(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 August 2006 (03.08.2006)

PCT

(10) International Publication Number
WO 2006/081237 A2

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 17/30* (2006.01)
G06K 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/002466

(22) International Filing Date: 25 January 2006 (25.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/647,692 26 January 2005 (26.01.2005) US
60/750,643 14 December 2005 (14.12.2005) US

(71) Applicant *(for all designated States except US)*: **LOCKDOWN NETWORKS, INC.** [US/US]; 100 West Harrison, North Tower, Suite 300, Seattle, Washington 98119 (US).

(72) Inventors; and

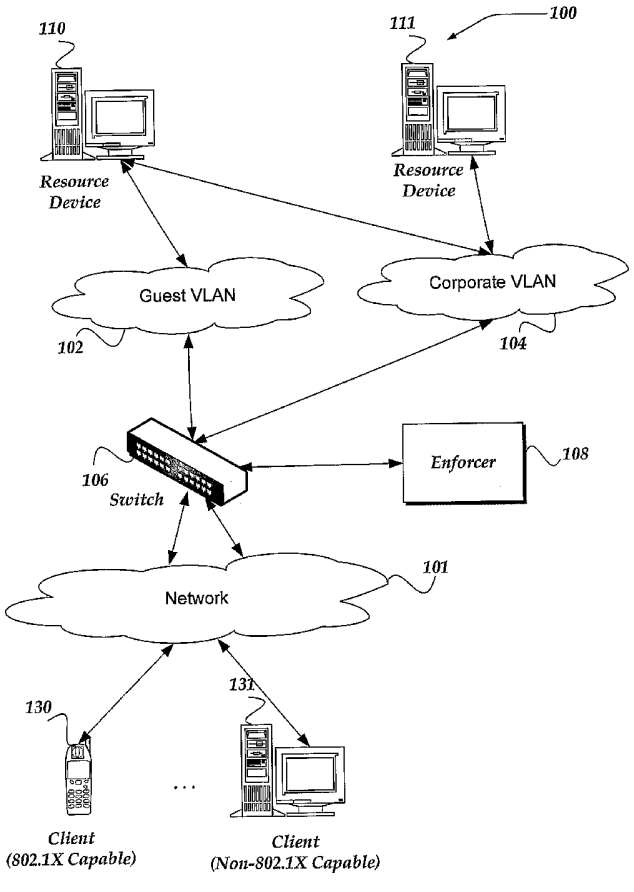
(75) Inventors/Applicants *(for US only)*: **VANK, Alexandru, Zsolt** [CA/US]; 14533 NE 43rd Place, Apt. N1212, Bellevue, Washington 98007 (US). **SHEN, Xin** [US/US]; 7719 Ridgecrest Lane, Mercer Island, Washington 98040 (US). **COBB, Matt, Brian** [US/US]; 26021 NE 27th Drive, Redmond, Washington 98053-9803 (US). **ROBEL-FORREST, Brad** [US/US]; 7149 Moon Valley Rd. SE, North Bend, Washington 98045 (US). **WEBB, Evan, McClendon** [US/US]; 1700 N. Northlake Way #206, Seattle, Washington 98103 (US).

(74) Agents: **BRANCH, John, W.** et al.; Darby & Darby P.C., P.O. Box 5257, New York, New York 10150-5257 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI,

[Continued on next page]

(54) Title: ENABLING DYNAMIC AUTHENTICATION WITH DIFFERENT PROTOCOLS ON THE SAME PORT FOR A SWITCH



(57) Abstract: The invention enables a client device that does not support IEEE 802. IX authentication to access at least some resources provided through a switch that supports 802. IX authentication by using dynamic authentication with different protocols. When the client device attempts to join a network, the switch monitors for an 802. IX authentication message from the client device. In one embodiment, if the client fails to send an 802. IX authentication message, respond to an 802. IX request from the switch, or a predefined failure condition is detected the client may be deemed incapable of supporting 802. IX authentication. In one embodiment, the client may be initially placed on a quarantine VLAN after determination that the client fails to perform an 802. IX authentication within a backoff time limit. However, the client may still gain access to resources based on various non-802. IX authentication mechanisms, including name/passwords, digital certificates, or the like.

WO 2006/081237 A2

NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ENABLING DYNAMIC AUTHENTICATION WITH DIFFERENT PROTOCOLS ON THE SAME PORT FOR A SWITCH

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application Serial No. 60/647,692 filed on January 26, 2005, entitled "Enabling Dynamic Authentication With Different Protocols On The Same Port For A Switch," and of U.S. Provisional Application Serial No. 60/750,643 filed on December 14, 2005, entitled "Enabling Dynamic Authentication With Different Protocols On The Same Port For A Switch," the benefit of the earlier filing dates of which is hereby claimed under 35 U.S.C. § 119 (e) and each being further incorporated by reference.

FIELD OF THE INVENTION

The present invention relates to network security, and in particular, but not exclusively, to enabling enforcement of access control on a network.

BACKGROUND OF THE INVENTION

Businesses are deriving tremendous financial benefits from using the internet to strengthen relationships and improve connectivity with customers, suppliers, partners, and employees. Progressive organizations are integrating critical information systems including customer service, financial, distribution, and procurement from their private networks with the Internet. The business benefits are significant, but not without risk. Unfortunately, the risks are growing.

In response to the growing business risks of attacks, potentials for legal suits, federal compliance requirements, and so forth, companies have spent millions to protect the digital assets supporting their critical information systems. In particular, many companies have recognized that the first security barrier to their business's information systems is their access control system.

Access control pertains to an infrastructure that is directed towards enforcing access rights for network resources. Access control may grant or deny permission to a given device user, device or node, for accessing a resource and may protect resources by limiting access to only authenticated and authorized users and/or devices.

Most of today's switches have an IEEE 802.1X port authenticator built in to the switch. This allows for 802.1X authentication on any of its ports, but it also has the requirement that every client has to support the 802.1X protocol. However, for clients that do not support the 802.1X protocol, they cannot gain access to any of the resources provided by the switch. Therefore, it is with respect this and other considerations, that the present invention has been made.

BRIEF DESCRIPTION OF THE DRAWINGS

Non-limiting and non-exhaustive embodiments of the present invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

For a better understanding of the present invention, reference will be made to the following Detailed Description of the Preferred Embodiment, which is to be read in association with the accompanying drawings, wherein:

FIGURE 1 illustrates one embodiment of system for enabling dynamic authentication with different protocols on the same port for a switch;

FIGURE 2 illustrates one embodiment of a network appliance that may be included in a system implementing the invention;

FIGURE 3 shows one embodiment of a client device in accordance with the present invention;

FIGURE 4 illustrates a logical flow diagram generally showing one embodiment of a process for enabling dynamic authentication with different protocols using a backoff timer; and

FIGURE 5 illustrates a logical flow diagram generally showing one embodiment of a process for enabling dynamic authentication with different protocols on the same port for a switch independent of a backoff timer, in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific exemplary embodiments by which the invention may be practiced. This invention may, however, be embodied in many different forms and

should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Among other things, the present invention may be embodied as methods or devices. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

Throughout the specification and claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise. The phrase "in one embodiment" as used herein does not necessarily refer to the same embodiment, though it may. As used herein, the term "or" is an inclusive "or" operator, and is equivalent to the term "and/or," unless the context clearly dictates otherwise. The term "based on" is not exclusive and allows for being based on additional factors not described, unless the context clearly dictates otherwise. In addition, throughout the specification, the meaning of "a," "an," and "the" include plural references. The meaning of "in" includes "in" and "on."

As used herein, the term node, including virtually any computing device that is capable of connecting to a network. Such devices include, but are not limited to, personal computers, mobile devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, servers, network appliances, and the like.

The IEEE 802.1X authentication standard uses an existing protocol, Extensible Authentication Protocol (EAP), for message exchange during an authentication process. Thus, 802.1X may employ a variety of EAP authentication mechanisms, including, but not limited to MD5, Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Lightweight EAP (LEAP), PEAP, or the like. 802.1X is configured to work over Ethernet, Token rings, and other wired, as well as wireless networks. Typically, in a wireless network with 802.1X, a client device requests access to a resource through an 802.1X enabled switch, access point, or the like, sometimes called an authenticator. The client device may then provide an EAP message to the switch. In one embodiment, the message may be an EAP start message. In turn, the switch may provide an EAP message

to the client device requesting its identity. When the client provides its identity, the switch may repackage the identity and forward it to an authentication server. The authentication server may then authenticate the client device, and return an accept or reject message to the switch. In one embodiment, the authentication server may employ a Remote Authentication Dial-In User Service (RADIUS), however, the invention is not so limited, and virtually any authentication service may be employed, including an X.509 Certification Authority server, or the like. As used throughout this application, including the claims, 802.1X refers to the IEEE 802.1X protocol and all authentication protocols derived therefrom.

Briefly stated, the present invention is directed towards an apparatus, system, and method for enabling a client that does not support IEEE 802.1X authentication to still gain access to at least some resources provided through a switch that supports 802.1X authentication. The invention enables such access to at least some resources by using dynamic authentication with different protocols on the same port for the switch. In one embodiment, the switch port may begin in a mode that enables 802.1X authentication. When a client attempts to join a network to access the resources, the switch may monitor for an 802.1X authentication message from the client. In one embodiment, the message may be an 802.1X start message, or the like. In one embodiment, the switch may select to send an 802.1X authentication message to the client in the form of a request for the client's identity. In another embodiment, other predefined failure conditions may also be monitored for, including an incorrect authentication credential associated with the client, an improperly configured supplicant (e.g., client accessing the port), inoperable switch, or the like.

In any event, if the client fails to send an 802.1X authentication message, to respond to the 802.1X request for the client's identity, or a predefined failure condition is detected the client may be deemed incapable of supporting 802.1X authentication. In one embodiment, the client may be initially placed on a Virtual Local Area Network (VLAN) that is arranged to quarantine the client when the client requests access to the network. In another embodiment, the client may be placed on the quarantine VLAN after a determination that the client fails to perform an 802.1X authentication within a backoff time limit. In one embodiment, network traffic to and/or from the client is redirected through the switch towards a network device arranged to manage and/or filter the client's

network traffic. Although the client may be deemed incapable of supporting 802.1X authentication, the client may still gain access to at least some resources provided through the switch based on use of a non-802.1X authentication mechanism. Such non-802.1X authentication mechanisms include, but are not limited to name/passwords, digital certificates, or the like. In one embodiment, the network device, or another device, may present the quarantined client with an interface, or the like, that enables the client to employ a non-802.1X authentication mechanism. In one embodiment, the interface may include a web page, Command Line Interface (CLI), or the like.

Illustrative Operating Environment

FIGURE 1 illustrates one embodiment of system for enabling dynamic authentication with different protocols on the same port for a switch. As shown in the figure, system 100 includes switch 106, enforcer 108, resource devices 110-111, client devices 130-131 network 101, and Virtual Local Area Networks (VLANs) that are segmented into at least guest VLAN 102 and corporate VLAN 104.

Client devices 130-131 are in communication through network 101 to a switch port on switch 106. Switch 106 is in communication with guest VLAN 102 and corporate VLAN 104. Enforcer 108 is in communication with switch 106. Resource device 110 is in communication with guest VLAN 102 and corporate VLAN 104. Resource device 111 is in communication with corporate VLAN 104.

One embodiment of client devices 130-131 is described in more detail below in conjunction with FIGURE 3. Generally, however, client devices 130-131 may include virtually any computing device capable of connecting to another computing device and receiving information. Such devices may also include portable devices such as, cellular telephones, smart phones, display pagers, radio frequency (RF) devices, infrared (IR) devices, Personal Digital Assistants (PDAs), handheld computers, wearable computers, tablet computers, integrated devices combining one or more of the preceding devices, and the like. Client devices 130-131 may also include other computing devices, such as personal computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network devices, and the like. As such, client devices 130-131 may range widely in terms of capabilities and features. For example, a client device

configured as a cell phone may have a numeric keypad and a few lines of monochrome LCD display on which only text may be displayed.

In another example, a web-enabled client device may have a touch sensitive screen, a stylus, and several lines of color LCD display in which both text and graphics may be displayed. Moreover, the web-enabled client device may include a browser application enabled to receive and to send wireless application protocol messages (WAP), and/or wired application messages, and the like. In one embodiment, the browser application is enabled to employ HyperText Markup Language (HTML), Dynamic HTML, Handheld Device Markup Language (HDML), Wireless Markup Language (WML), WMLScript, JavaScript, EXtensible HTML (xHTML), Compact HTML (CHTML), and the like, to display and send a message.

Moreover, some client devices may be configured to support 802.1X authentication mechanisms, while other client device may be not be so configured. As shown in the figure, client device 130 represents one embodiment of a client device that is capable of 802.1X authentication, while client device 131 represents one embodiment of a client device that is incapable of 802.1X authentication. However, client device 131 may be configured to employ a variety of other authentication mechanisms, including, but not limited to user name/passwords, digital certificates, tokens, browser based authentication, windows based authentication, Kerberos, one-time passwords, public key authentication, biometrics, or the like.

Client devices 130-131 also may include at least one client application that is configured to receive content from another computing device. The client application may include a capability to provide and receive textual content, graphical content, audio content, alerts, messages, and the like. Moreover, client devices 130-131 may be further configured to communicate a message, such as through a Short Message Service (SMS), Multimedia Message Service (MMS), instant messaging (IM), internet relay chat (IRC), mIRC, Jabber, and the like, between another computing device, and the like.

In one embodiment, client devices 130-131 may be configured such that an end-user may operate the computing device to make requests for data and/or services from other computers on the network. In one embodiment, client devices 130-131 may employ a network interface unit (sometimes called a transceiver), such as described

below, to communicate information with another computing device. In one embodiment, the requested data resides in computing devices such as resource devices 110-111. In this specification, the term "client" refers to a computer's general role as a requester of data or services, and the term "server" refers to a computer's role as a provider of data or services. In general, it is possible that a computer can act as a client, requesting data or services in one transaction and act as a server, providing data or services in another transaction, thus changing its role from client to server or vice versa. In one embodiment, client devices 130-131 are a computing device that is not operated by an end-user.

Network 101, guest VLAN 102, and corporate VLAN 104 are configured to couple one computing device with another computing device. Guest VLAN 102 and corporate VLAN 104 represent particular types of networking structures; however, all three may be described generically to employ any form of computer readable media for communicating data from one electronic device to another. Generally, such networks can include the Internet in addition to local area networks (LANs), wide area networks (WANs), direct connections, such as through a universal serial bus (USB) port, other forms of computer-readable media, or any combination thereof. On an interconnected set of LANs, including those based on differing architectures and protocols, a router acts as a link between LANs, enabling messages to be sent from one to another.

Also, communication links within LANs can include, for example, twisted wire pair or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links including satellite links, or other communications links known to those skilled in the art. Furthermore, remote computers and other related electronic devices can be remotely connected to either LANs or WANs via a modem and temporary telephone link.

Such networks may further employ a plurality of access technologies including 2nd (2G), 3rd (3G) generation radio access for cellular systems, WLAN, Wireless Router (WR) mesh, and the like. Access technologies such as 2G, 3G, and future access networks may enable wide area coverage for mobile devices, such as a mobile device with various degrees of mobility. For example, such networks may enable a radio

connection through a radio network access such as Global System for Mobil communication (GSM), General Packet Radio Services (GPRS), Enhanced Data GSM Environment (EDGE), Wideband Code Division Multiple Access (WCDMA), and the like. In essence, such networks may include virtually any wireless and/or wired communication mechanism by which data may travel between one computing device and another computing device.

The media used to transmit data in communication links as described above illustrates one type of computer-readable media, namely communication media. Generally, computer-readable media includes any media that can be accessed by a computing device. Computer-readable media may include computer storage media, communication media, or any combination thereof.

Additionally, communication media typically embodies computer-readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any data delivery media. The terms "modulated data signal," and "carrier-wave signal" includes a signal that has one or more of its characteristics set or changed in such a manner as to encode data, instructions, data, and the like, in the signal. By way of example, communication media includes wired media such as twisted pair, coaxial cable, fiber optics, wave guides, and other wired media and wireless media such as acoustic, RF, infrared, and other wireless media.

Shown are two VLANs (guest VLAN 102 and corporate VLAN 104). However, the invention is not so limited and can be employed with a plurality of segmented VLANs. As shown, guest VLAN 102 may represent a particular network configuration that may be managed through a network device. In one embodiment, the network device is arranged to effectively filter network traffic from and/or to devices on guest VLAN 102 and to restrict access to particular resources by such clients. Corporate VLAN 104 may represent a particular network configuration such as an intranet for a corporation, or the like. The two networks may differ in a level of computing access security enforcement. For example, devices placed onto guest VLAN 102 may be more restricted in what resources may be accessed, what network traffic may flow beyond guest VLAN 102, or the like, than a device placed on corporate VLAN 104. In one embodiment, for example,

virtually all network traffic from and/or to a device on guest VLAN 102 may filtered through the network device to effectively quarantine a device from virtually every other device

One embodiment of enforcer 108 is described in more detail below in conjunction with FIGURE 2. Briefly, however, enforcer 108 includes virtually any network device that is configured to manage and enforce a networking security policy. Enforcer 108 is configured to listen for authentication requests on the ports of switch 106. Enforcer 108 and switch 106 may authenticate client devices 130-131 through a variety of mechanisms including an 802.1X authentication, or non-802.1X authentication protocols. In one embodiment, in a non-802.1X authentication mode, enforcer 108 may not act as an authentication server or an authentication proxy for the 802.1X authentication. However, in another embodiment, in non-802.1X authentication mode, enforcer 108 may provide an interface such as a web page, CLI screen, or the like, for use in authentication. In one embodiment, enforcer 108 may employ inputs provided by the client device to perform authentication, or forward the inputs to another device (not shown) for authentication.

Enforcer 108 may conduct an audit of various network devices on-schedule or on-demand to ensure conformance with various security policies. Enforcer 108 may be configured to ensure the right users are on the network segments, and that devices comply with the security policy to minimize exposure to unauthorized access, exploits, and/or attacks.

Enforcer 108 may be configured to manage access in part by remotely managing switch 106 using various mechanisms, including SNMP, SSH, Telnet, or the like. Enforcer 108 may enable the configuration of switch 106 to be changed on the fly. Enforcer 108 can also receive Layer 2 (OSI Reference Model) broadcasts from clients through switch 106. In one embodiment, this attribute can be useful if EAP over LAN (EAPOL) frames from the clients are sent to the 01:80:C2:00:00:03 broadcast group. Additionally, in one embodiment, enforcer 108 can operate as an authentication server or a proxy authenticator for the client that is authenticating via 802.1X. For example, enforcer 108 may process EAP-success and EAP-reject packets. In one embodiment, enforcer 108 may also provide authentication information to another device (not shown), for authentication.

In one embodiment, enforcer 108 is a network appliance. It is important to note, however, that while enforcer 108 can be configured as a network appliance, the invention is not so limited, and the invention may employ virtually any implementation, including a server, or the like. Thus, enforcer 108 may be implemented using one or more personal computers, servers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, radio frequency (RF) devices, infrared (IR) devices, integrated devices combining one or more of the preceding devices, or the like. Moreover, enforcer 108 may communicate with other devices using a variety of networking communication protocols, including wireless and/or wired protocols and related mechanisms. In one embodiment, enforcer 108 may employ a secure channel over which communications may travel.

In networks, a switch may filter and forward packets between LAN segments. Switches typically operate at a data link layer (layer 2) and sometimes a network layer (layer 3) of the OSI Reference Model and therefore typically support any packet protocol. LANs that use switches to join segments are called switched LANs. Typically, packet protocols such as TCP/IP and UDP/IP are employed at layer 3 of the OSI Reference Model for processing packets. Switches can also support secure protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), or the like. Switch 106 is one embodiment of a switch.

Switch 106 may receive network packets from one computing device on one network segment and route the network packets over another network segment to another computing device. Switch 106 may employ a variety of network ports to manage various network packets.

Switch 106 may enable client devices 130-131 access to guest VLAN 102 and/or corporate VLAN 104 based in part on directions from enforcer 108. Guest VLAN 102 may provide access to resource device 110. Corporate VLAN 104 may provide access to resource devices 110-111. In general corporate VLAN 104 may grant access to more or different resources than accessible by guest VLAN 102.

In one embodiment, switch 106 is capable of supporting IEEE 802.1X authentication. For example, switch 106 may be enabled to be an access point capable of processing EAP-start packets, EAP-request identity packets, EAP-response packets, EAP-

success packets, EAP-reject packets, or the like. Also, switch 106 may be configured to support VLANs including, but not limited to port based VLANs, subnet based VLANs, protocol based VLANs, and Media Access Control (MAC) Layer based VLANs. Additionally, a port on switch 106 can be placed in at least one of two modes, including auto and authorized.

In the auto mode, IEEE 802.1X authentication is enabled on a port of switch 106. Also, in one embodiment, the port may start in the unauthorized mode where no packets are passed through the port until an 802.1X authentication has been completed.

In the authorized mode, IEEE 802.1X authentication may be disabled on a port of switch 106. Also, the port may start in the authorized mode. For the authorized mode, any packets including 802.1X packets may be treated as regular network packets and are forwarded through switch 106.

Moreover, enforcer 108 may have access to guest VLAN 102 with no router disposed between it, and switch 106. In this way, enforcer 108 can see 802.1X packets coming from a client when a switch port on switch 106 is in the authorized mode.

Although, switch 106 is illustrated (and referred to) as a switch, the invention is not so limited, and other devices may be employed instead of a switch, including, but not limited to a router, bridge, gateway, network appliance, access point, server, or the like.

Resource devices 110-111 may include any computing device capable of communicating packets to provide a response to a request for data and/or services. Each packet may convey a piece of information. A packet may be sent for handshaking, e.g., to establish a connection or to acknowledge receipt of data. The packet may include information such as a request, a response, or the like. Generally, packets received by resource devices 110-111 will be formatted according to TCP/IP, but they could also be formatted using another transport protocol, such as User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), NETbeui, IPX/SPX, token ring, and the like. Moreover, the packets may be communicated between resource devices 110-111 employing HTTP, HTTPS,or the like.

In one embodiment, resource devices 110-111 are configured to operate as a website server. However, resource devices 110-111 are not limited to web servers, and may also operate a messaging server, a File Transfer Protocol (FTP) server, a database server, content server, LDAP servers, printing services, or the like.

Additionally, each of resource devices 110-111 may be configured to perform a different operation. Thus, for example, resource device 110 may be configured as a messaging server, while server 110 is configured as a database server. In one embodiment, resource device 110 may provide a more restricted set of resources, a reduced subset of resources, or the like, from resource device 111. Resource device 110 may be a more limited resource, such as a web page enabled to provide a non-802.1X authentication mechanism, information about why 802.1X authentication for a client has been denied, remediation information, and the like. Moreover, while resource devices 110-111 may operate as other than a website, they may still be enabled to receive an HTTP communication.

Illustrative Network Appliance As An Enforcer

FIGURE 2 illustrates one embodiment of a network appliance that may be included in a system implementing the invention, in accordance with the present invention. The network appliance may include many more components than those shown. The components shown, however, are sufficient to disclose an illustrative embodiment for practicing the invention. In addition, although the invention illustrates use of a network appliance, the invention is not so constrained, and virtually any network computing device may be employed, including a server, and the like. Network appliance 200 may be employed, in one embodiment, as enforcer 108 of FIGURE 1.

Network appliance 200 includes processing unit 212, and a mass memory, all in communication with each other via bus 222. The mass memory generally includes RAM 216, ROM 232, and one or more permanent mass storage devices, such as hard disk drive 228, tape drive, optical drive, and/or floppy disk drive. The mass memory stores operating system 220 for controlling the operation of network appliance 200. Any general-purpose operating system may be employed. Basic input/output system ("BIOS") 218 is also provided for controlling the low-level operation of network appliance 200. As illustrated in FIGURE 2, network appliance 200 also can communicate with the Internet,

or some other communications network, via network interface unit 210, which is constructed for use with various communication protocols including the TCP/IP protocol. Network interface unit 210 is sometimes known as a transceiver, transceiving device, network interface card (NIC), and the like.

Network appliance 200 may also include an SMTP handler application for transmitting and receiving email. Network appliance 200 may also include an HTTP handler application for receiving and handing HTTP requests, and an HTTPS handler application for handling secure connections. The HTTPS handler application may initiate communication with an external application in a secure fashion.

Network appliance 200 also includes input/output interface 224 for communicating with external devices, such as a mouse, keyboard, scanner, or other input devices not shown in FIGURE 2. Likewise, network appliance 200 may further include additional mass storage facilities such as hard disk drive 228. Hard disk drive 228 is utilized by network appliance 200 to store, among other things, application programs, databases, and the like.

The mass memory as described above illustrates another type of computer-readable media, namely computer storage media. Computer storage media may include volatile, nonvolatile, removable, and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules, or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computing device.

The mass memory also stores program code and data. One or more applications 250 are loaded into mass memory and run on operating system 220. Examples of application programs include email programs, schedulers, calendars, web services, transcoders, database programs, word processing programs, spreadsheet programs, and so forth. Applications 250 may further include an SNMP client, an SNMP trap sink, an 802.1X authentication server application, a Virtual Local Area Network

(VLAN) Assignment Protocol (VLAP) peer application, a proxy web server, and a directory service. However, the invention is not limited to these applications, and others may be implemented, without departing from the scope of spirit of the invention. Additionally, Enforcer Manager 252 enables at least a portion of the actions discussed below in conjunction with FIGURES 4.

Illustrative Client Device

FIGURE 3 shows one embodiment of a client device that may operate as a client device, such as client devices 130-131 of FIGURE 1. In one embodiment, client device 300 is a mobile phone that is arranged to send and receive voice communications, text-based messages, multimedia data, and other data by way of one or more wireless communication interfaces. Generally, client device 300 may include any electronic device capable of such wireless communication, including, but not limited to, any personal electronic device. Client devices are typically capable of communication by connecting to one or more wireless networks, connecting to multiple nodes of a single wireless network, communicating over one or more channels to one or more networks, or otherwise engaging in one or more communication sessions. Such devices include mobile phones, cellular phones, smart phones, pagers, RF devices, IR devices, integrated devices combining one or more of the preceding devices, and the like. Client device 300 may also include other electronic devices such as personal digital assistants, handheld computers, personal computers, microprocessor-based or programmable consumer electronic devices, wearable computers, and the like.

Client device 300 may include many more components than those shown in FIGURE 3, and need not include all of the components shown therein. However, the components shown are sufficient to disclose an illustrative embodiment for practicing the present invention. As shown in the figure, client device 300 includes CPU 352 in communication with memory 360 by way of bus 354.

Client device 300 also includes power supply 356, one or more wireless interfaces 380, audio interface 382, display 384, keypad 386, illuminator 388, input/output interface 390, and haptic interface 392. Power supply 356 provides power to client device 300. A rechargeable or non-rechargeable battery may be used to provide

power. The power may also be provided by an external power source, such as an AC adapter or a powered docking cradle that supplements and/or recharges a battery.

Client device 300 may optionally communicate with a base station (not shown), or directly with another wireless mobile or non-mobile device. Input/output interface 390 includes circuitry for coupling client device 300 to one or more wireless networks, and is constructed for use with one or more communication protocols and technologies including, but not limited to, GSM, CDMA, TDMA, EDGE, UMTS, WCDMA, CDMA 2000, UDP, TCP/IP, SMS, GPRS, WAP, UWB, WiMax, IEEE 802.11x, and the like. Audio interface 382 is arranged to produce and receive audio signals, such as the sound of a human voice. For example, audio interface 382 may be coupled to a speaker and microphone (not shown) to enable telecommunication with others and/or to generate an audio acknowledgement for some action. Display 384 may be a liquid crystal display, gas plasma, light emitting diode, or any other type of display used with a client device or other wireless device. Display 384 may also include a touch sensitive screen arranged to receive input from an object such as a stylus or a human digit.

Keypad 386 may include any input device arranged to receive input from a user. For example, keypad 386 may include a push button numeric dial or an alphanumeric keyboard. Keypad 386 may also include command buttons that are associated with selecting and sending images. Illuminator 388 may provide a status indication and/or provide light. Illuminator 388 may remain active for specific periods of time or in response to events. For example, if illuminator 388 is active, it may backlight the buttons on keypad 386 and remain active while client device 300 is powered. Also, illuminator 388 may backlight these buttons in various patterns if particular actions are performed, such as dialing another client device. Illuminator 388 may also cause light sources positioned within a transparent or translucent case of client device 300 to illuminate in response to actions.

Client device 300 also includes input/output interface 390 for communicating with external devices. Input/output interface 390 may employ one or more appropriate communication technologies, such as USB, IR, Bluetooth, and the like. Haptic interface 392 is arranged to provide tactile feedback to a user of client device 300. For example,

haptic interface 392 may be employed to vibrate client device 300 in a particular way when a user of another device, such as a mobile phone, is calling client device 300.

Memory 360 may include RAM 362, ROM 364, and other storage means. Memory 360 also provides data storage 372 and storage of programs, including, for example, operating system 371, client program 374, 802.1X authentication manager 376, and non-802.1X authentication manager 377, and other applications 378. Such programs may include processor-executable instructions which, when executed on client device 300, cause transmission, reception, and other processing of audio data, video data, text messaging data, web pages, Wireless Markup Language (WML) pages, and the like, and enable wireless communication with another device.

In one embodiment, the client device may include 802.1X authentication manager 376, and/or non-802.1X authentication manager 377. 802.1X authentication manager 376 may authenticate a client device through the 802.1X protocol. Non-802.1X authentication manager 377 may authenticate the client device through another authentication mechanism, as described above.

Generalized Operations

The operation of certain aspects of the invention will now be described with respect to FIGURES 4-5. FIGURE 4 illustrates a logical flow diagram generally showing one embodiment of a process for enabling dynamic authentication with different protocols using a backoff timer. FIGURE 4 may be enabled by enforcer 108 and switch 106 of FIGURE 1.

As shown in the figure, process 400 begins, after a start block, at block 402, where a switch and an authentication server are enabled to employ 802.1X authentication. In one embodiment, the enforcer may act as the authentication server. In one embodiment, the enforcer puts a switch port on the switch into an auto mode, thus enabling 802.1X authentication detection. In one embodiment, 802.1X packets may be processed on the switch port, while other packets may be dropped, or otherwise ignored by the switch.

Processing then continues to block 404, where the switch and/or the enforcer detect a client's request to join a network. In one embodiment, the client connects to the

port, and the switch emits a Link Up request. In one embodiment, the Link Up request may be emitted because the client that is connected to the switch port has booted up its physical interface. In any event, the enforcer may detect the Link Up request and enable a backoff timer. The backoff timer may be employed as a mechanism to limit an amount of time to monitor for 802.1X authentication messages. Associated with the backoff timer is a time limit. The time limit may be set to a value based on a variety of criteria, including, but not limited to network characteristics, switch characteristics, engineering judgment, or the like. In one embodiment, the time limit may be set between about 1-5 minutes. Moreover, the invention may also use another mechanism to determine when to initiate the backoff timer, including but not limited to an event, signal, or message from the client.

Processing next continues to decision block 406, where a determination is made whether the client is 802.1X capable within the backoff time-limit. In one embodiment, the client may automatically send an 802.1X authentication request, such as an EAP-response message, to the switch, thereby indicating that it is 802.1X capable. In another embodiment, the switch may send an 802.1X initiation request, such as an EAP-request identity message, to the client. If the client is 802.1X capable, it may respond with an 802.1X authentication request. In one embodiment, upon receipt of an 802.1X authentication request message from the client, the determination is made that the client is 802.1X capable. For example, the enforcer acting as an authentication server may determine that the client is 8021.X capable upon receipt of the 802.1X authentication request forwarded from the switch. In another embodiment, the enforcer, acting as an authentication proxy may make this determination upon detecting an 802.1X traffic request being forwarded between the switch and the authentication server. However, the invention is not limited to a client's failure to respond and/or provide an 802.1X authentication message. For example, a variety of other predefined failure conditions may also be employed to determine if the client is 802.1X authentication capable, including, but not limited to the client providing an incorrect authentication credential; a failed, out of date, or otherwise improperly configured supplicant (e.g., the client seeking access to the LAN port providing the request); an inoperable switch; or the like.

In any event, if it is determined that the client is 802.1X authentication capable within the backoff time-limit, processing then flows to block 408. However, if

the backoff time limit is exceeded before the enforcer detects an 802.1X authentication request, or the like as described above, a determination is made that the client is not 802.1X capable and processing branches to block 410.

At block 408 the enforcer disables the backoff timer. Processing then continues to decision block 409, where the determination is made whether the client is successfully authenticated with the 802.1X protocol. If the client is successfully authenticated using an 802.1X authentication protocol, the processing continues to block 416 where the client is enabled to access another resource, such as resource devices 110-111, based on a first policy. The enforcer may enable the access. In one embodiment, the switch port associated with the client device may be switched to a corporate VLAN to enable access to additional resources. In one embodiment (not shown), a backend Remote Authentication Dial-In User Service (RADIUS) server could put the client back to a different VLAN on the switch, depending on a policy of the RADIUS server. Processing then continues to block 420, where the enforcer may re-enable 802.1X authentication on the switch port. In one embodiment, this action may be performed if the enforcer detects that the client has requested to disconnect from the network. In one embodiment, when the client disconnects from the switch, a Link Down request (trap or event) may be emitted to the enforcer. The enforcer may clear out a client table, file, database, or the like, for the client that previously existed on that switch port. In one embodiment, if the switch port associated with the client is in a backoff mode, the enforcer may reset the mode of the switch port into an auto mode, thereby re-enabling 802.1X authentication on the switch port. Processing then returns to a calling process.

If, at decision block 409, the client is not successfully authenticated using the 802.1X authentication protocol, then processing may return to the calling process. In another embodiment (not shown), processing may loop back to decision block 409, where the client may be enabled to perform another authentication attempt using an 802.1X authentication protocol. In yet another embodiment, the client may be determined to be 802.1X incapable, and processing may branch to block 410.

At block 410 the enforcer may disable 802.1X processing on the switch port. In one embodiment, the enforcer may set the switch port into a backoff mode. For example, non-802.1X packets, such as HTTP and DHCP, may be enabled to flow through

the switch port. In one embodiment, the backoff mode may be the authorized mode. Processing then continues to block 412, where the client is enabled to access quarantined resources, such as resource device 110 of FIGURE 1, or the like. In another embodiment, the client may be unable to access resources until it has been authenticated. In still another embodiment, the client's network traffic is routed through the enforcer. In one embodiment, the enforcer enables the switch port to access a quarantined or guest VLAN, such as guest VLAN 102. For example, the enforcer may put the switch port on the guest VLAN through Simple Network Management Protocol (SNMP), SSH Telnet, a proprietary Application Programming Interface (API), or the like.

Processing then continues to block 413, where the enforcer may be enabled to employ a non-802.1X authentication detection mechanism. Processing then continues to decision block 414, where a determination is made whether the client is successfully authenticated using the non-802.1X authentication mechanism. If the client is authenticated successfully, processing continues to block 418 where the enforcer may enable the client device to access more resources or different resources based on a second policy. In one embodiment, the switch port associated with the client device may be switched to a corporate VLAN to enable the access to the other resources, or enable access to another set of resources within the guest VLAN, or the like. Processing then continues to block 420, where the enforcer may re-enable 802.1X authentication on the switch port if the enforcer detects that the client has requested to disconnect from the network. Processing then continues to a calling process.

If, at decision block 414, the client is not successfully authenticated with the non-802.1X authentication mechanism, then processing may continue to block 420, where the enforcer may re-enable 802.1X authentication on the switch port. In one embodiment, this action may be performed if it is detected that the client has requested to disconnect from the network. The process then returns to the calling process. In another embodiment (not shown), processing may loop back to decision block 414, where the client is allowed to make another attempt to connect using a non-802.1X authentication mechanism.

FIGURE 5 illustrates a logical flow diagram generally showing one embodiment of a process for enabling dynamic authentication with different protocols on

the same port for a switch independent of a backoff timer. FIGURE 5 may be enabled by enforcer 108 and switch 106 of FIGURE 1. As shown in the figure, process 500 begins, after a start block, at block 502, where a switch and/or an enforcer detect a client's request to join a network. In one embodiment, the client connects to the port and the switch emits a Link Up request. In one embodiment, the Link Up request may be emitted because the client that is connected to the switch port has booted up its physical interface. In one embodiment, the switch port may be in any mode. In another embodiment, the switch port may be in the authorized mode. In this mode, non-802.1X packets, such as HTTP and DHCP, may be enabled to flow through the switch port.

Processing next continues to block 504 where the client is enabled to access quarantined resources, such as resource device 110 of FIGURE 1. In another embodiment, the client may be unable to access resources until it is authenticated. In still another embodiment, the client's network traffic is routed through the enforcer. In one embodiment, the enforcer enables the switch port to access a quarantined or guest VLAN, such as guest VLAN 102. For example, the enforcer may put the switch port on the guest VLAN through Simple Network Management Protocol (SNMP), SSH Telnet, a proprietary Application Programming Interface (API), or the like

Processing then continues to decision block 506, where a determination is made whether the client is 802.1X capable. In one embodiment, the client may automatically send an 802.1X authentication request, such as an EAP-response message, to the switch, thereby indicating that it is 802.1X capable. In another embodiment, the switch may send an 802.1X initiation request, such as an EAP-request identity message, or the like, to the client. If the client is 802.1X capable, it may respond with an 802.1X authentication request. In one embodiment, upon receipt of an 802.1X authentication request message from the client, the determination is made that the client is 802.1X capable. For example, the enforcer may act as an authentication server to determine that the client is 8021.X capable upon receipt of the 802.1X authentication request. In another embodiment, the enforcer, acting as an authentication proxy may make this determination upon detecting an 802.1X traffic request being forwarded between the switch and an authentication server. This approach of listening for 802.1X messages from the client device enables slower client devices, and/or client devices on slower network interfaces, or the like, to respond independent of a backoff time constraint.

In one embodiment, the enforcer, or another network device, may provide a web page, or other interface, to the client device. In one embodiment, the interface may enable a user of the client device to initiate a non-802.1X authentication mechanism. Initiation of the non-802.1X authentication mechanism may then indicate that the client device in incapable of 802.1X authentication.

However, the invention is not limited to a client device's failure to respond and/or provide an 802.1X authentication message, or to further initiate a non-802.1X authentication mechanism. For example, a variety of other predefined failure conditions may also be employed to determine if the client device is 802.1X authentication capable, including, but not limited to the client device providing an incorrect authentication credential, a failed or out of date supplicant, an inoperable switch, or the like.

In any event, if, at decision block 506, the determination is made that the client device is 802.1X capable, processing then continues to block 508 where the switch and the authentication server are enabled to employ 802.1X authentication. In one embodiment, the enforcer may act as the authentication server. In one embodiment, the enforcer puts a switch port on the switch into an auto mode, thus enabling 802.1X authentication detection. In one embodiment, 802.1X packets may be processed on the switch port, while other packets may be dropped, or otherwise ignored by the switch. Processing then continues to decision block 512. If, at decision block 506, the determination is made that the client is not 802.1X capable, processing then continues to block 510.

At decision block 512, the determination is made whether the client is successfully authenticated with the 802.1X protocol. If the client is successfully authenticated using an 802.1X authentication protocol, the processing continues to block 516 where the client is enabled to access another resource, such as resource devices 110-111, based on a first policy. The enforcer may enable the access. In one embodiment, the switch port associated with the client device may be switched to a corporate VLAN to enable access to additional resources. In one embodiment (not shown), a backend Remote Authentication Dial-In User Service (RADIUS) server could put the client back to a different VLAN on the switch, depending on the policy of the RADIUS server. Processing may then continue to a calling process.

If, at decision block 512, the client is not successfully authenticated using the 802.1X authentication protocol, then processing may return to the calling process. In another embodiment (not shown), processing may loop back to decision block 512, where the client may be enabled to perform another authentication attempt using an 802.1X authentication protocol. In yet another embodiment, the client may be determined to be 802.1X incapable, and processing may continue to block 510.

At block 510, the enforcer may be enabled to employ a non-802.1X authentication detection mechanism. In one embodiment, this may be through an interface, such as a Command Line Interface (CLI), a web page, or the like, that may be provided to the client device. The interface may enable entry of such non-802.1X authentication inputs as a user name/password, a digital certificate, a token, or the like.

Processing then continues to decision block 514, where a determination is made whether the client is successfully authenticated using the non-802.1X authentication mechanism. If the client is authenticated successfully, processing continues to block 518 where the enforcer may enable the client device to access more resources or different resources based on a second policy. In one embodiment, the switch port associated with the client device may be switched to a corporate VLAN to enable the access to the other resources, or enable access to another set of resources within the guest VLAN, or the like. Processing then continues to a calling process.

If, at decision block 514, the client is not successfully authenticated with the non-802.1X authentication mechanism, then processing may continue to a calling process. In another embodiment (not shown), processing may loop back to decision block 514, where the client is allowed to make another attempt to connect using a non-802.1X authentication mechanism.

It will be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer implemented

process such that the instructions, which execute on the processor to provide steps for implementing the actions specified in the flowchart block or blocks.

Accordingly, blocks of the flowchart illustration support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustration, and combinations of blocks in the flowchart illustration, can be implemented by special purpose hardware-based systems which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

The above specification, examples, and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

CLAIMS

What is claimed as new and desired to be protected by Letters Patent of the United States is:

1. A method of authentication of a client over a network, comprising:

detecting a request to join the network from the client;

if it is determined that the client is 802.1X authentication capable within a backoff time-limit, employing an 802.1X authentication mechanism to authenticate the client; and

if the backoff time-limit is exceeded before the client is determined to be 802.1X capable, employing a non-802.1 X authentication mechanism to authenticate the client.

2. The method of Claim 1, wherein the non-802.1X authentication mechanism further comprises at least one of a user name/password, digital certificate, token, browser based authentication, windows based authentication, Kerberos, one-time password, public key authentication, or biometrics.

3. The method of Claim 1, wherein determination that the client is 802.1X authentication capable further comprises at least one of receiving an Extensible Authentication Protocol (EAP) response message, receiving a client identity in response to an 802.1X request for identity, or receiving an 802.1X start message.

4. The method of Claim 1, wherein determination that the client is 802.1X authentication capable further comprises detecting of at least one of an incorrect authentication credential associated with the client, an improperly configured supplicant, or an inoperable switch.

5. The method of Claim 1, further comprising configuring a switch such that the client is quarantined to a pre-determined network.

6. The method of Claim 1, wherein employing a non-802.1X authentication mechanism further comprises providing to the client at least one of a web page, or a Command Line Interface for use at least in part in performing non-802.1X authentication.

7. The method of Claim 1, wherein employing an 802.1X authentication mechanism further comprises employing an authentication server to authenticate the client.

8. A modulated data signal configured to include program instructions for performing the method of Claim 1.

9. A system of authentication of a client over a network, comprising:

a network switch that is operative to route network traffic; and

an enforcer component in communication with the network switch and that includes program code operative to perform actions, comprising:

receiving a request to access a resource on a restricted network from the client through the network switch;

if it is determined that the client is 802.1X authentication capable within a backoff time-limit, employing an 802.1X authentication mechanism to authenticate the client; and

if the backoff time-limit is exceeded before the client is determined to be 802.1X capable, enabling the client to employ a non-802.1 X authentication mechanism for authentication to join the network.

10. The system of Claim 9, the actions further comprising configuring the network switch to detect an 802.1X authentication message.

11. The system of Claim 9, wherein receiving a request to access a resource further comprises receiving a link up request.

12. The system of Claim 9, wherein the determination that the client is 802.1X authentication capable further comprises at least one of receiving an Extensible Authentication Protocol (EAP) response message, receiving a client identity in response to an 802.1X request for identity, or receiving an 802.1X start message.

13. The system of Claim 9, wherein the enforcer component is further configured to forward authentication information to an authentication server.

14. The system of Claim 9, the actions further comprising:

in response to receiving the request, directing the network switch to place the client on a quarantined network; and

configuring the switch to route network traffic associated with the client through the enforcer component.

15. A system of authentication of a client over a network, comprising:

a network switch that is operative to route network traffic; and

an enforcer component in communication with the network switch and that includes program code operative to perform actions, comprising:

receiving a request to access a resource on a restricted network from the client through the network switch;

if it is determined that the client is 802.1X authentication capable, employing an 802.1X authentication mechanism to authenticate the client; and

if it is determined that the client is 802.1X authentication incapable, enabling the client to employ a non-802.1 X authentication mechanism for authentication to join the network.

16. The system of Claim 15, the actions further comprising:

if a backoff time limit is exceeded before it is determined that the client is 802.1X authentication capable, designating the client as 802.1X authentication incapable.

17. The system of Claim 15, wherein determination that the client is 802.1X authentication capable further comprises detecting of at least one of an incorrect authentication credential associated with the client, an improperly configured supplicant, or an inoperable switch.

18. The system of Claim 15, the actions further comprising:

providing to the client a non-802.1X authentication mechanism; and

if the client employs the non-802.1X authentication mechanism, designating the client as 802.1X authentication incapable.

19. The system of Claim 15, the actions further comprising:

in response to receiving the request, directing the network switch to place the client on a quarantined network.

20. The system of Claim 15, wherein the actions further comprising:

in response to receiving the request, directing the network switch to route network traffic from or to the client device to the enforcer component.

21. The system of Claim 15, wherein determination that the client is 802.1X authentication capable further comprises at least one of receiving an Extensible Authentication Protocol (EAP) response message, receiving a client identity in response to an 802.1X request for identity, or receiving an 802.1X start message.

22. The system of Claim 15, wherein if it is determined that the client is 802.1X authentication incapable further comprises, configuring the network switch for non-802.1X authentication.

23. A network device for managing an authentication of a client over a network, comprising:

a transceiver to send and receive data over the network; and

means for receiving a request to access a resource from the client;

means for determining if the client is 802.1X authentication capable or 802.1 authentication incapable; and

means for employing an authentication mechanism to authenticate the client based in part on whether the client is determined to be 802.1X authentication capable or determined to be 802.1 authentication incapable.

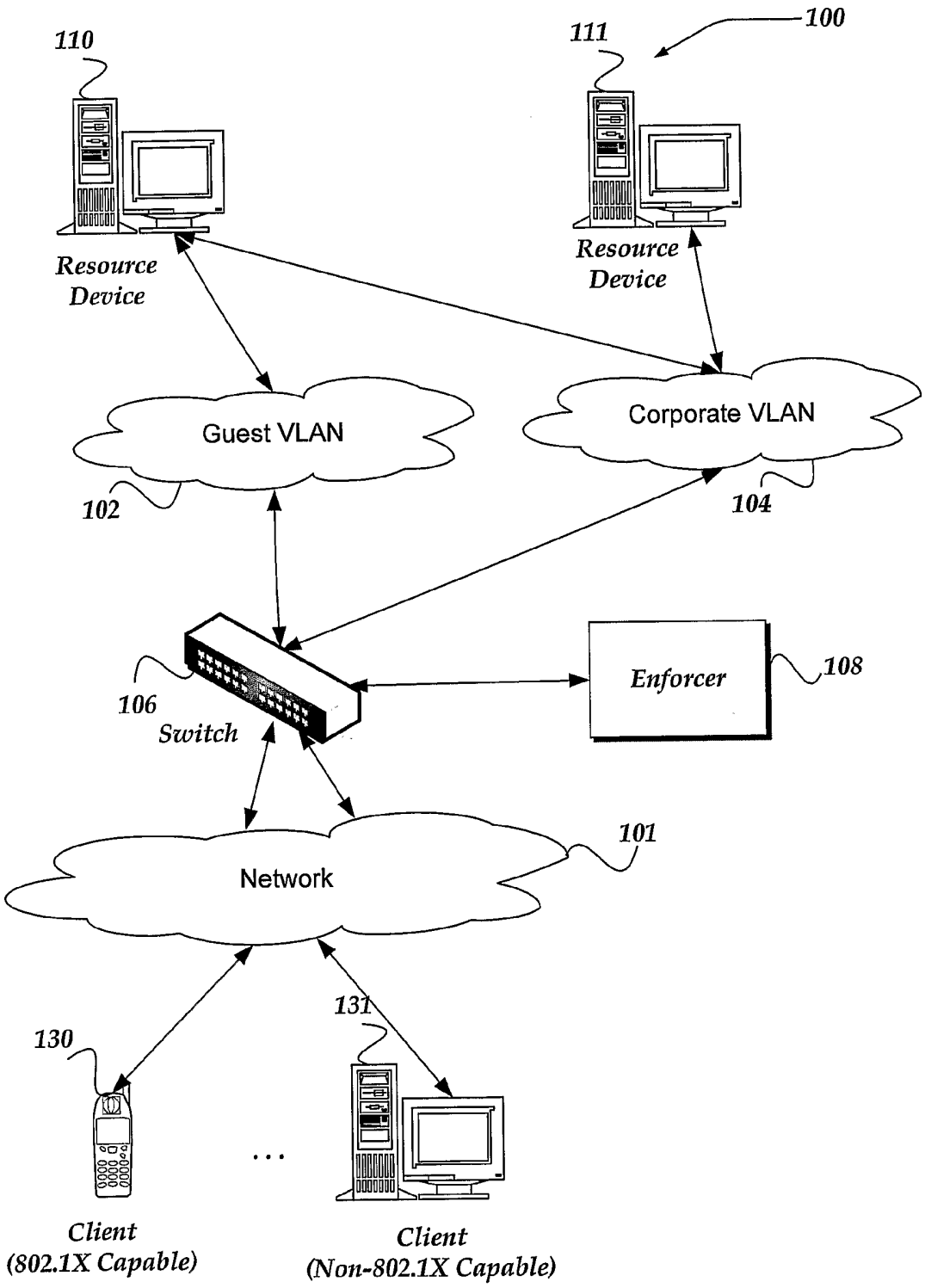

110
111
100
Resource Device
Resource Device
Guest VLAN
Corporate VLAN
102
104
106
Switch
Enforcer
108
Network
101
131
130
Client (802.1X Capable)
Client (Non-802.1X Capable)

FIG. 1

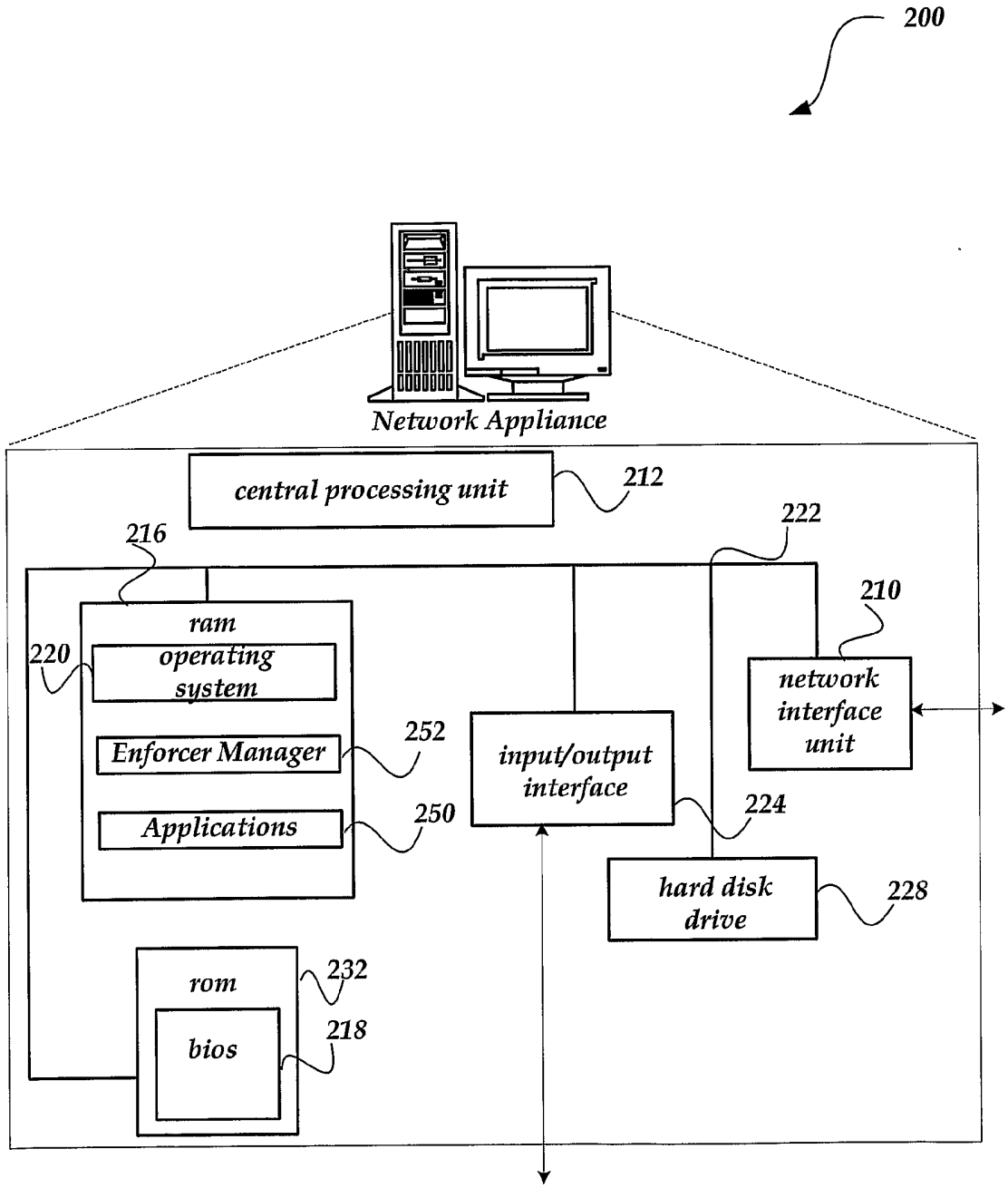

200
Network Appliance
central processing unit
212
216
222
210
ram
220
operating system
Enforcer Manager
252
Applications
250
input/output interface
224
network interface unit
hard disk drive
228
rom
232
bios
218

FIG. 2

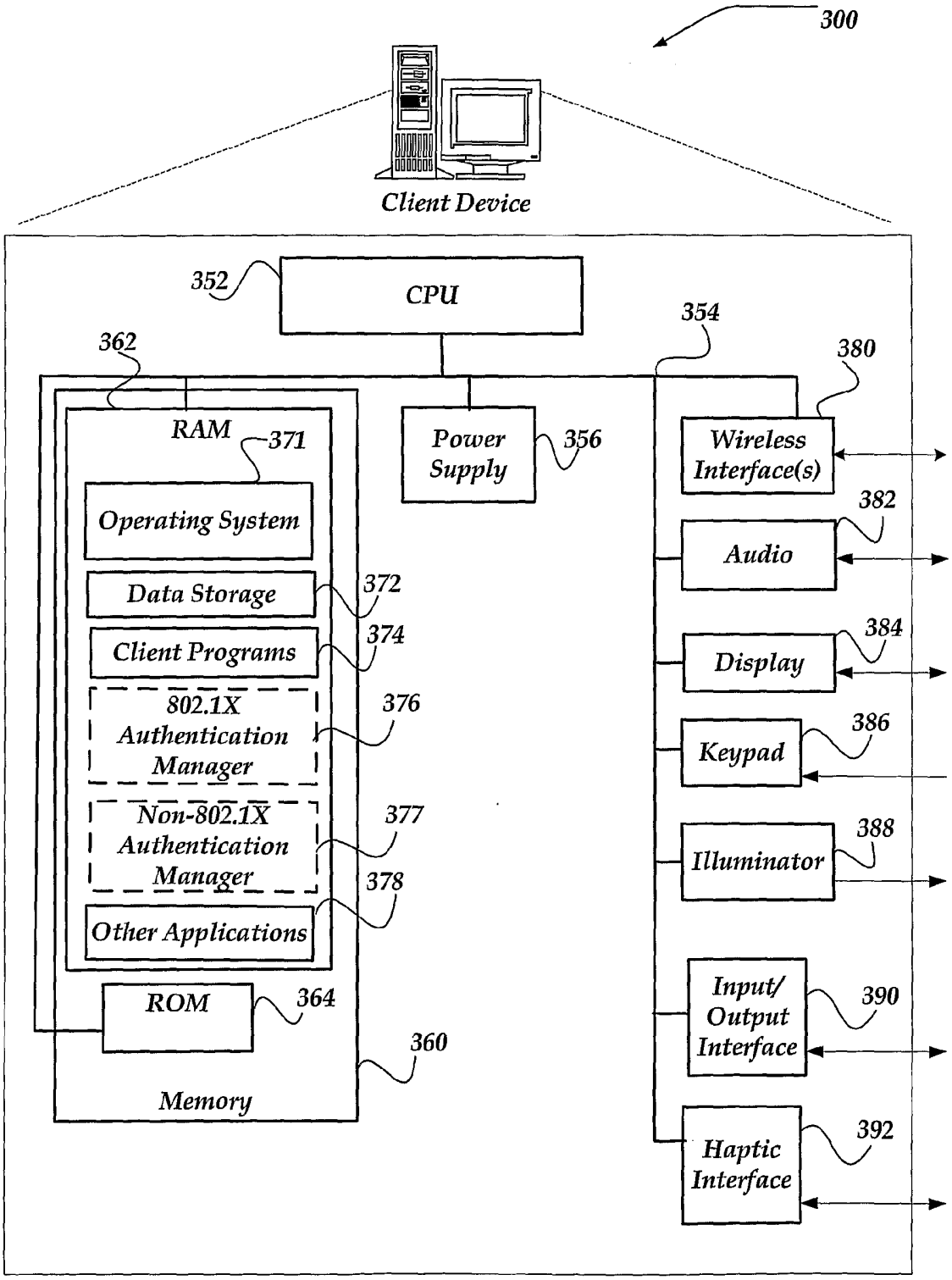

300
Client Device
352
CPU
354
362
380
RAM
371
Power Supply
356
Wireless Interface(s)
Operating System
382
Audio
Data Storage
372
Client Programs
374
384
Display
802.1X Authentication Manager
376
386
Keypad
Non-802.1X Authentication Manager
377
388
Illuminator
378
Other Applications
ROM
364
Input/ Output Interface
390
360
Memory
Haptic Interface
392

FIG. 3

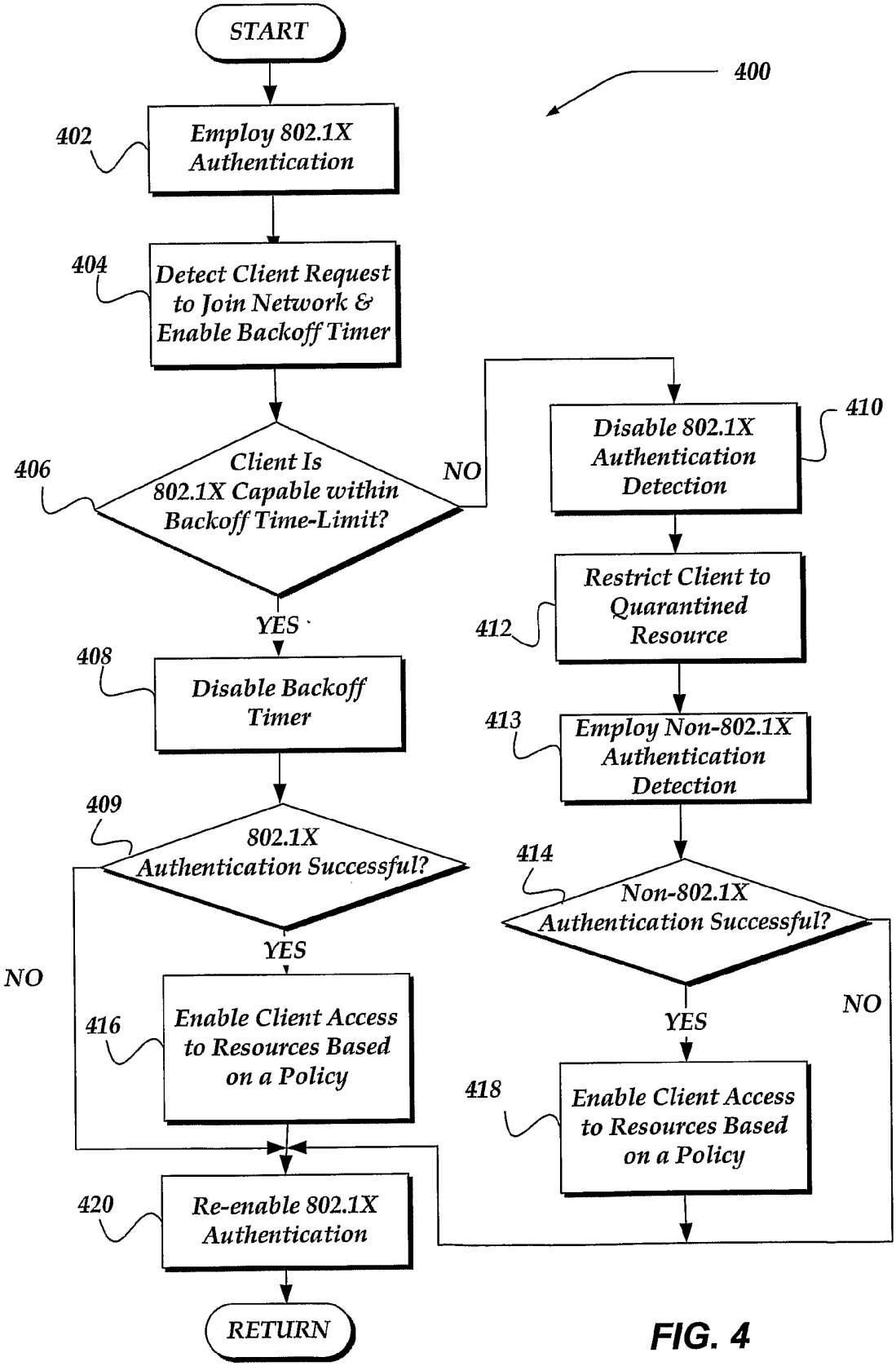

START
400
402
Employ 802.1X Authentication
404
Detect Client Request to Join Network & Enable Backoff Timer
406
Client Is 802.1X Capable within Backoff Time-Limit?
NO
410
Disable 802.1X Authentication Detection
412
Restrict Client to Quarantined Resource
413
Employ Non-802.1X Authentication Detection
414
Non-802.1X Authentication Successful?
YES
NO
418
Enable Client Access to Resources Based on a Policy
YES
408
Disable Backoff Timer
409
802.1X Authentication Successful?
YES
NO
416
Enable Client Access to Resources Based on a Policy
420
Re-enable 802.1X Authentication
RETURN

FIG. 4

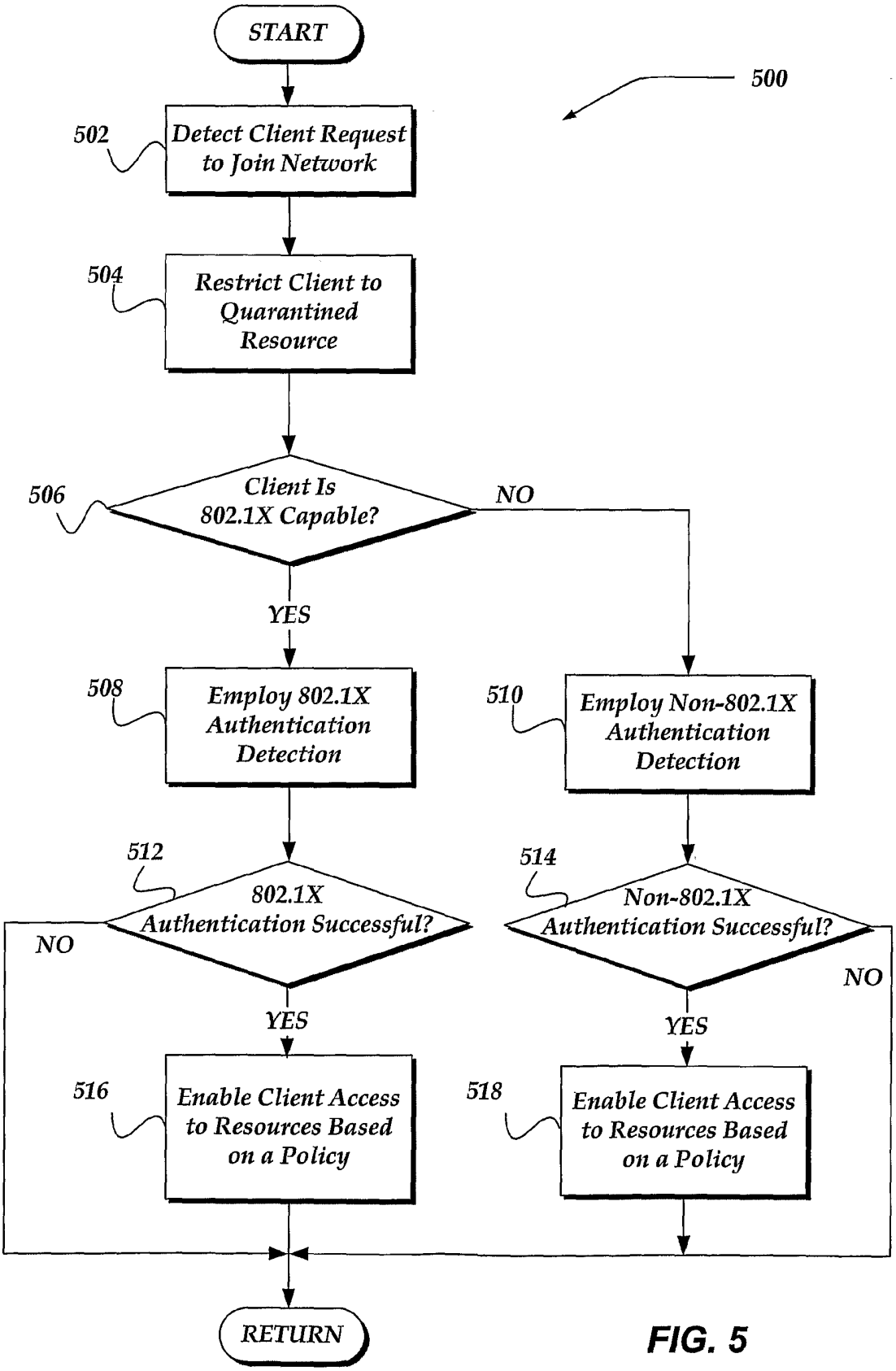

START
500
502
Detect Client Request to Join Network
504
Restrict Client to Quarantined Resource
506
Client Is 802.1X Capable?
NO
YES
508
Employ 802.1X Authentication Detection
510
Employ Non-802.1X Authentication Detection
512
802.1X Authentication Successful?
NO
YES
514
Non-802.1X Authentication Successful?
NO
YES
516
Enable Client Access to Resources Based on a Policy
518
Enable Client Access to Resources Based on a Policy
RETURN

FIG. 5