See, e.g.*: Richmond '067 at [0088]: In another aspect of this embodiment, user information about the user is stored on a computer-readable medium residing on the communications network, where the user information includes identification information and the assigned role of the user. The authentication module is operative to control accessing the stored user information to determine if the identification information included therein matches the identification information included in the received packet, and to determine the assigned role from the stored user information if it is determined that the stored identification information matches the received identification information. Richmond '067 at [0121]: In another embodiment of the invention, one or more roles may be created. As used herein, a "role" or "role abstraction" is an abstraction representing a named set of one or more packet rules associated with a role of a person, for example, in relation to an organization or communications network. In an aspect of this embodiment, a role is an abstraction representing a named set of one or more service abstractions. Such roles may be stored and later modified, and may be distributed to one or more network devices. Roles may be assigned to one or more users of the network, and may be used to configure a port module of a network device. Richmond '067 at [0140]: Regardless of the method by which a relationship hierarchy is created, it may be desirable to design the structure of the hierarchy using a top-down approach. Using such approach, the roles that are to be created are first determined. Such roles may be designed to reflect the infrastructure of a network and/or roles within an organization whose members are users of the network. Next, for each role, the service abstractions to be associated with the role may be determined.

	Richmond '067 at [0141]: For example, it may be determined that users that are assigned an executive role 204 should have Internet access, but should not be able to transmit packets on the network for managing devices on the network. This may lead to the creation of the Internet Access service abstraction 214 and the inclusion of this service abstraction in an executive role 204 , and the creation of the NO SNMP service abstraction 210 and the inclusion of this service abstraction in the executive role 204 . The Simple Network Management Protocol (SNMP) is a set of protocols for managing a network. Richmond '067 at [0143]: Returning to FIG. 3, in Act 308 , the relationship hierarchy may be stored for later use, for example, on a computer-readable medium such as relationship database 410 described below in relation to FIG. 4. Richmond '067 at [0149]: The relationship database 410 may include one or more relationship hierarchies 423 , each relationship hierarchy 423 including one or more roles 424 , one or more service abstractions 426 and one or more packet rules 428 , such as those described below in relation to FIGS. 5 7 . Richmond '067 at [0150]: FIG. 5 is a block diagram illustrating an example of a packet rule data structure 500 for storing one or more packet rules. Such data structure 500 may be a table of a relational database, an object of an object-oriented database, a record of a flat file, a combination thereof, or other type of data structure. Data structure 500 may be included as part of relationship database 410 and may store one or more of the packet rules 428 . Richmond '067 at [0170]: FIG. 6 is a block diagram illustrating an example of a service data structure 600 for storing one or more service abstractions. Such data structure 600 may be a table of a relational database, an object of an object-oriented database, a record of a file, a combination thereof, or other type of data structure. Data structure 600 may be included as part of relationship database 410 and may include one or more of the service abstractions 426 . The data structure may include a plurality of entries, including entry 602 . Each entry may include a plurality of fields including, but not limited to, name field 604 and rule fields 606 612.

	Richmond '067 at [0175]: FIG. 7 is a block diagram illustrating an example of a role data structure 700 for storing one or more roles. Such role data structure 700 may be a table of a relational database, an object of an object-oriented database, a record of a file, a combination thereof or other type of data structure. Data structure 700 may be included as part of relationship database 410 and may include one or more of the roles 424 . Richmond '067 at [0181]: Field 704 of entry 702 specifies that this role is named "Engineering." This role may correspond to an engineering department of a company and/or one or more subnetworks of the communications network associated with the engineering department. Field 706 of entry 702 specifies that the default VLAN for the engineering role is VLAN 5 . Field 708 of entry 702 specifies that there is not a default COS for the engineering role. Richmond '067 at [0215]: In Act 1308 , user information about the one or more users to which the respective roles are assigned may be stored on the communications network. This user information may include identification information of the user and the assigned role of the user. The identification information may include a user name, password, and other credentials of the user, for example, personal information about the user such as the user's social security number, birth date, or other piece of information. The user information may be stored in an authentication database, for example, authentication database 1508 described below in relation to FIG. 15. Richmond '067 at [0223]: If it is determined in Act 1314 that the identification information is valid, then in Act 1318 , the role of the user may be determined. For example, the entry information 1529 extracted from authentication database 1508 may include a role identifier (ID) corresponding to the user, from which the authentication module may determine the role of the user. Alternatively, the authentication module may access another database that includes a plurality of entries, where each entry corresponds to a user and includes a role assigned to the user, from which the authentication module 1506 may determine the role of a user. Richmond '067 at [0228]: In addition to or as an alternative to Acts 1318 and 1320 , one or more service abstractions corresponding to a user may be determined, and the entry port module may be configured with the

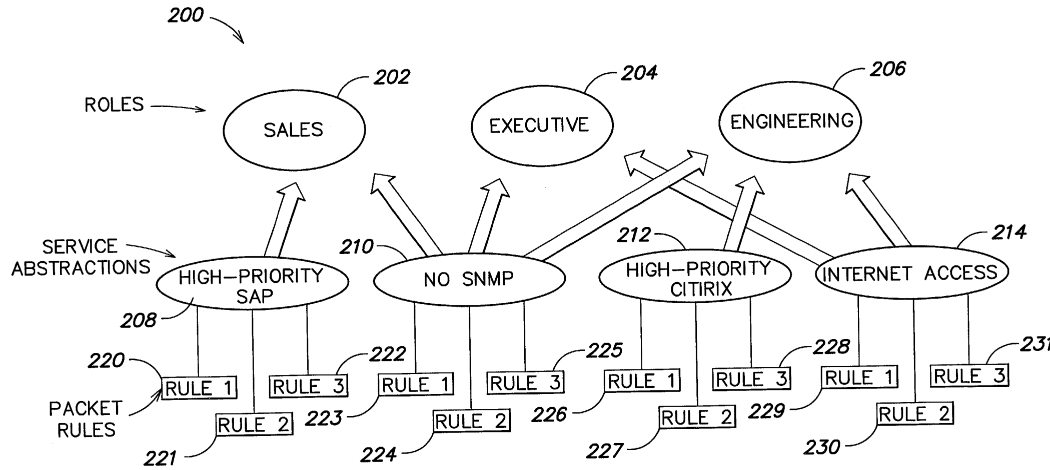
	packet rules associated with the one or more determined service abstractions. As described above in relation to distribution module 408 of FIG. 4, in addition to or as an alternative to distributing roles 432 to devices of a network, one or more relationship hierarchies and/or service abstractions also may be distributed. Thus, entries of authentication database 1508 or another database accessible by the authentication module 1506 may specify the one or more service abstractions assigned to a user, and this information may be used to determine the one or more service abstractions assigned to a user and to configure the entry port module with the packet rules associated with these one or more service abstractions, as similarly described in relation to Acts 1318 and 1320 with respect to the assigned role of a user. Richmond '067 at [0275]: The authentication module 1506 may be configured such that an entry 1528 is accessed using user information 1526 , and entry information 1529 is retrieved. Entry information 1529 may include credential information such as a password and other information, including a role identifier (ID) or one or more service abstraction IDs. The authentication module 1506 may be configured such that if the credential information of entry information 1529 does not match the credential information included in packet 1522 , then authentication response packet 1520 may include an indication that the identification information of the user is not valid. Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 .

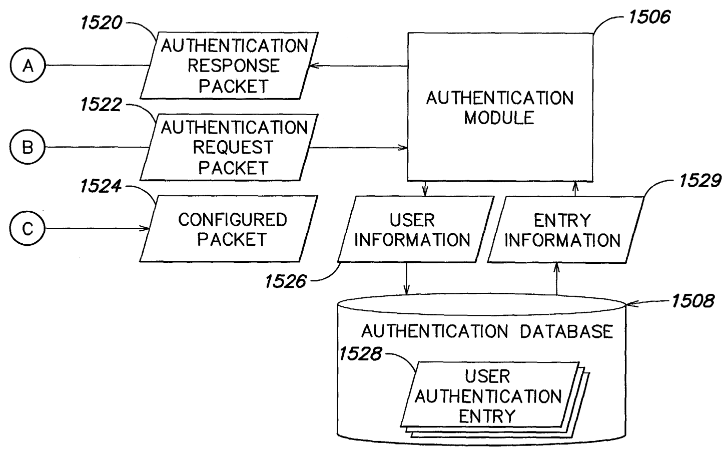
	Richmond '067 at [0279]: In an alternative embodiment of network entry device 1504 , port module 1510 may already be configured with one or more rule sets 1518 , but the rule sets have a disabled status. In response to a successful authentication, the port configuration logic of the port module 1510 may be configured to enable the one or more rule sets associated with the role ID or one or more service abstraction IDs included in authentication response packet 1520 .
[8] A method according to claim 1, further comprising determining whether the user has authenticated.	Richmond discloses: A method according to claim 1, further comprising determining whether the user has authenticated. *See, e.g.*: Richmond '067 at [0110]: For each of the one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. Richmond '067 at [0209]: 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. Thus, a user cannot send any packets onto the network or receive any packets from the network until the user has successfully authenticated. Richmond '067 at [0210]: A port module of the network entry device may be configured with 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. For example, a network administrator may decide that all users should have access to some basic network services, such as access to the Internet or access to a word processing application, but not access to other network resources. Further, this state may be defined such that a port module that does not have an authenticated user attached thereto may be restricted such that all packets received at the port module and/or transmitted from the port module are assigned a lower priority, until a user is authenticated on the port module.

	Richmond '067 at [0220]: In a following Act 1312 , the received identification information may be authenticated. Any of a variety of authentication techniques may be used to authenticate the received identification information, for example, RADIUS, a NOS login, or 802.1X. Other types of authentication techniques may be used. For example, referring to FIG. 15, an authentication database 1508 may be searched using user information 1526 for a user authentication entry 1528 corresponding to the identification information received in the login packet. If such user authentication entry 1528 is not found, the identification information may be deemed invalid. If such entry 1528 is found, then entry information 1529 may be sent from the authentication database to the authentication module 1506 . If the identification information included in the entry information 1529 does not match the identification information of the login packet, the identification information of the login packet may be deemed invalid. Richmond '067 at [0222]: If in Act 1314 it is determined that the identification information is invalid (e.g., it does not match any entry of an authentication database), then in Act 1316 , the user may be denied access to the communications network. Whether or not the user is denied access may depend on the state defined for the entry port module in Act 1301 . Richmond '067 at [0223]: If it is determined in Act 1314 that the identification information is valid, then in Act 1318 , the role of the user may be determined. For example, the entry information 1529 extracted from authentication database 1508 may include a role identifier (ID) corresponding to the user, from which the authentication module may determine the role of the user. Alternatively, the authentication module may access another database that includes a plurality of entries, where each entry corresponds to a user and includes a role assigned to the user, from which the authentication module 1506 may determine the role of a user. Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0273]: The authentication logic of port processing logic 1516 may be configured such that, if a packet 1502 is received and is a login packet including identification information of a user, the authentication logic controls the forwarding of an authentication request packet 1522 that includes the identification information from the port module 1510 through the port connecting medium 1511 and port module 1512 to authentication module 1506 . Such user information may include a user identifier (ID) (i.e., a user name), a password and other user credentials. In an embodiment, for example, when the authentication module 1506 resides on the network entry device 1504 , the authentication logic may be integrated as part of the authentication module 1506 . Further, the authentication logic may not be included as part of the port processing logic, but may be a separate and distinct component of network entry device 1504 . Richmond '067 at [0274]: Authentication module 1506 may be configured to perform authentication in accordance with one or more authentication technologies, for example, RADIUS, a NOS, and IEEE 802.1X. The authentication module 1506 may be configured to access a user authentication entry 1528 of authentication database 1508 using user information 1526 , for example, using the user ID. If the authentication module 1506 cannot find an entry 1528 corresponding to the user information 1526 , then an authentication response packet 1520 sent from the authentication module to the authentication logic of port processing logic 1516 may indicate that the user is not a valid user of the network. Richmond '067 at [0275]: The authentication module 1506 may be configured such that an entry 1528 is accessed using user information 1526 , and entry information 1529 is retrieved. Entry information 1529 may include credential information such as a password and other information, including a role identifier (ID) or one or more service abstraction IDs. The authentication module 1506 may be configured such that if the credential information of entry information 1529 does not match the credential information included in

	packet 1522 , then authentication response packet 1520 may include an indication that the identification information of the user is not valid. Richmond '067 at [0277]: The authentication module 1506 may be configured such that if the credential information of packet 1522 matches the credential information of entry information 1529 , then authentication response packet 1520 includes the role ID or one or more service abstraction IDs corresponding to the user. Such role ID or one or more service abstraction IDs may have been stored in the entry 1528 corresponding to the user and included in entry information 1529 or may have been stored in another location (e.g., another database) accessed by authentication module 1506 . Richmond '067 at [0278]: As described above in relation to Act 1301 , one or more port modules of a network entry device may be configured with a state. Accordingly, port configuration logic of port processing logic 1516 may be operative to configure port module 1510 in accordance with one of the states described above in relation to act 1301 if authentication response packet 1520 indicates that authentication of the user has failed and port module 1510 is not already configured with one or more packet rules corresponding to another user. The port configuration logic further may be configured such that, if the authentication response packet 1520 indicates that authentication of the user was successful, and packet 1520 includes a role ID or one or more service abstraction IDs of the user, the port configuration logic selects and extracts a rule set 1518 from rule database 1514 using the role ID 1517 or the one or more service abstraction IDs. As a result, port configuration logic receives rule set 1519 and configures port module 1510 accordingly, for example, as described above in relation to Act 1320 of method 1300 . Richmond '067 at [0279]: In an alternative embodiment of network entry device 1504 , port module 1510 may already be configured with one or more rule sets 1518 , but the rule sets have a disabled status. In response to a successful authentication, the port configuration logic of the port module 1510 may be configured to enable the one or more rule sets associated with the role ID or one or more service abstraction IDs included in authentication response packet 1520 .

	Richmond '067 at Fig. 2:  FIG. 2

	Richmond '067 at Fig. 15b:  FIG. 15B

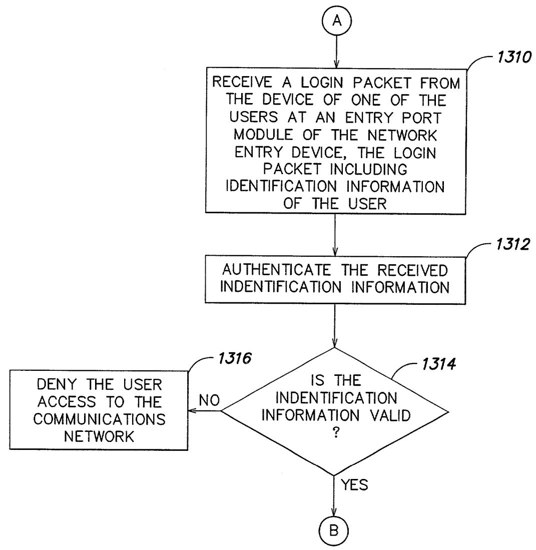
<table>
<tr>
<td></td>
<td>Richmond '067 at Fig. 13a2:


FIG. 13A(2)</td>
</tr>
<tr>
<td>[9] A method according to claim 8, wherein the user has not authenticated, further comprising:</td>
<td>Richmond discloses: A method according to claim 8, wherein the user has not authenticated. See, e.g.:

Richmond '067 at Abstract:
Controlling 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. A plurality of users may be connected to an entry point of a network of a network device by a shared transmission medium. Each users' usage of network resources is controlled, after such user has been authenticated, without using any network resources beyond such user's entry point to the network. For each one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. If a plurality of users are connected to an entry point by a shared transmission medium, packet rules associated with the users may be provisioned to the entry point and applied to packets</td>
</tr>
</table>

	received from the users before any network resources beyond the entry point are used. Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0209]: 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. Thus, a user cannot send any packets onto the network or receive any packets from the network until the user has successfully authenticated. Richmond '067 at [0210]: A port module of the network entry device may be configured with 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. For example, a network administrator may decide that all users should have access to some basic network services, such as access to the Internet or access to a word processing application, but not access to other network resources. Further, this state may be defined such that a port module that does not have an authenticated user attached thereto may be restricted such that all packets received at the port module and/or transmitted from the port module are assigned a lower priority, until a user is authenticated on the port module. Richmond '067 at [0220]: In a following Act 1312 , the received identification information may be authenticated. Any of a variety of authentication techniques may be used to authenticate the received identification information, for example, RADIUS, a NOS login, or 802.1X. Other types of authentication techniques may be used. For example, referring to FIG. 15, an authentication database 1508 may be searched using user information 1526 for a user authentication entry 1528 corresponding to the identification information received in the login packet. If such user authentication entry 1528 is not found, the identification information may be deemed invalid. If such entry 1528 is found, then entry information 1529 may be sent from the authentication database to the authentication module 1506 . If the identification information included in the entry information 1529 does not match the identification information of the login packet, the identification information of the login packet may be deemed invalid.

	Richmond '067 at [0222]: If in Act 1314 it is determined that the identification information is invalid (e.g., it does not match any entry of an authentication database), then in Act 1316 , the user may be denied access to the communications network. Whether or not the user is denied access may depend on the state defined for the entry port module in Act 1301 . Richmond '067 at [0274]: Authentication module 1506 may be configured to perform authentication in accordance with one or more authentication technologies, for example, RADIUS, a NOS, and IEEE 802.1X. The authentication module 1506 may be configured to access a user authentication entry 1528 of authentication database 1508 using user information 1526 , for example, using the user ID. If the authentication module 1506 cannot find an entry 1528 corresponding to the user information 1526 , then an authentication response packet 1520 sent from the authentication module to the authentication logic of port processing logic 1516 may indicate that the user is not a valid user of the network. Furthermore, the publication *Enterasys User Personalized Network*, incorporated into Richmond by reference (*see* Richmond at [0239]), provides further disclosure of this claim. Exemplary citations have been provided in Ex. C-4.
[9.1] redirecting the user to a login web page that requests user credentials; and	Richmond discloses: redirecting the user to a login web page that requests user credentials. *See, e.g.*: Richmond '067 at [0027]: One technique used to control usage of network resources is to apply user authentication to restrict access to network resources. Technologies that employ user authentication techniques include, among others, network operating systems (NOSs) (e.g., Netware by Novell and Windows NT), Remote Authentication Dial-In User Service (RADIUS) and IEEE 802.1X: Port Based Network Access Control , 2001. RADIUS is described in Request For Comments (RFC) 2138, entitled Remote Authentication Dial In User Service (RADIUS) by C. Rigney et al., promulgated by the Internet Engineering Task Force (IETF), published April, 1997, and available as of the date of this filing at: http://www.ietf.org/rfc/rfc2138.txt? number=2138., the entire contents of which are hereby incorporated by reference. IEEE 802.1X, the entire contents of which are hereby incorporated by reference, defines a standard for providing port-based network access control on a Media Access Control (MAC) bridge.

	Richmond '067 at [0028]: Typically, such authentication technologies require a user to initially log-in to a network, for example, by entering a username, password and possibly other credentials, before having access to information stored on the network. Logging in may include exchanging packets between a device of the user (e.g., user device 102 , 104 , 110 , 133 or 150) and one or more network devices (e.g., switching device 136 and authentication server 142), and these packets may be transmitted through a network device (e.g., 114 , 116 , 124 or 144) serving as the user's entry point in to the network. Richmond '067 at [0217]: In Act 1310 , a login packet may be received from a device of one of the users at an entry port module of the network entry device, the login packet including identification information of the user. The login packet may be received in response to the user's device sending a signaling packet to the network entry device and the network entry device requesting login information. Richmond '067 at [0220]: In a following Act 1312 , the received identification information may be authenticated. Any of a variety of authentication techniques may be used to authenticate the received identification information, for example, RADIUS, a NOS login, or 802.1X. Other types of authentication techniques may be used. For example, referring to FIG. 15, an authentication database 1508 may be searched using user information 1526 for a user authentication entry 1528 corresponding to the identification information received in the login packet. If such user authentication entry 1528 is not found, the identification information may be deemed invalid. If such entry 1528 is found, then entry information 1529 may be sent from the authentication database to the authentication module 1506 . If the identification information included in the entry information 1529 does not match the identification information of the login packet, the identification information of the login packet may be deemed invalid. Richmond '067 at [0288]: By leveraging the process of authenticating and authorizing users, which can be implemented using any number of known or later developed technologies, for example, RADIUS, 802.1X, NOS login, Smart cards, Kerberos and biometrics, the identity of a user may be determined, and network usage parameters may be dynamically provisioned to the user's entry point to the network, whether wired, or wireless or a combination thereof. This leveraging allows the authentication process, which historically has provided drive, file, and system level access, to be extended to the edge of the network, which may provide a significant increase in the security, resiliency, and scalability of the network.

	Furthermore, the publication *Enterasys User Personalized Network*, incorporated into Richmond by reference (*see* Richmond at [0239]), provides further disclosure of this limitation. Exemplary citations have been provided in Ex. C-4.
[9.2] using the user credentials received from the user to authenticate the user.	Richmond discloses: using the user credentials received from the user to authenticate the user. *See, e.g.*: Richmond '067 at [0028]: Typically, such authentication technologies require a user to initially log-in to a network, for example, by entering a username, password and possibly other credentials, before having access to information stored on the network. Logging in may include exchanging packets between a device of the user (e.g., user device 102 , 104 , 110 , 133 or 150) and one or more network devices (e.g., switching device 136 and authentication server 142), and these packets may be transmitted through a network device (e.g., 114 , 116 , 124 or 144) serving as the user's entry point in to the network. Richmond '067 at [0084]: In another aspect of this embodiment, the user information about the user is stored on a computer-readable medium residing on the communications network, and the user information includes identification information and the assigned role of the user. The stored user information is accessed to determine if the identification information included therein matches the identification information included in the received packet. If it is determined that the stored identification information matches the received identification information, the assigned role is determined from the stored user information. Richmond '067 at [0220]: In a following Act 1312 , the received identification information may be authenticated. Any of a variety of authentication techniques may be used to authenticate the received identification information, for example, RADIUS, a NOS login, or 802.1X. Other types of authentication techniques may be used. For example, referring to FIG. 15, an authentication database 1508 may be searched using user information 1526 for a user authentication entry 1528 corresponding to the identification information received in the login packet. If such user authentication entry 1528 is not found, the identification information may be deemed invalid. If such entry 1528 is found, then entry information 1529 may be sent from the authentication database to the authentication module 1506 . If the identification information included in the entry information 1529 does not match the identification information of the login packet, the identification information of the login packet may be deemed invalid.

	Richmond '067 at [0221]: If a user authentication entry 1528 corresponding to the identification information of the login packet is found and the identification information of this entry matches the identification information of the login packet, then the identification information may be deemed valid. Authentication is described in more detail below in relation to FIG. 15. Richmond '067 at [0273]: The authentication logic of port processing logic 1516 may be configured such that, if a packet 1502 is received and is a login packet including identification information of a user, the authentication logic controls the forwarding of an authentication request packet 1522 that includes the identification information from the port module 1510 through the port connecting medium 1511 and port module 1512 to authentication module 1506 . Such user information may include a user identifier (ID) (i.e., a user name), a password and other user credentials. In an embodiment, for example, when the authentication module 1506 resides on the network entry device 1504 , the authentication logic may be integrated as part of the authentication module 1506 . Further, the authentication logic may not be included as part of the port processing logic, but may be a separate and distinct component of network entry device 1504 . Richmond '067 at [0274]: Authentication module 1506 may be configured to perform authentication in accordance with one or more authentication technologies, for example, RADIUS, a NOS, and IEEE 802.1X. The authentication module 1506 may be configured to access a user authentication entry 1528 of authentication database 1508 using user information 1526 , for example, using the user ID. If the authentication module 1506 cannot find an entry 1528 corresponding to the user information 1526 , then an authentication response packet 1520 sent from the authentication module to the authentication logic of port processing logic 1516 may indicate that the user is not a valid user of the network. Richmond '067 at [0275]: The authentication module 1506 may be configured such that an entry 1528 is accessed using user information 1526 , and entry information 1529 is retrieved. Entry information 1529 may include credential information such as a password and other information, including a role identifier (ID) or one or more service abstraction IDs. The authentication module 1506 may be configured such that if the credential information of entry information 1529 does not match the credential information included in

	packet 1522 , then authentication response packet 1520 may include an indication that the identification information of the user is not valid. Richmond '067 at [0277]: The authentication module 1506 may be configured such that if the credential information of packet 1522 matches the credential information of entry information 1529 , then authentication response packet 1520 includes the role ID or one or more service abstraction IDs corresponding to the user. Such role ID or one or more service abstraction IDs may have been stored in the entry 1528 corresponding to the user and included in entry information 1529 or may have been stored in another location (e.g., another database) accessed by authentication module 1506 . Furthermore, the publication *Enterasys User Personalized Network*, incorporated into Richmond by reference (*see* Richmond at [0239]), provides further disclosure of this limitation. Exemplary citations have been provided in Ex. C-4.
[10] 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:	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. *See, e.g.*: Richmond '067 at [0047]: This embodiment and/or aspects thereof may be implemented as a computer program product that includes a computer-readable medium and computer-readable signals stored on the computer-readable medium, which signals define appropriate instructions. These instructions, as a result of being executed by a computer, instruct the computer to perform the acts described above for this illustrative embodiment. Richmond '067 at [0147]: Method 300 , acts thereof and various embodiments and variations of these methods and acts, individually or in combination, 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. Such computer program product may comprise computer-readable signals tangibly embodied on the computer-readable medium, where such signals 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 herein, and/or various embodiments, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBAL, etc., or any of a variety of combinations thereof. The computer-readable medium on which such instructions are stored may reside on one or more of the components of network 100 described above and/or system 400 described below, and may be distributed across one or more of such components. Richmond '067 at [0242]: Method 1300 , acts thereof and various embodiments and variations of these methods and acts, individually or in combination, 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. Such computer program product may comprise computer-readable signals tangibly embodied on the computer-readable medium, where such signals 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 herein, and/or various embodiments, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBAL, etc., or any of a variety of combinations thereof. The 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, and may be distributed across one or more of such components. Richmond '067 at [0260]: Method 1400 , acts thereof and various embodiments and variations of these methods and acts, individually or in combination, 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. Such computer program product may comprise computer-readable signals tangibly embodied on the computer-readable medium, where such signals 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 herein, and/or various embodiments, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual

	Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBAL, etc., or any of a variety of combinations thereof. The computer-readable medium on which such instructions are stored may reside on one or more of the components of network 100 described above and/or system 1500 described below, and may be distributed across one or more of such components.
[10.1] 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: 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* [1.1].
[10.2] processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;	Richmond discloses: processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage. *See* [1.2].
[10.3] 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, 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. *See* [1.3].
[10.4] at the user specific rule stage, accessing the user specific traffic control rules and user specific	Richmond discloses: 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

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.	governed by at least one user specific class of service rule associated with the user on the user device in the first network. *See* [1.4].
[11] The computer program product of claim 10, wherein the plurality of stages further comprises an interface specific stage and wherein the computer instructions are further translatable by the processor to perform: 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: The computer program product of claim 10, wherein the plurality of stages further comprises an interface specific stage and wherein the computer instructions are further translatable by the processor to perform: 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. *See* [2].
[12] The computer program product of claim 10, wherein the plurality of stages further comprises a global stage and wherein the computer instructions	Richmond discloses: The computer program product of claim 10, wherein the plurality of stages further comprises a global stage and wherein the computer instructions are further translatable by the processor to perform: at the global stage, applying global firewall rules to the packet. *See* [3].

are further translatable by the processor to perform: at the global stage, applying global firewall rules to the packet.	
[13] 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: 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. *See, e.g.*: Richmond '067 at [0010]: Controlling usage of network resources may include, but is not limited to: denying one or more packets access to any network resources beyond a network device (i.e., dropping the packet); regulating bandwidth on the network consumed by packets received from the user, for example, by assigning priorities to received packets or applying rate limiting to received packets; denying access to certain network resources, for example, by assigning a Virtual Local Area Network (VLAN) to the packet; and routing the packet. VLANs are described in more detail in IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks , Dec. 8, 1998, the entire contents of which are hereby incorporated by reference. Assigning a VLAN to a packet and/or assigning a priority to a packet, may be referred to herein as "classifying" a packet. As used herein, a "packet" is a unit of communication exchanged between devices. Richmond '067 at [0158]: Rate limit field 520 may store a value representing a rate limit to be applied to a packet if it satisfies the rule. Some rules may be defined such that if the condition of the rule is satisfied by a packet, then rate limiting will be applied to a packet. In such case, rate limit field 520 may specify a threshold value (e.g., 1 megabyte (MB)). This threshold value may specify a threshold volume of bytes that may be received during a specified temporal interval (e.g., one second) in packets that satisfy a particular rule. The temporal interval may be specified in field 520 itself or in another field.

	Richmond '067 at [0159]: For example, an entry of 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. Further, a network device may be configured to drop some or all of the bytes of a packet that contains an amount of packets that exceeds the threshold amount during the unit interval. Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume in sending packets to a particular network device specified by conditions 508 512 , or limit the amount of bandwidth that a user consumes on the network in sending packets corresponding to a particular application specified by conditions 508 512 . The consumption of bandwidth by a user also may be limited by the priority specified in field 516 . Richmond '067 at [0167]: Rate limit field 520 of entry 502 has a value of "none." Such value may specify that no rate limiting is to be applied to a received packet if the received packet satisfies the conditions specified in fields 508 512 of entry 502 . Richmond '067 at [0249]: In a following Act 1428 , it may be determined whether the packet rules dictate that rate limiting is to be applied to the received packet. An entry port module may be configured to apply one or more rate limiting techniques, known now or later developed. Rate limiting is described above in more detail in relation to rate limit field 520 of packet rule data structure 500 of FIG. 5. Richmond '067 at [0250]: If it is determined in Act 1428 that rate limiting is not to be applied to the received packet, then in Act 1432 , the configured packet may be forwarded to the appropriate destination. The appropriate destination may be determined from information already included in the received packet, information added or changed by application of the packet rules, or a combination thereof. Richmond '067 at [0251]: If it is determined in Act 1428 that the packet rules dictate that rate limiting be applied to the received packet, then in Act 1430 rate limiting may be applied to the received packet.

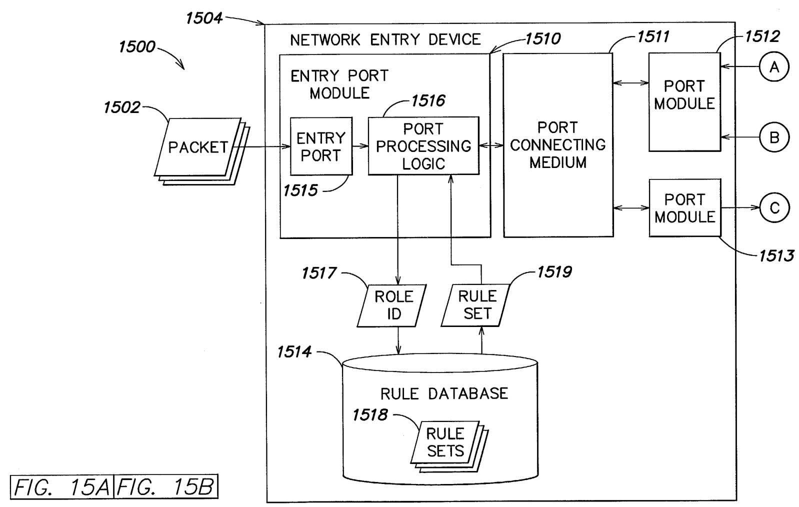
	Richmond '067 at [0257]: Thus, application of method 1400 to a received packet may result in a packet being configured based on user-based packet rules, default packet rules, and other additional rules with which the entry port module is configured. For example, the user-based packet rules may have assigned a VLAN to the received packet, the default packet rules may have assigned a priority to the received packet, and other rules may have applied rate limiting to the packet.
[14] The computer program product of claim 10, wherein the computer instructions are further translatable by the processor to establish the user specific traffic control rules and the user specific firewall rules 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: The computer program product of claim 10, wherein the computer instructions are further translatable by the processor to establish the user specific traffic control rules and the user specific firewall rules 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. *See* [7].
[15] The computer program product of claim 10, wherein the computer instructions are further translatable by the processor to determine whether the user has authenticated.	Richmond discloses: The computer program product of claim 10, wherein the computer instructions are further translatable by the processor to determine whether the user has authenticated. *See* [8].
[16] The computer program product of claim	Richmond discloses: The computer program product of claim 15, wherein the user has not authenticated and wherein the computer instructions are further translatable by the processor to perform.

15, wherein the user has not authenticated and wherein the computer instructions are further translatable by the processor to perform:	*See* [9] (preamble).
[16.1] redirecting the user to a login web page that requests user credentials; and	Richmond discloses: redirecting the user to a login web page that requests user credentials. *See* [9.1].
[16.2] using the user credentials received from the user to authenticate the user.	Richmond discloses: using the user credentials received from the user to authenticate the user. *See* [9.2].
[17] A control device for network access control, comprising:	Richmond discloses: A control device for network access control. *See, e.g.*: Richmond '067 at [0012]: Network 100 may include a plurality of devices of varying type, including any of network entry devices 114 , 116 , 120 , 124 and 144 , printer 122 , fax machine 123 , application server 134 , switching device 136 , device 138 and authentication server 142 . Switching device 136 may be configured as a core switching device that serves as a more centralized switching device for network 100 than the network entry devices. Richmond '067 at [0013]: A network entry device may include one or more port modules, and one or more of these port modules may be an entry port module. Richmond '067 at [0016]: As used herein, a "network entry device" is a network device that includes at least one entry port module. Thus, from the perspective of other devices, a network entry device serves as an entry point to

	the network for at least one user. A network entry device may reside at an edge or boundary of the communications network and provide connectivity between network resources of the communications network and devices located external to the communications network. Such network entry device may be any of a variety of types of devices, for example, a switching device. Richmond '067 at [0041]: In an embodiment of the invention, a network device of a communications network is used to control usage of network resources of the communications network by a plurality of users, where the network device serves as an entry point to the communications network for the plurality of users and includes a port module. The port module is connected by a transmission medium to a first user device used by a first of the plurality of users and located externally to the communications network. The port module also is connected by the transmission medium to a second user device used by a second of the plurality of users and located externally to the communications network. The port module is configured with one or more packet rules, where at least a first of the one or more packet rules is associated with the identity of the first user and at least one of the packet rules is associated with the identity of the second user. Richmond '067 at [0063]: In another embodiment, provided is a network device serving as an entry point to a communications network for a user and operative to control usage of network resources by the user beyond the network device. The network device includes a port module including port configuration logic to configure the port module with one or more packet rules corresponding to an identity of the user, a physical port to receive a packet from a device of the user and rule application logic to apply the one or more packet rules to the received packet before using any of the network resources beyond the network device. Richmond '067 at [0265]: Network entry device 1504 may include entry port module 1510 , port modules 1512 and 1513 , port connecting medium 1511 and rule database 1514 . Network entry device 1504 may be any of a plurality of types of switching devices, for example, one of the Matrix family of switches available from Enterasys Networks, Inc. Richmond '067 at [0269]: Entry port module 1510 may be connected to a single device of a user by a dedicated transmission medium or may be connected to multiple user devices by a shared transmission medium. Further, entry

	port module 1510 may be directly-coupled to one or more user devices and may be connected to one or more user devices through one or more switching devices and multiple transmission media. Richmond '067 at [0271]: Entry port 1515 is the physical component in which packets 1502 are received, and port processing logic 1516 processes packets received at entry port 1515 . Port processing logic 1516 may include several logic components (not shown), including: authentication logic to assist in authenticating a user, identification logic to determine the identity of a user device from which a packet is received, for example, as recited above in relation to Act 1401 of method 1400 , port configuration logic for configuring port module 1510 , for example, in accordance with the respective identities of one or more users, and rule application logic for applying one or more packet rules to a packet received at entry port 1515 .
[17.1] a processor;	Richmond discloses: a processor. *See, e.g.*: Richmond '067 at [0014]: As used herein, a "port module" of a switching device includes a physical port of the device and port processing logic associated with the physical port. Such port processing logic may include 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. Such port processing logic may be divided into one or more virtual ports, each virtual port corresponding to a communication channel of the physical port. The port processing logic may include separate switching logic, memory and processors for each virtual port or may share such components between one or more virtual ports. Further, the switching logic, memory and processors of a port module may be shared with several other port modules. A port module may be implemented as part of a port interface card (PIC), which may include one or more port modules. Richmond '067 at [0047]: This embodiment and/or aspects thereof may be implemented as a computer program product that includes a computer-readable medium and computer-readable signals stored on the computer-readable medium, which signals define appropriate instructions. These instructions, as a result of being executed by a computer, instruct the computer to perform the acts described above for this illustrative embodiment.

	Richmond '067 at [0147]: Method 300 , acts thereof and various embodiments and variations of these methods and acts, individually or in combination, 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. Such computer program product may comprise computer-readable signals tangibly embodied on the computer-readable medium, where such signals 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 herein, and/or various embodiments, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBAL, etc., or any of a variety of combinations thereof. The computer-readable medium on which such instructions are stored may reside on one or more of the components of network 100 described above and/or system 400 described below, and may be distributed across one or more of such components. Richmond '067 at [0198]: Further, on each of the one or more machines that include one or more components of system 400 , each of the components may reside in one or more locations on the machine. For example, different portions of the components 406 , 408 and 410 may reside in different areas of memory (e.g., RAM, ROM, disk, etc.) on the machine. Each of such one or more machines may include, among other components, a plurality of known components such as one or more processors, a memory system, a disk storage system, one or more network interfaces, and one or more busses or other internal communication links interconnecting the various components. Richmond '067 at [0270]: Entry port module 1510 may include an entry port 1515 and port processing logic 1516 . 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. Port processing logic 1516 may be divided into one or more virtual ports (not shown), each virtual port corresponding to a communication channel of the entry port 1515 (e.g., if entry port 1515 is connected to a shared wireless transmission medium). Port processing logic 1516 may include separate switching logic, memory and processors for each virtual port or may share such components between one or more

	virtual ports. Further, the switching logic, memory and processors of port processing logic 1516 may be shared with port processing logic of other port modules (e.g., 1512 and 1513). Richmond '067 at [0285]: Further, on each of the one or more machines that include one or more components of system 1500 , each of the components may reside in one or more locations on the machine. For example, different portions of the components 1510 , 1512 and 1513 may reside in different areas of memory (e.g., RAM, ROM, disk, etc.) on the machine. Each of such one or more machines may include, among other components, a plurality of known components such as one or more processors, a memory system, a disk storage system, one or more network interfaces, and one or more busses or other internal communication links interconnecting the various components. Richmond '067 at Fig. 15a:  FIG. 15A
[17.2] at least one computer-readable storage medium storing computer	Richmond discloses: at least one computer-readable storage medium storing computer instructions translatable by the processor to perform. *See* [10] (preamble).

instructions translatable by the processor to perform:	
[17.3] 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;	Richmond discloses: 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* [1.1].
[17.4] processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage;	Richmond discloses: processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage. *See* [1.2].
[17.5] 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, 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. *See* [1.3].
[17.6] at the user specific rule stage, accessing the user specific traffic control rules and user specific firewall rules based on the extracted information	Richmond discloses: 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.

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* [1.4].
[18] The control device of claim 17, wherein the plurality of stages further comprises an interface specific stage and wherein the computer instructions are further translatable by the processor to perform: 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: The control device of claim 17, wherein the plurality of stages further comprises an interface specific stage and wherein the computer instructions are further translatable by the processor to perform: 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. *See* [2].
[19] The control device of claim 17, wherein the plurality of stages further comprises a global stage and wherein the computer instructions are further translatable by the processor to perform: at the global stage, applying	Richmond discloses: The control device of claim 17, wherein the plurality of stages further comprises a global stage and wherein the computer instructions are further translatable by the processor to perform: at the global stage, applying global firewall rules to the packet. *See* [3].

global firewall rules to the packet.	
[20] The control device of claim 17, 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: The control device of claim 17, 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. *See* [13].
[21] 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: 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. *See, e.g.*: Richmond '067 at [0010]: Controlling usage of network resources may include, but is not limited to: denying one or more packets access to any network resources beyond a network device (i.e., dropping the packet); regulating bandwidth on the network consumed by packets received from the user, for example, by assigning priorities to received packets or applying rate limiting to received packets; denying access to certain network resources, for example, by assigning a Virtual Local Area Network (VLAN) to the packet; and routing the packet. VLANs are described in more detail in IEEE 802.1Q: IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks , Dec. 8, 1998, the entire contents of which are hereby incorporated by reference. Assigning a VLAN to a packet and/or assigning a priority to a packet, may be referred to herein as "classifying" a packet. As used herein, a "packet" is a unit of communication exchanged between devices.

	Richmond '067 at [0049]: In an aspect of this embodiment, the port module further comprises a physical port to receive a first packet from a user device and user identification logic to determine an identity of a user of the user device. The port module further comprises rule application logic to apply at least the first rule to the first packet, before using any of the network resources beyond the network device in response to processing packet, if the determined identity is the identity of the first user. Richmond '067 at [0158]: Rate limit field 520 may store a value representing a rate limit to be applied to a packet if it satisfies the rule. Some rules may be defined such that if the condition of the rule is satisfied by a packet, then rate limiting will be applied to a packet. In such case, rate limit field 520 may specify a threshold value (e.g., 1 megabyte (MB)). This threshold value may specify a threshold volume of bytes that may be received during a specified temporal interval (e.g., one second) in packets that satisfy a particular rule. The temporal interval may be specified in field 520 itself or in another field. Richmond '067 at [0159]: For example, an entry of 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. Further, a network device may be configured to drop some or all of the bytes of a packet that contains an amount of packets that exceeds the threshold amount during the unit interval. Such rate limiting technique may be used to limit the amount of bandwidth that a user may consume in sending packets to a particular network device specified by conditions 508 512 , or limit the amount of bandwidth that a user consumes on the network in sending packets corresponding to a particular application specified by conditions 508 512 . The consumption of bandwidth by a user also may be limited by the priority specified in field 516 . Richmond '067 at [0167]: Rate limit field 520 of entry 502 has a value of “none.” Such value may specify that no rate limiting is to be applied to a received packet if the received packet satisfies the conditions specified in fields 508 512 of entry 502 . Richmond '067 at [0249]: In a following Act 1428 , it may be determined whether the packet rules dictate that rate limiting is to be applied to the received packet. An entry port module may be configured to apply one or more rate

	limiting techniques, known now or later developed. Rate limiting is described above in more detail in relation to rate limit field 520 of packet rule data structure 500 of FIG. 5.
[22] 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: 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. *See, e.g.*: Richmond '067 at Abstract: Controlling 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. A plurality of users may be connected to an entry point of a network of a network device by a shared transmission medium. Each users' usage of network resources is controlled, after such user has been authenticated, without using any network resources beyond such user's entry point to the network. For each one or more users, packet rules may be provisioned to the user's entry point to the network, where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user before any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provisioned to the user's entry point in response to the user being authenticated. If a plurality of users are connected to an entry point by a shared transmission medium, packet rules associated with the users may be provisioned to the entry point and applied to packets received from the users before any network resources beyond the entry point are used. Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. An entry port module of a network entry device may be configured based on an identity of one or more users as a result of the authentication of the one or more users, respectively, and each packet received from each user may be examined to control usage of network resources by the user. Richmond '067 at [0035]: Use of a firewall (e.g., firewall 140) is another example of a technique for controlling usage of network resources by analyzing information included in packets and forwarding the received packets based on the information. A firewall resident on a device (e.g., device 138) of a private network (e.g., 100) may include one or more programs configured to analyze packets transmitted from a device of an authorized user (e.g., user device 102 or 133) of the private network, and to determine whether and/or how much usage of resources external to the private network is allowed for the authorized user. For example, the

	authorized user may attempt to access a web page by transmitting a packet destined for the Internet (e.g., Internet 148). The firewall may be configured to intercept such packets and determine whether to allow the packets to proceed on to the Internet, or apply some form of rate limiting to limit the amount of bandwidth the user can use in communicating with the web site. Richmond '067 at [0112]: Such packet rules may be provisioned to a number of network entry devices and may serve as a distributed firewall for users of a network, as opposed to a centralized firewall. 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, as opposed to applying the rules after the user has already consumed bandwidth and processing resources as is typical on a network with a more centralized firewall. Richmond '067 at [0123]: In an embodiment of the invention, usage of network resources by one or more users is controlled based on the identity of each user, respectively. For example, packet rules corresponding to the identity of each user may be applied to packets received from the user's device at an entry port module. Richmond '067 at [0194]: Returning to FIG. 4, the distribution module 408 may be configured to access one or more roles 430 from relationship database 410 and distribute one or more roles 432 to one or more devices of a network. For example, system 400 may reside on a user device, for example, one of the user devices of network 100 , and distribution module 408 may be configured to distribute the roles 432 to any of the devices described above in relation to FIG. 1. Roles 432 then may be used to configure a component of a network device, for example, a port module or a firewall, as described below in more detail. Richmond '067 at [0206]: FIGS. 13 A13 C comprise a flow chart illustrating an example of a method 1300 of configuring an entry port module of a network device based on the respective identities of one or more users to control usage of network resources by such users. Although methods 1300 and 1400 below are primarily directed to configuring an entry port module of a network device based on the respective identities of one more users, the invention is not limited as such, as other components of network devices, for example, a firewall resident on a network device, may be configured based on the respective identities of one or more users similar to as described below for port modules.

	Richmond '067 at [0230]: The packet received in Act 1322 may be from any device coupled to the entry port module. The entry port module may be connected to a plurality of user devices by a shared transmission medium. In an embodiment, if the entry port module is connected to multiple user devices, it may be desirable to configure the port module to drop any received packets that are not from a specific user's device until such user logs off of the port module. 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, which may have been stored for the entry port module as part of Act 1319 . Thus, if the port module is connected to a transmission medium dedicated to a user, the port module may use an address of the user's device (or other information specific to the user while the user is logged on) to filter out packets received from other users, for example, from addresses other than the one or more addresses recorded for the authenticated user, until the user logs off. Richmond '067 at [0244]: In Act 1401 , an identity of a user of the user device from which the packet was received is determined. For example, information from the received packet may be compared against a list of user identifiers maintained by the entry port module as a result of performing Act 1319 . For example, 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 from an authentication packet received from the user device of the user, and Act 1319 may be repeated for a plurality of users. Accordingly, Act 1401 may include 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. Richmond '067 at [0246]: In Act 1402 , the user-based packet rules are applied to the received packet. 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. 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. Richmond '067 at [0262]: Although system 1500 illustrates an entry port module 1510 of a network entry device 1504 configured to control usage of network resources by one or more users based on the respective identities of such

	users, other port modules of the network entry device (e.g., port modules 1512 and 1513) may be configured as such. Further other components of the network entry device 1504 or components (e.g., a firewall) of other devices of the network may be configured as such.
[23] The control device of claim 20, wherein the provisioning module further comprises an authentication module for authenticating the user.	Richmond discloses: The control device of claim 20, wherein the provisioning module further comprises an authentication module for authenticating the user. *See, e.g.*: Richmond '067 at [0086]: In yet another embodiment of the invention, provided is a system for controlling usage of network resources of a communications network by a user. The user has an assigned role with respect to the communications network, and the assigned role is associated with one or more packet rules, each packet rule including a condition and action to be taken if a packet received at a device satisfies the condition. The system includes a port module including a physical port to receive a packet including identification information of the user from a device of the user and port configuration logic to configure the port module with the one or more packet rules associated with the assigned role of the user, and an authentication module to determine the assigned role of the user based on the identification information. Richmond '067 at [0088]: In another aspect of this embodiment, user information about the user is stored on a computer-readable medium residing on the communications network, where the user information includes identification information and the assigned role of the user. The authentication module is operative to control accessing the stored user information to determine if the identification information included therein matches the identification information included in the received packet, and to determine the assigned role from the stored user information if it is determined that the stored identification information matches the received identification information. Richmond '067 at [0220]: In a following Act 1312 , the received identification information may be authenticated. Any of a variety of authentication techniques may be used to authenticate the received identification information, for example, RADIUS, a NOS login, or 802.1X. Other types of authentication techniques may be used. For example, referring to FIG. 15, an authentication database 1508 may be searched using user information 1526 for a user authentication entry 1528 corresponding to the identification information received in

	the login packet. If such user authentication entry 1528 is not found, the identification information may be deemed invalid. If such entry 1528 is found, then entry information 1529 may be sent from the authentication database to the authentication module 1506 . If the identification information included in the entry information 1529 does not match the identification information of the login packet, the identification information of the login packet may be deemed invalid. Richmond '067 at [0228]: In addition to or as an alternative to Acts 1318 and 1320 , one or more service abstractions corresponding to a user may be determined, and the entry port module may be configured with the packet rules associated with the one or more determined service abstractions. As described above in relation to distribution module 408 of FIG. 4, in addition to or as an alternative to distributing roles 432 to devices of a network, one or more relationship hierarchies and/or service abstractions also may be distributed. Thus, entries of authentication database 1508 or another database accessible by the authentication module 1506 may specify the one or more service abstractions assigned to a user, and this information may be used to determine the one or more service abstractions assigned to a user and to configure the entry port module with the packet rules associated with these one or more service abstractions, as similarly described in relation to Acts 1318 and 1320 with respect to the assigned role of a user. Richmond '067 at [0261]: FIG. 15 is a block diagram illustrating an example of a system 1500 for controlling usage of network resources by one or more users beyond such users' entry point to a communications network based on the respective identities of one or more users. The system 1500 may include a network entry device 1504 , a authentication module 1506 and an authentication database 1508 . Although authentication module 1506 and authentication database 1508 are shown as not being part of network entry device 1504 in FIG. 15, module 1506 or database 1508 or both may be part of network entry device 1504 . Richmond '067 at [0273]: The authentication logic of port processing logic 1516 may be configured such that, if a packet 1502 is received and is a login packet including identification information of a user, the authentication logic controls the forwarding of an authentication request packet 1522 that includes the identification information from the port module 1510 through the port connecting medium 1511 and port module 1512 to authentication module 1506 . Such user information may include a user identifier (ID) (i.e., a user name), a password and other user credentials. In an embodiment, for example, when the

	authentication module 1506 resides on the network entry device 1504 , the authentication logic may be integrated as part of the authentication module 1506 . Further, the authentication logic may not be included as part of the port processing logic, but may be a separate and distinct component of network entry device 1504 . Richmond '067 at [0274]: Authentication module 1506 may be configured to perform authentication in accordance with one or more authentication technologies, for example, RADIUS, a NOS, and IEEE 802.1X. The authentication module 1506 may be configured to access a user authentication entry 1528 of authentication database 1508 using user information 1526 , for example, using the user ID. If the authentication module 1506 cannot find an entry 1528 corresponding to the user information 1526 , then an authentication response packet 1520 sent from the authentication module to the authentication logic of port processing logic 1516 may indicate that the user is not a valid user of the network. Richmond '067 at [0275]: The authentication module 1506 may be configured such that an entry 1528 is accessed using user information 1526 , and entry information 1529 is retrieved. Entry information 1529 may include credential information such as a password and other information, including a role identifier (ID) or one or more service abstraction IDs. The authentication module 1506 may be configured such that if the credential information of entry information 1529 does not match the credential information included in packet 1522 , then authentication response packet 1520 may include an indication that the identification information of the user is not valid.
[24] The control device of claim 17, wherein the computer instructions are further translatable by the processor to establish the user specific traffic control rules and the user specific firewall rules for the user based on a user profile that includes parameters that determine an extent of the	Richmond discloses: The control device of claim 17, wherein the computer instructions are further translatable by the processor to establish the user specific traffic control rules and the user specific firewall rules 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. *See* [7].

user's access to the second network, services available to the user, or a combination thereof.	
[25] The control device of claim 17, wherein the computer instructions are further translatable by the processor to determine whether the user has authenticated.	Richmond discloses: The control device of claim 17, wherein the computer instructions are further translatable by the processor to determine whether the user has authenticated. *See* [8].
[26] The control device of claim 25, wherein the user has not authenticated and wherein the computer instructions are further translatable by the processor to perform:	Richmond discloses: The control device of claim 25, wherein the user has not authenticated and wherein the computer instructions are further translatable by the processor to perform. *See* [9] (preamble).
[26.1] redirecting the user to a login web page that requests user credentials; and	Richmond discloses: redirecting the user to a login web page that requests user credentials. *See* [9.1].
[26.2] using the user credentials received from the user to authenticate the user.	Richmond discloses: using the user credentials received from the user to authenticate the user. *See* [9.2].
[27] A control device for network access control, comprising:	Richmond discloses: A control device for network access control, comprising. *See* [17] (preamble).
[27.1] a processor;	Richmond discloses: a processor.

	See [17.1].
[27.2] at least one computer-readable storage medium storing computer instructions translatable by the processor to perform:	Richmond discloses: at least one computer-readable storage medium storing computer instructions translatable by the processor to perform. *See* [10] (preamble).
[27.3] 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;	Richmond discloses: 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* [1.1].
[27.4] determining whether the user has authenticated;	Richmond discloses: determining whether the user has authenticated. *See* [8].
[27.5] if the user has not authenticated:	Richmond discloses: if the user has not authenticated. *See* [9] (preamble).
[27.5.1] redirecting the user to a login web page that requests user credentials; and	Richmond discloses: redirecting the user to a login web page that requests user credentials. *See* [9.1].
[27.5.2] using the user credentials received from the user to authenticate the user;	Richmond discloses: using the user credentials received from the user to authenticate the user. *See* [9.2].
[27.6] processing the packet according to a	Richmond discloses: processing the packet according to a plurality of stages, including a client discrimination stage and a user specific rule stage.

plurality of stages, including a client discrimination stage and a user specific rule stage;	*See* [1.2].
[27.7] 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, 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. *See* [1.3].
[27.8] 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, 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* [1.4].