US009270454B2

(12) **United States Patent**
Maruti et al.

(10) **Patent No.: US 9,270,454 B2**
(45) **Date of Patent: Feb. 23, 2016**

(54) **PUBLIC KEY GENERATION UTILIZING MEDIA ACCESS CONTROL ADDRESS**

(75) Inventors: **Kamat Maruti**, Bangalore Karnataka (IN); **Chuck A Black**, Rocklin, CA (US)

(73) Assignee: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP**, Houston, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 727 days.

(21) Appl. No.: **13/600,318**

(22) Filed: **Aug. 31, 2012**

(65) **Prior Publication Data**

US 2014/0068252 A1 Mar. 6, 2014

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 9/08	(2006.01)
H04L 9/32	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/0866*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/3263*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 9/0866; H04L 9/3263; H04L 9/3247
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,234,163	B1	6/2007	Rayes et al.
7,516,487	B1	4/2009	Szeto et al.
7,587,751	B2	9/2009	Potter et al.
7,921,290	B2	4/2011	Albert et al.
7,958,352	B2	6/2011	Edgett et al.
7,975,289	B2	7/2011	Hashimoto et al.
8,239,549	B2	8/2012	Aura et al.
2003/0056092	A1	3/2003	Edgett et al.
2004/0213172	A1	10/2004	Myers et al.
2005/0021979	A1	1/2005	Wiedmann et al.
2006/0114863	A1	6/2006	Sanzgiri et al.
2006/0174106	A1	8/2006	Bell et al.
2008/0040773	A1	2/2008	AlBadarin et al.
2008/0092214	A1	4/2008	Zavalkovsky et al.
2008/0134308	A1	6/2008	Yalakanti et al.
2008/0209207	A1	8/2008	Parupudi et al.
2010/0146609	A1	6/2010	Bartlett

FOREIGN PATENT DOCUMENTS

WO PCT/US2011/049402 8/2011

OTHER PUBLICATIONS

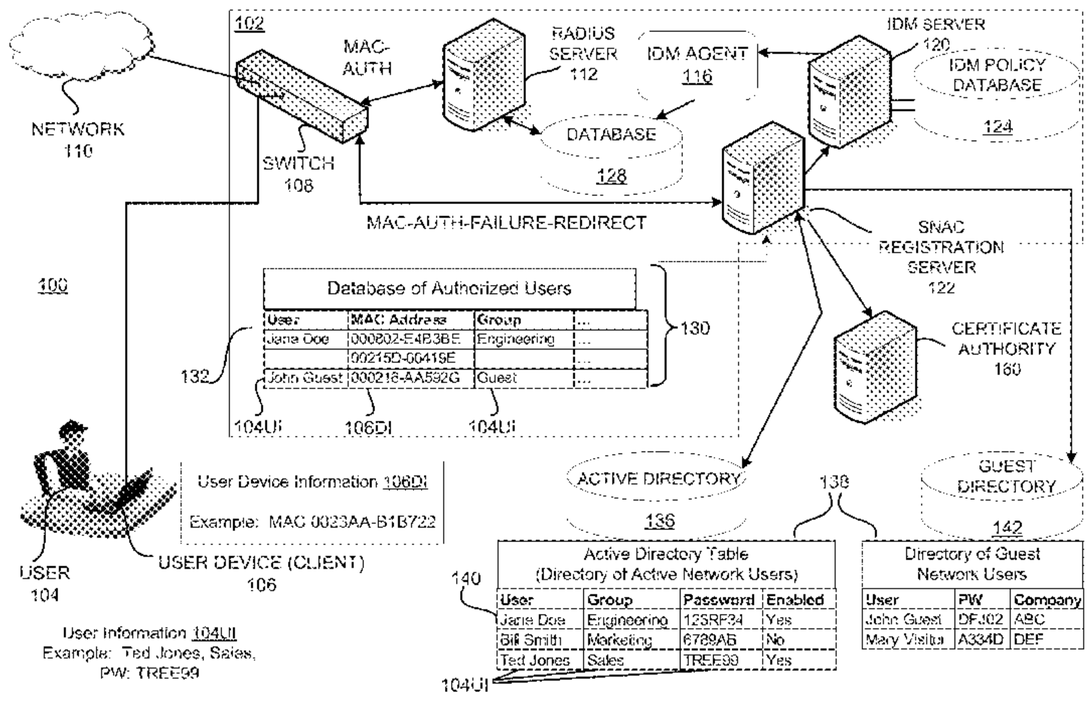
"AAA Protocol," Wikipedia, Feb. 2011. <http:en.wikipedia.org/wiki/AAA_protocol>.
"How to configure MAC authentication on a ProCurve switch," An HP ProCurve Networking Application Note, Jul. 2008.
"Preventing MAC Spoofing," Research Paper, Avenda Systems, 2011. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CGMQFjAE>.
"Transport Layer Security," Wikipedia, Jul. 2012. <http://en.wikipedia.org/wiki/Transport_Layer_Security>.
Lei Han, "A Threat Analysis of the Extensible Authentication Protocol," Carleton University, Apr. 2006. <http://people.scs.carleton.ca/~barbeau/Honours/Lei_Han.pdf>.
Pahwa, P. et al., "Spoofing Media Access Control (MAC) and Its Counter Measures," Jan. 2010. <http://www.steps-india.com/ijaea/32.pdf >.
Sunghyuck Hong, "Secure MAC address-based Authentication on X.509 v3 Certificate in Group Communication," Texas Tech University.

Primary Examiner — Krisna Lim
(74) *Attorney, Agent, or Firm* — Hewlett Packard Enterprise Patent Department

(57) **ABSTRACT**

In some embodiments, in a registration process where a user device is registering for access to a network, a public/private key pair may be generated based on a media access control (MAC) address of a user device. The generated public/private key pair may be transmitted to the user device for future access to the network. In some embodiments, where a user device is requesting access to a network, a MAC address embedded in a public key may be utilized to determine whether access to the network should be granted.

15 Claims, 10 Drawing Sheets



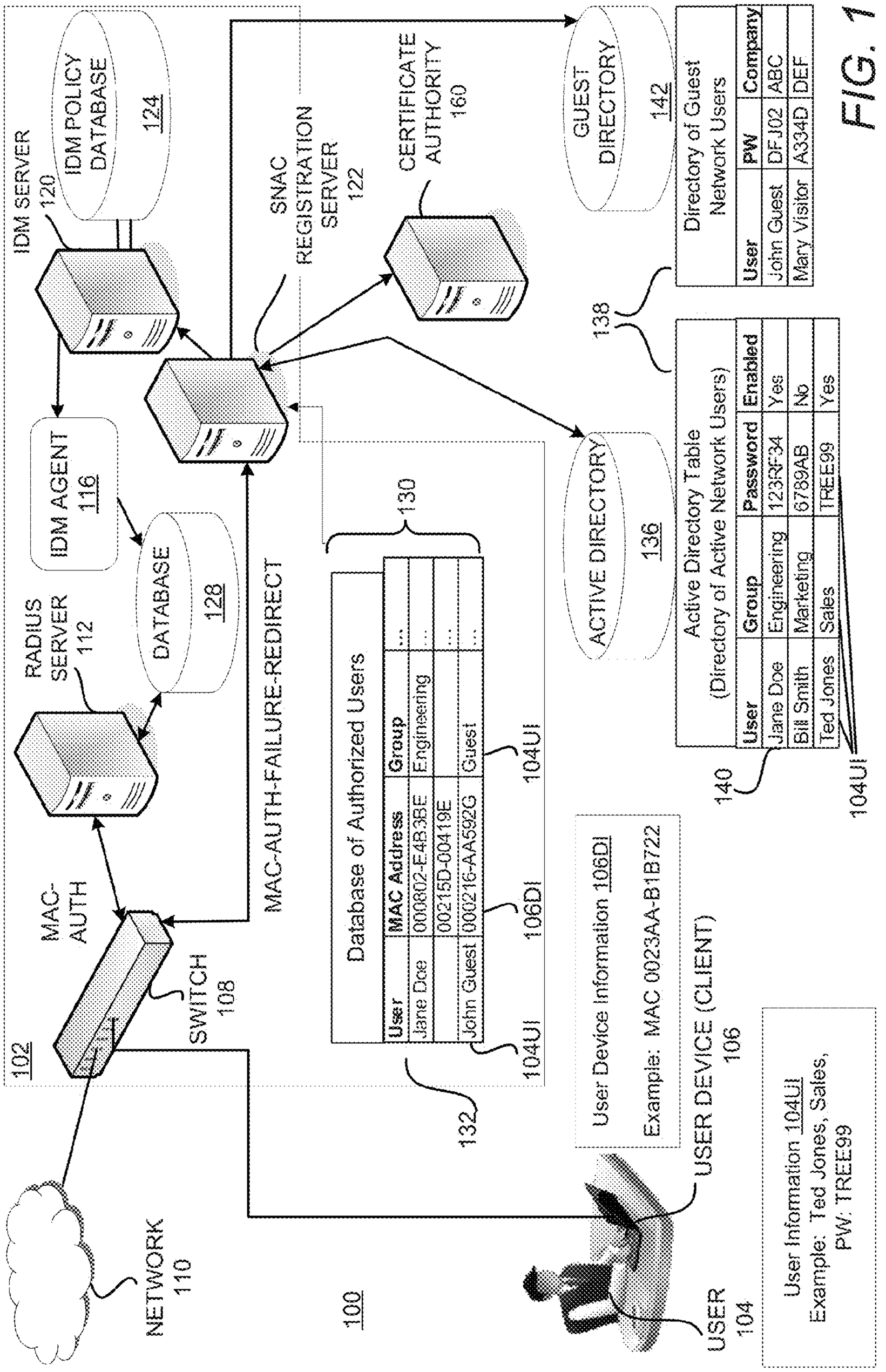

IDM SERVER
120
IDM POLICY DATABASE
124
SNAC REGISTRATION SERVER
122
CERTIFICATE AUTHORITY
160
GUEST DIRECTORY
142
Directory of Guest Network Users
User | PW | Company
John Guest | DFJ02 | ABC
Mary Visitor | A334D | DEF
138
IDM AGENT
116
RADIUS SERVER
112
DATABASE
128
MAC-AUTH
SWITCH
108
MAC-AUTH-FAILURE-REDIRECT
Database of Authorized Users
130
User | MAC Address | Group
Jane Doe | 000802-E4B3BE | Engineering
00215D-00419E
John Guest | 000216-AA592G | Guest
106DI
104UI
ACTIVE DIRECTORY
136
Active Directory Table
(Directory of Active Network Users)
User | Group | Password | Enabled
Jane Doe | Engineering | 123RF34 | Yes
Bill Smith | Marketing | 6789AB | No
Ted Jones | Sales | TREE99 | Yes
140
104UI
User Device Information 106DI
Example: MAC 0023AA-B1B722
USER DEVICE (CLIENT)
106
User Information 104UI
Example: Ted Jones, Sales,
PW: TREE99
USER
104
NETWORK
110
102
100
132

FIG. 1

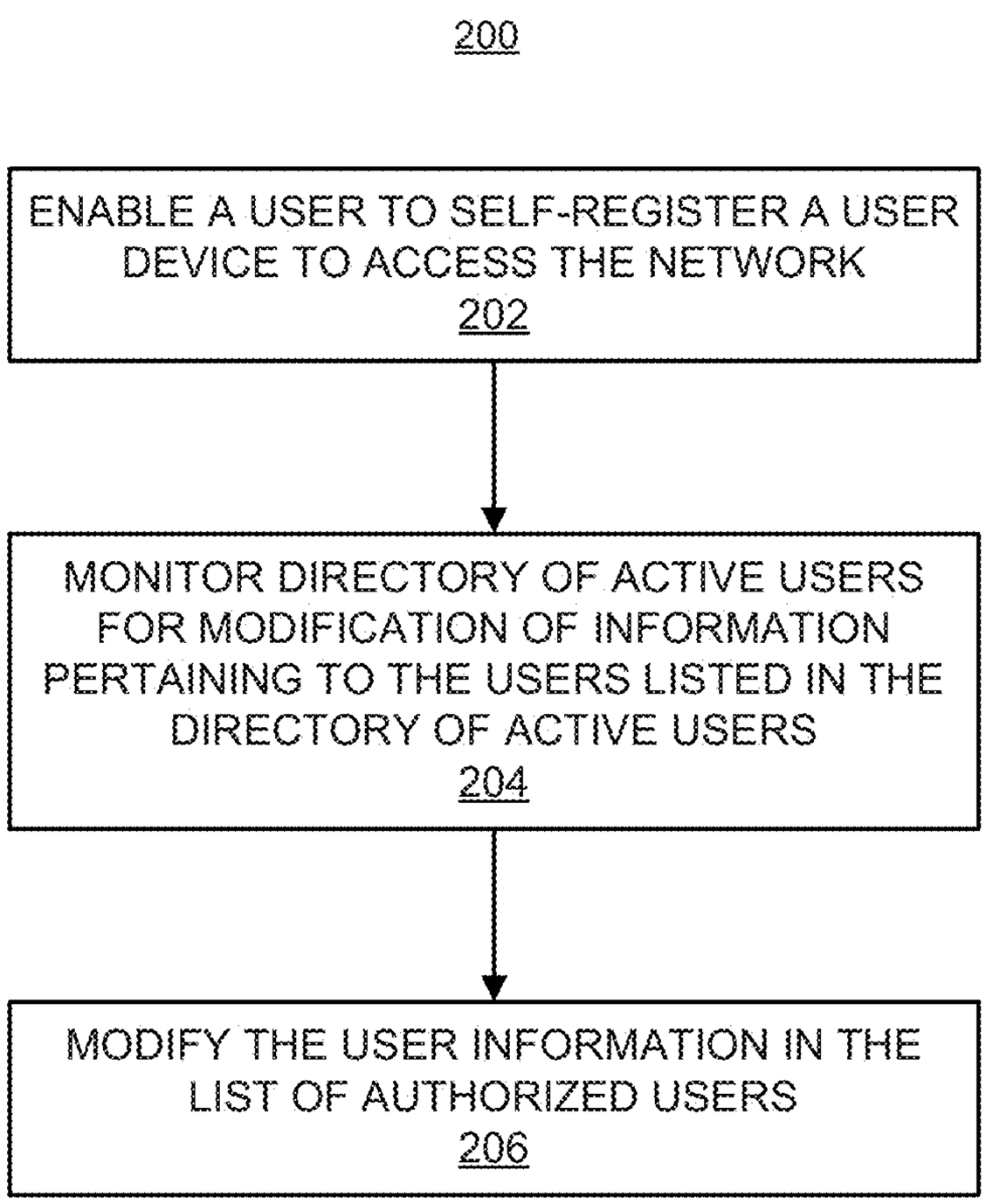

200
ENABLE A USER TO SELF-REGISTER A USER DEVICE TO ACCESS THE NETWORK
202
MONITOR DIRECTORY OF ACTIVE USERS FOR MODIFICATION OF INFORMATION PERTAINING TO THE USERS LISTED IN THE DIRECTORY OF ACTIVE USERS
204
MODIFY THE USER INFORMATION IN THE LIST OF AUTHORIZED USERS
206

FIG. 2

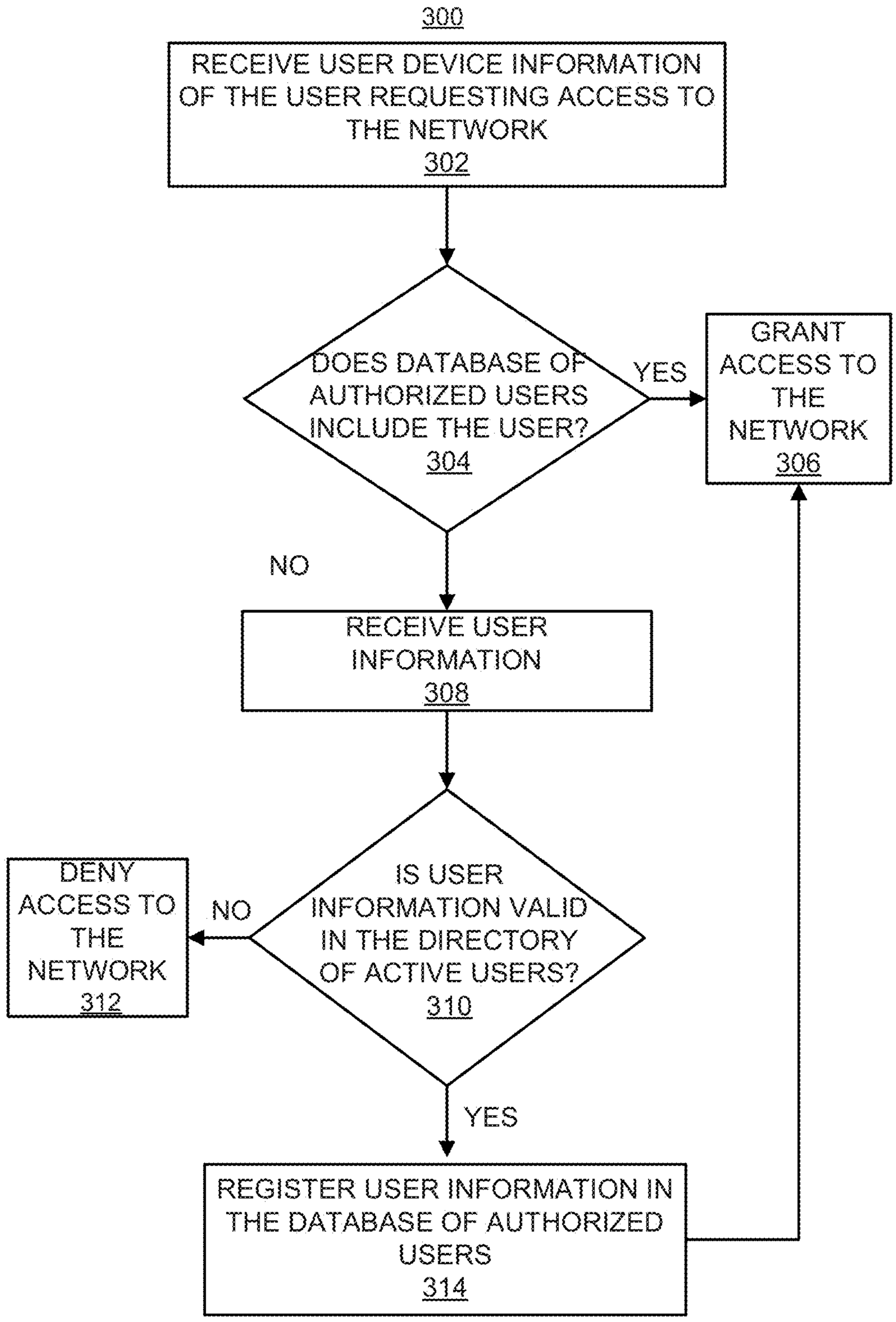

300
RECEIVE USER DEVICE INFORMATION OF THE USER REQUESTING ACCESS TO THE NETWORK
302
DOES DATABASE OF AUTHORIZED USERS INCLUDE THE USER?
304
YES
GRANT ACCESS TO THE NETWORK
306
NO
RECEIVE USER INFORMATION
308
IS USER INFORMATION VALID IN THE DIRECTORY OF ACTIVE USERS?
310
NO
DENY ACCESS TO THE NETWORK
312
YES
REGISTER USER INFORMATION IN THE DATABASE OF AUTHORIZED USERS
314

FIG. 3

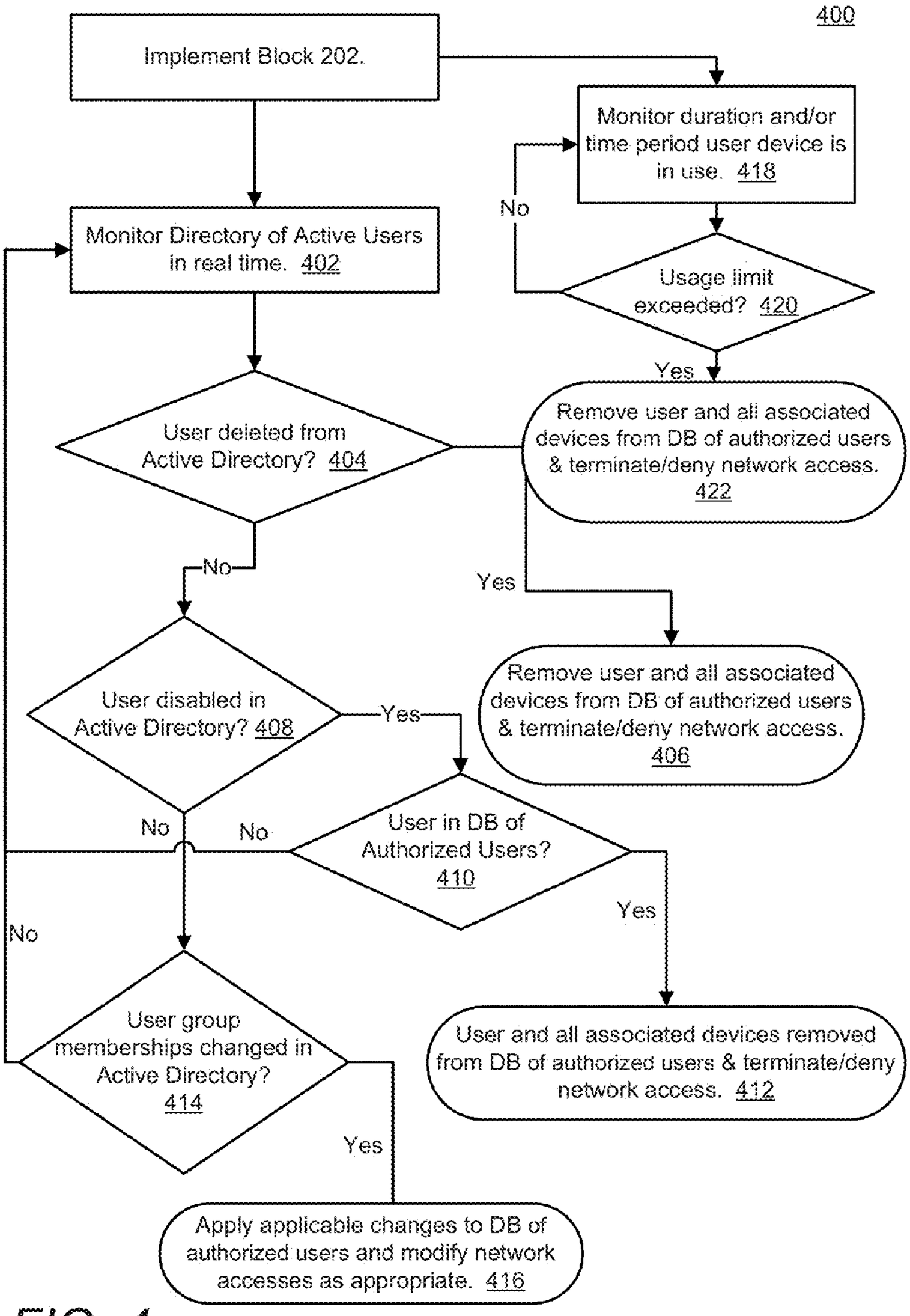

400
Implement Block 202.
Monitor Directory of Active Users in real time. 402
User deleted from Active Directory? 404
Yes
Remove user and all associated devices from DB of authorized users & terminate/deny network access. 422
No
User disabled in Active Directory? 408
Yes
Remove user and all associated devices from DB of authorized users & terminate/deny network access. 406
No
No
User in DB of Authorized Users? 410
Yes
User and all associated devices removed from DB of authorized users & terminate/deny network access. 412
No
User group memberships changed in Active Directory? 414
Yes
Apply applicable changes to DB of authorized users and modify network accesses as appropriate. 416
Monitor duration and/or time period user device is in use. 418
No
Usage limit exceeded? 420
Yes

FIG. 4

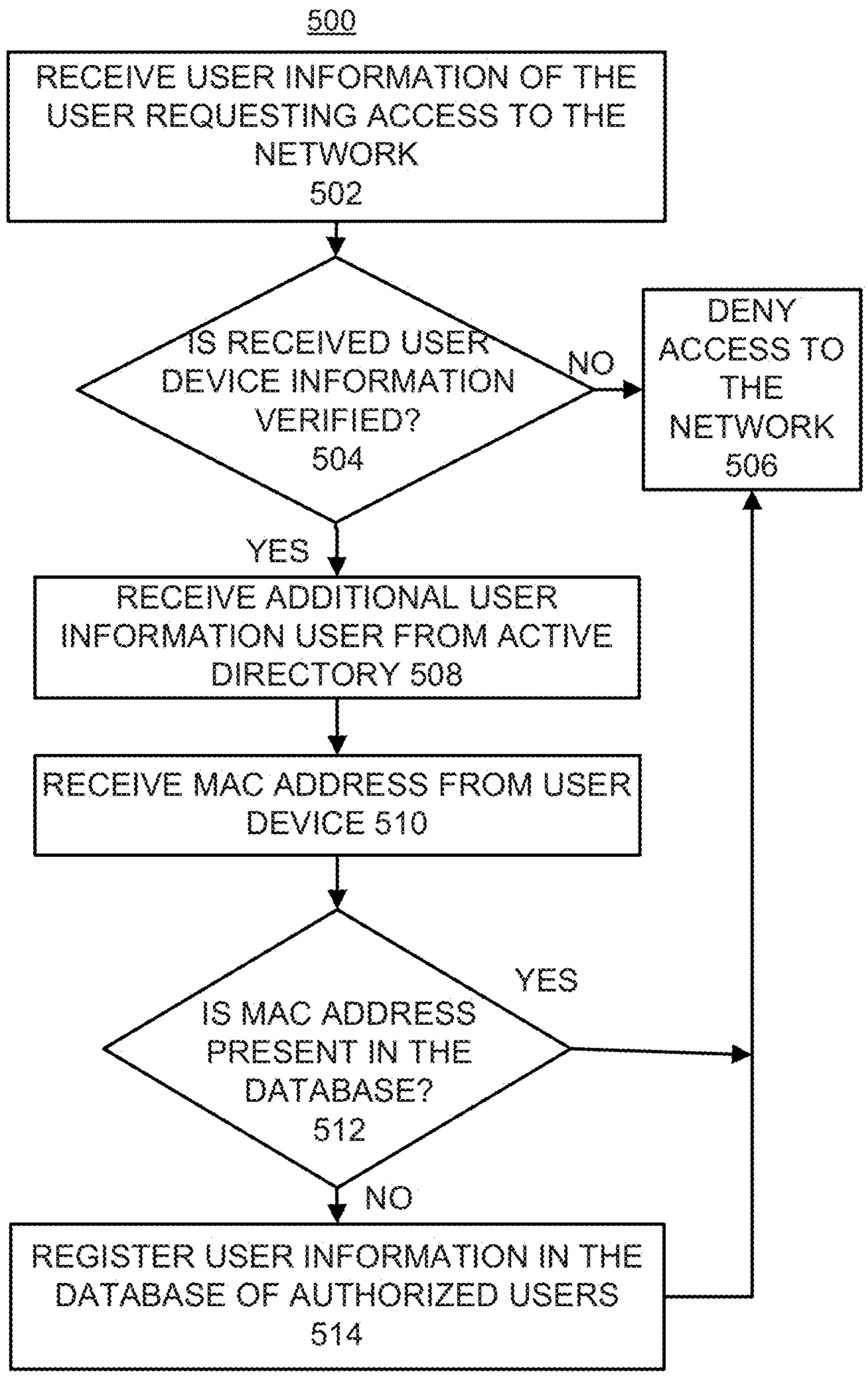

500
RECEIVE USER INFORMATION OF THE USER REQUESTING ACCESS TO THE NETWORK
502
IS RECEIVED USER DEVICE INFORMATION VERIFIED?
504
NO
DENY ACCESS TO THE NETWORK
506
YES
RECEIVE ADDITIONAL USER INFORMATION USER FROM ACTIVE DIRECTORY 508
RECEIVE MAC ADDRESS FROM USER DEVICE 510
IS MAC ADDRESS PRESENT IN THE DATABASE?
512
YES
NO
REGISTER USER INFORMATION IN THE DATABASE OF AUTHORIZED USERS
514

FIG. 5A

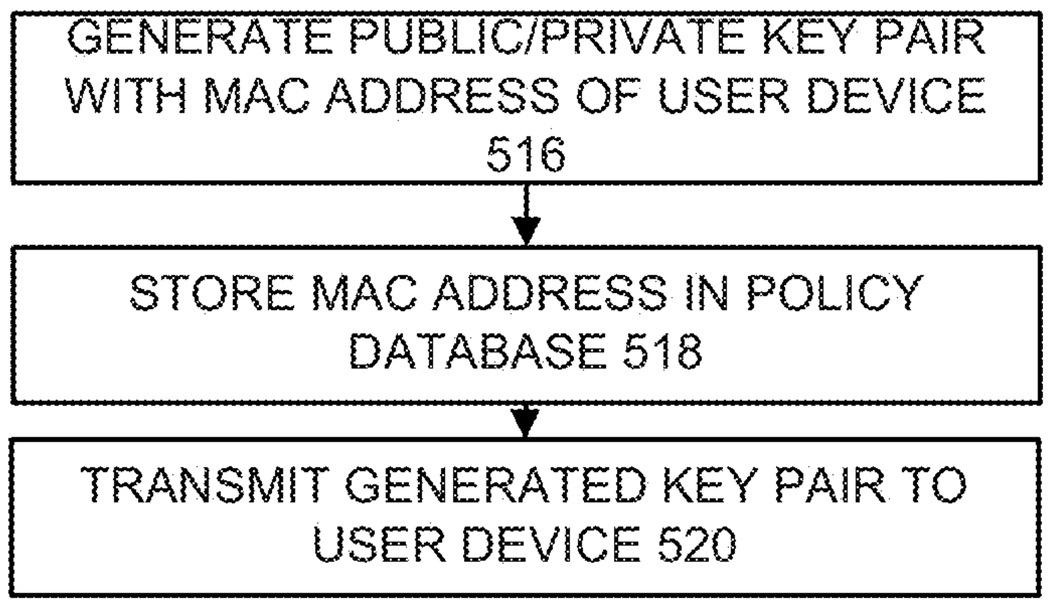

GENERATE PUBLIC/PRIVATE KEY PAIR WITH MAC ADDRESS OF USER DEVICE 516
STORE MAC ADDRESS IN POLICY DATABASE 518
TRANSMIT GENERATED KEY PAIR TO USER DEVICE 520

FIG. 5B

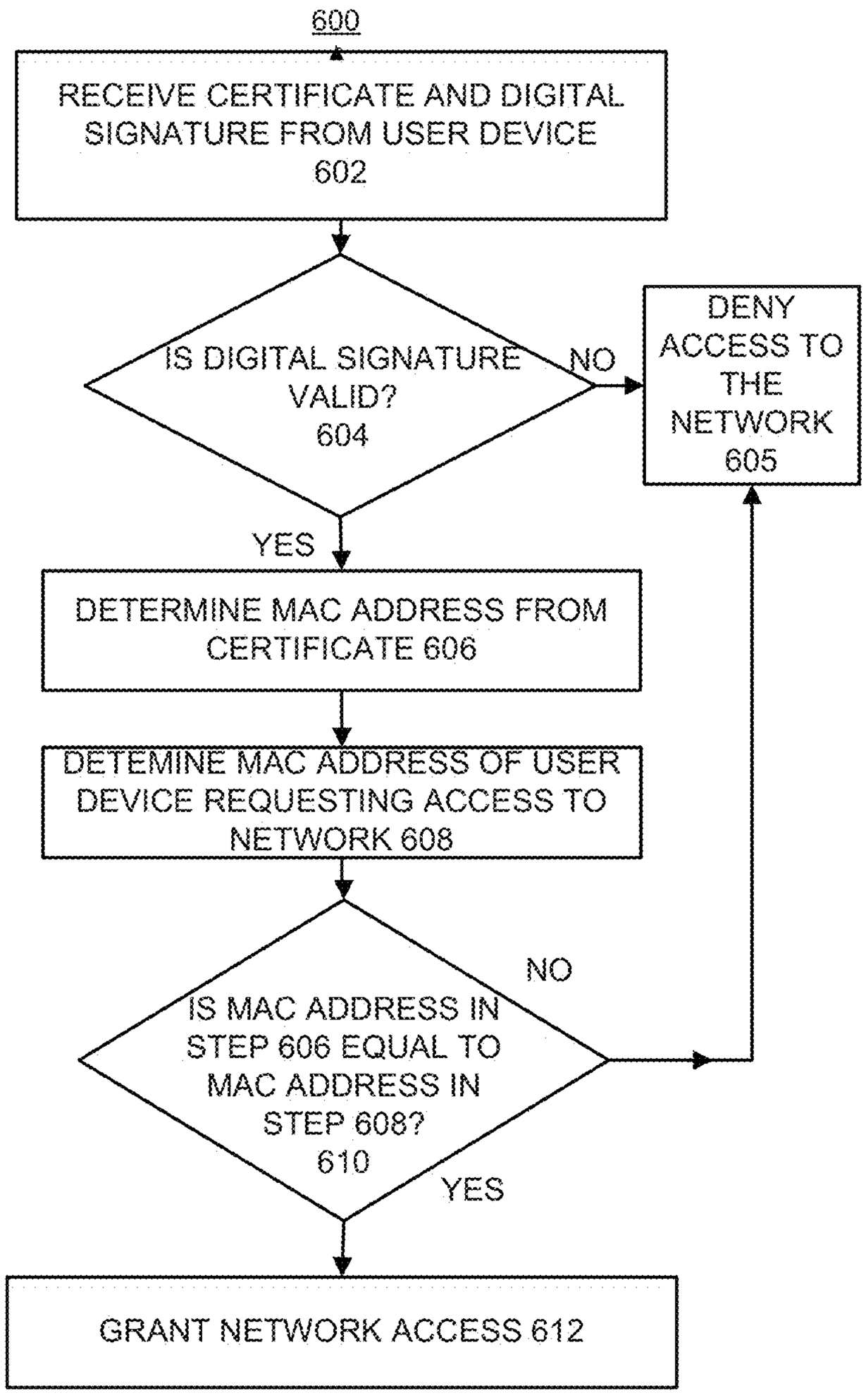

600
RECEIVE CERTIFICATE AND DIGITAL SIGNATURE FROM USER DEVICE 602
IS DIGITAL SIGNATURE VALID? 604
NO
DENY ACCESS TO THE NETWORK 605
YES
DETERMINE MAC ADDRESS FROM CERTIFICATE 606
DETEMINE MAC ADDRESS OF USER DEVICE REQUESTING ACCESS TO NETWORK 608
NO
IS MAC ADDRESS IN STEP 606 EQUAL TO MAC ADDRESS IN STEP 608? 610
YES
GRANT NETWORK ACCESS 612

FIG. 6

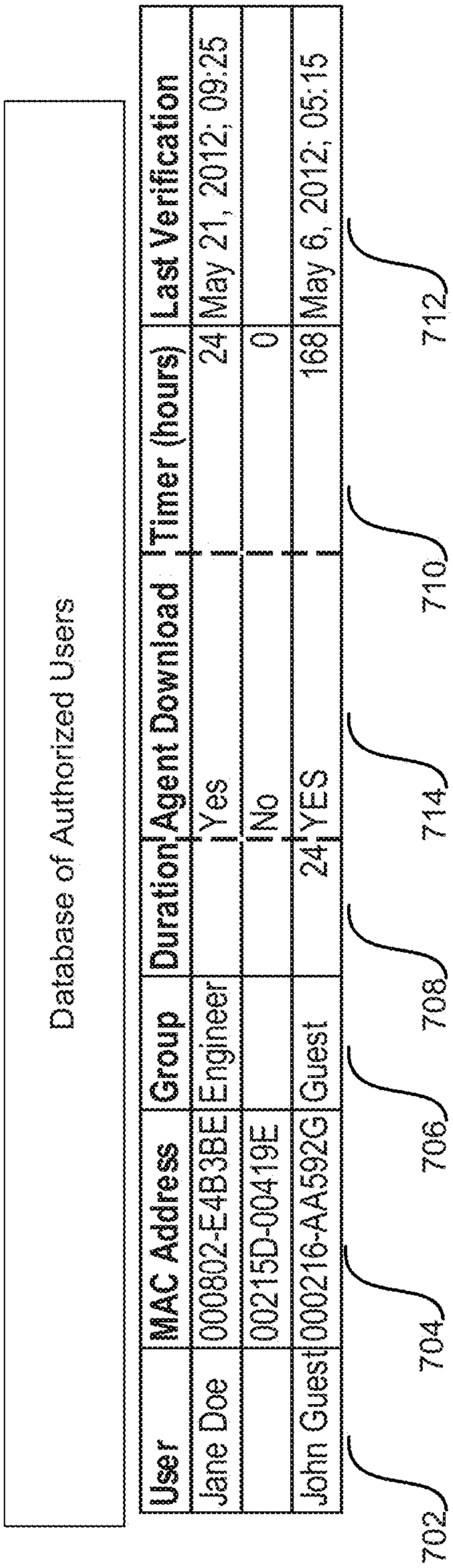

700
Database of Authorized Users
User
MAC Address
Group
Duration
Agent Download
Timer (hours)
Last Verification
Jane Doe
000802-E4B3BE
Engineer
Yes
24
May 21, 2012; 09:25
00215D-00419E
No
0
John Guest
000216-AA592G
Guest
24
YES
168
May 6, 2012; 05:15
702
704
706
708
710
712
714

FIG. 7

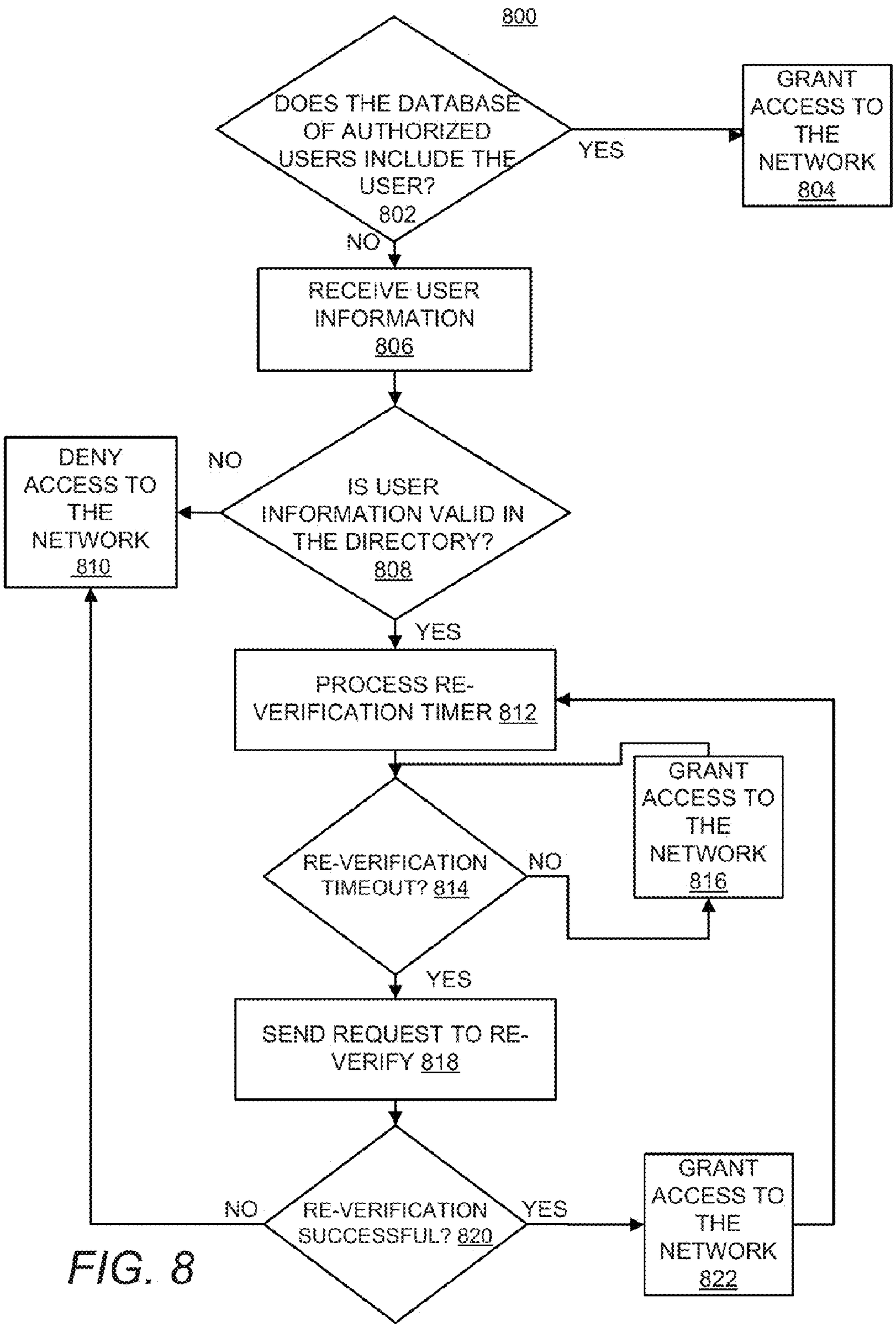

800
DOES THE DATABASE OF AUTHORIZED USERS INCLUDE THE USER? 802
YES
GRANT ACCESS TO THE NETWORK 804
NO
RECEIVE USER INFORMATION 806
IS USER INFORMATION VALID IN THE DIRECTORY? 808
NO
DENY ACCESS TO THE NETWORK 810
YES
PROCESS RE-VERIFICATION TIMER 812
RE-VERIFICATION TIMEOUT? 814
NO
GRANT ACCESS TO THE NETWORK 816
YES
SEND REQUEST TO RE-VERIFY 818
RE-VERIFICATION SUCCESSFUL? 820
NO
YES
GRANT ACCESS TO THE NETWORK 822

FIG. 8

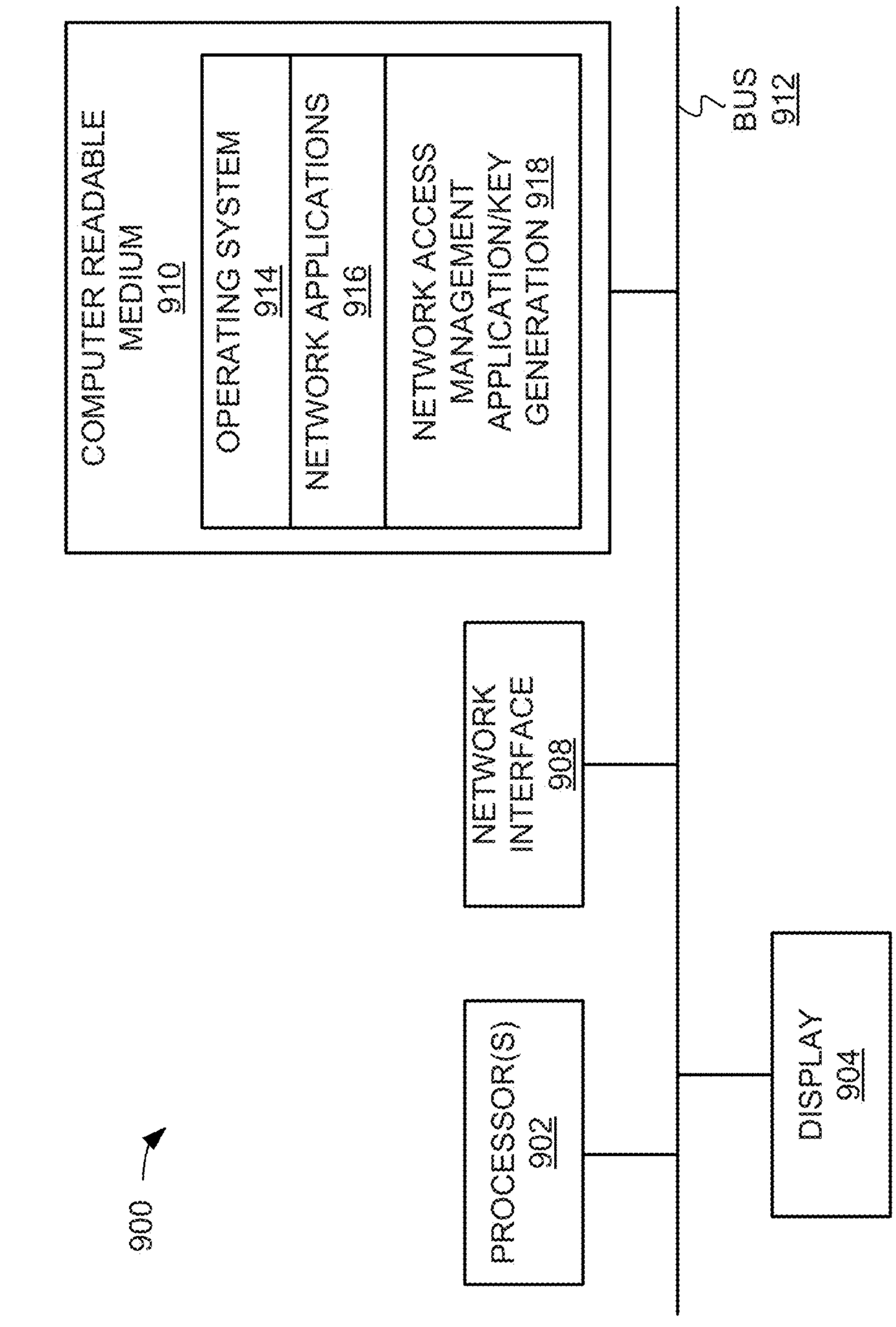

900
PROCESSOR(S)
902
DISPLAY
904
NETWORK
INTERFACE
908
BUS
912
COMPUTER READABLE
MEDIUM
910
OPERATING SYSTEM
914
NETWORK APPLICATIONS
916
NETWORK ACCESS
MANAGEMENT
APPLICATION/KEY
GENERATION 918

FIG. 9

PUBLIC KEY GENERATION UTILIZING MEDIA ACCESS CONTROL ADDRESS

BACKGROUND

User-oriented processing and communications devices, such as personal computers, laptop computers, cell phones, PDAs, printers, and similar devices are frequently connected to computer networks and/or communications networks. These may include corporate, educational, government, public access and other networks.

Network connectivity entails not just a physical connection, such as a hardwired coupling or a coupling via a wireless connection, but also software-based authorization to access network resources. Such authorized access typically provides the ability for a user device to communicate over the network, access and use other devices on the network such as printers, and possibly to access various database and other information resources on the network, such as e-mail. In order to ensure the security of a network, only authorized network users and devices should be permitted to obtain access to network resources.

Network interfaces on network devices have a unique machine identifier, for example, a media access control (MAC) address. When the end user device registers in the network, certain rights, services, resources, etc., may be assigned to the end user device and associated with the unique machine identifier. Thus, when the end user device accesses the network, the end user device has access to those rights, services, resources, etc., that are assigned to and associated with the unique machine identifier of the end user device.

BRIEF DESCRIPTION OF THE DRAWINGS

Features of the present disclosure are illustrated by way of example and not limited in the following figure(s), in which like numerals indicate like elements, in which:

FIG. **1** shows an example functional block diagram of an environment in which a network device for managing access to a network by a user device may be implemented, according to an example of the present disclosure;

FIG. **2** depicts an example flow diagram of a method for managing access to a network, according to an example of the present disclosure;

FIG. **3** depicts an example flow diagram of a method for enabling a user to self-register a user device into a database of authorized users to access a network, according to an example of the present disclosure;

FIG. **4** depicts an example flow diagram of a method for ongoing management of a user and user device already granted access to a network, according to an example of the present disclosure;

FIGS. **5**A-**5**B depict an example flow diagram of a method for determining whether to permit registration of a user device to a network, according to an example of the present disclosure;

FIG. **6** depicts an example flow diagram of a method for determining whether to grant access to a network, according to an example of the present disclosure;

FIG. **7** depicts an example database of authorized users, according to an example of the present disclosure;

FIG. **8** depicts an example flow diagram of a method for performing a re-verification process, according to an example of the present disclosure; and

FIG. **9** illustrates an example schematic representation of a computing device, which may be employed to perform various functions of devices depicted in FIG. **1**, according to an example of the present disclosure.

DETAILED DESCRIPTION

For simplicity and illustrative purposes, the present disclosure is described by referring mainly to an example thereof. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be readily apparent however, that the present disclosure may be practiced without limitation to these specific details. In other instances, some methods and structures have not been described in detail so as not to unnecessarily obscure the present disclosure. As used herein, the term "includes" means includes but not limited to, the term "including" means including but not limited to. The term "based on" means based at least in part on.

Given a network of resources, communication devices such as personal computers, PDAs, cell phones, laptops, and similar devices may frequently join and leave a network. A network may include switches, routers, servers, desktops, databases, etc., which may provide services like internet access, access to services e.g., e-mail, etc. Network security plays important role in determining which device is authenticated to join the network and which resources it is authorized to access. Establishing, maintaining, monitoring and controlling network access rights, has become a daunting task for a network administrator. Existing network access solutions may be too complex to adopt, or time consuming, or most of the features of the solution may not be put to optimal use. Once users and user devices are registered and authorized to access a network and network resources, it is difficult to detect when an authorized device has been spoofed by an unauthorized device and/or user, thereby leaving the network and network resources open to non-authorized users.

Disclosed herein are methods and apparatuses for managing access to a network that requires a substantially minimal amount of administrative overhead. In other words, the methods and apparatuses disclosed herein substantially remove the need for large IT staffs or external consultants. The network access control (NAC) implementation disclosed herein is referred to as Simplified Network Access Control (SNAC), but other names may be employed as well. As disclosed herein, SNAC may simplify NAC for both the client (end user) and the system and/or domain administrators. According to an example, SNAC may simplify NAC for clients by providing a client service portal for self-registration, which allows clients to register for access to the network with the appropriate access rights and quality of service. In addition, SNAC may simplify NAC for the administrator as well, by substantially removing the need for learning and mastering a number of external technologies:

Does not need to become an expert in RADIUS servers.

Does not need to become an expert in directory services (e.g. Active Directory).

Does not need to become an expert in 802.1X technology.

Additionally, in at least some NAC implementations, the administrator is typically required to perform the initial and ongoing maintenance of all the clients that want access to the network. Typically, there is an initial bulk configured process, followed by ongoing updating (adding new clients, deleting old clients, updating clients for changes to access rights). The SNAC implementation disclosed herein removes this burden from the administrator through the self-registration capability and automated updating of the users' access rights. In addition, through use of a separate database of authorized users, the SNAC implementation disclosed herein enables for net-

work access control to be based upon information contained in the directory of active network users, such as, the Active Directory, without making changes to the Active Directory. Further, through the use of certificates that are generated based on a MAC address of a user device, an additional level of security may be provided to avoid spoofing devices from gaining access to the network.

Once a user is registered, a re-verification process may be implemented whereby the user is requested to re-verify the user's credentials, thereby maintaining security in the network by ensuring that only authorized users have access to the network and the network resources.

According to an example, the user self-registration operation disclosed herein enables the user to self-populate the database of authorized users if the user is able to be verified in the directory of active network users. The active network users contained in the directory of active network users are users who exist in the existing Domain. In this regard, the active network users have been granted access rights to the network, whether or not those access rights are actually being exercised by the active users, that is, whether or not those users have user devices connected to the network. A user is typically understood to be a person, though a user may be some other kind of entity. A user device is typically understood to be an electronic computer or computing device, or other electronic information device, and/or a communications device, such as a cell phone. Other types of electronic devices pertaining to data or information processing, such as printers or PDAs, may be user devices as well.

The directory of active network users includes data of the types typically used to define and authorize a user who may be allowed network access. Such information may include, for example and without limitation, a user name, a user company, a user group or department, a user e-mail address, a user password, a user phone number, and similar information pertaining to the user. The list of authorized users is to include data of a type typically used to define and authorize a user, at least some of which may overlap with the data type(s) listed in the directory of active network users. Such overlapping data may include, for example and without limitation, a user name, a user company, a user group or department, and similar information.

The list of authorized users is also to include user device information for computing devices, data processing devices, communications devices, and similar devices which a user may use. The user device information may include, for example and without limitation, a MAC (media access control address) for a device, or a port connection identification for a device. For each user in the list of authorized users, associated user device information, such as MAC address(es), may be listed as well, indicating the hardware device(s) is/are associated with the user.

A user device may be physically coupled to the network, for example through a network switch. At substantially the same time that the user device is coupled to the network, the network receives from the user device the user device information, for example, a MAC address, through an automated device handshake process. If this user device information is currently listed in the list of authorized users, the user device is considered authorized and is granted access to the network. However, if the user device information is not listed in the list of authorized users, the user may be presented with an interface for entry of user self-registration information. The interface may be a graphical user interface, and may be presented via the user device, which has been coupled to the network, but may be presented via other devices as well. The user interface presents data fields or other sections for the entry of user information including, for example and without limitation, a user name, a user password, a user company, a user group, and similar information.

According to an example, a network device receives the user self-registration information and determines whether the user self-registration information is listed in the directory of active network users. If the user is listed in the directory of active network users, the hardware self-identification information is listed in the list of authorized users. A public/private key pair may be generated, where the MAC address of the user device is included in the public key, for example, embedded in the certificate extension of the certificate, and the user device is granted network access. Upon future access requests to the network from the user device, the MAC address may be determined from the public key provided to the network device, and compared with the stored MAC address. If the two MAC addresses match, access may be provided to the network device.

Further, a real-time monitor may be maintained on the directory of active network users and any changes made by system and/or domain administrators to the directory of active network users may automatically result in appropriate changes to the list of authorized users, and to network access for the associated devices listed in the list of authorized users. This further simplifies network access security and control for system and/or domain administrators.

In one or more examples, once a user is registered, a re-verification timer may be set and stored in a database, e.g., the database of authorized users. Upon expiration of the re-verification timer, e.g., the re-verification timer times out, the user is requested to re-verify the user's credentials, thereby maintaining security in the network by ensuring that only authorized users have access to the network and the network resources.

Alternatively, once the user is registered, an agent may be selected, based on the type of user device, and transmitted to the user device for installation. Upon installation, the agent may be in communication with the network, thereby ensuring that the registered device is the user device that is authorized to access the network.

With reference to FIG. **1**, there is shown a functional block diagram of an environment **100**, in which a network device for managing access to a network **110** by a user device **106** may be implemented, according to an example. It should be readily apparent that the diagram depicted in FIG. **1** represents a generalized illustration and that other components may be added or existing components may be removed, modified or rearranged without departing from a scope of the environment **100**.

FIG. **1** depicts a system **102**, which may be referred to as a Simplified Network Access Control (SNAC) system, but other names may be employed as well. The system **102** is depicted as including a network switch **108**, an Identity Driven Manager (IDM) server **120** for hosting IDM modules (not shown), and a SNAC registration server **122** for hosting SNAC modules (not shown). In addition, the SNAC registration server **122** is depicted as being in communication with a certificate authority **160**, an Active Directory (AD) **136** and a guest directory **142**. The network switch **108** is also depicted as being in communication with a network **110**, which may include network servers and devices.

FIG. **1** also depicts a user device **106**, also known as a client or network client **106**. User devices **106** are used by users **104**, who are people or other entities seeking to log into and access the network **110**. A user **104** seeking to utilize resources of a network **110** will connect their user device **106** to the switch **108** or other connection element, such as a wireless access

point (not shown). Associated with the user **104** is user information **104**UI. Associated with the user device **106** is user device information **106**DI.

The switch **108** is depicted as communicating with a Remote Authentication Dial In User Service (RADIUS) server **112**, in which the switch **108** operates as a RADIUS client. More particularly, the RADIUS server **112** may employ RADIUS, which is a networking protocol that provides authentication, authorization, and accounting management for network access, for instance, as described in RFC 2865 and 2866. In addition, the switch **108** may operate as a RADIUS client to the RADIUS server **112**. The RADIUS server **112** is also depicted as being in communication with a database of authorized users **128**, which may host a list of authorized users **130**. An example list of authorized users **130** is depicted in FIG. **1** to include fields for a user name, a MAC address, a user group, and other information. The Database of Authorized Users may be more fully discussed with regard to FIG. **5**. According to an example, a user device **106** attempting to gain access to the network **110** may be denied access to the network **110** unless the user device information **106**DI of the user device **106** is listed in the list of authorized users **130**.

An IDM agent **116**, which provides management for an IDM policy database **124**, is also depicted as being in communication with the database of authorized users **128**. In addition, the IDM agent **116** is depicted as being in communication with the IDM server **120**, which may host an IDM policy database **124**. The IDM policy database **124** may contain a variety of tables and data defining user access rights and user access policies for various network users **104** and user devices **106**.

According to other examples, the RADIUS server **112** and/or the IDM agent **116** may be hosted on the switch **108** or hosted on the IDM server **120**, or on a combination of both. In addition, or alternatively, the RADIUS server **112** and/or the IDM agent **116** may be hosted on the SNAC registration server **122**. As a further example, the IDM server **120** and the SNAC registration server **122** may comprise a common server and the RADIUS server **112** and/or the IDM agent **116** may be hosted on the common server.

The Active Directory **136** is depicted as including a directory table of active network users **138**. The Active Directory **136** may be populated by an administrator, and functions to list users who are currently considered as having an active or valid association with a network **110**. An example Active Directory table **138** is depicted in FIG. **1**, which may have at least one data field or data type in common with the list of authorized users **130**, or may have pointers or similar arrangements, to associate users **140** in the Active Directory table **138** with users **132** in the list of authorized users **130**. In FIG. **1**, the list of authorized users **130** and the Active Directory table **138** have in common two user fields **104**UI, the User field and the Group field. In this way, it is possible to identify in the Active Directory table **138** a user who may potentially be listed for entry in the list of authorized users **130**.

In FIG. **1**, for example, both Jane Doe **132** and Jane Doe **140** are the same user listed in the respective list of authorized users **130** and the Active Directory table **138**. The Active Directory table **138** may also include additional identifying information, which may be used to validate a user during a self-registration or login process. For example, the Active Directory table **138** is depicted as containing a password field, which may in part contribute to verifying a user who is attempting to access the network **110**. The Active Directory table **138** may also contain a field or flag to indicate if a user listing is currently enabled. If enabled, the user is allowed network access. If disabled, the user is denied network access. This may be used to temporarily disable network access without a need to delete all user information **104**UI. Other fields and flags (not shown) may also be employed to determine other aspects of network access for a user or user group.

According to an example, the switch **108** may be a conventional switch, which is not configured to host or support the RADIUS server **112** or the IDM agent **116**. In such a case, the RADIUS server **112**, the database of authorized users **128**, and the IDM agent **116** may all be hosted on the SNAC registration server **122** and/or the IDM server **120**. In an alternative example, the RADIUS server **112**, the IDM agent **116**, the database of authorized users **128**, and the IDM policy database **124** may all be hosted on the switch **108**. Therefore, the system **102** as depicted in FIG. **1**, including the switch **108**, the SNAC registration server **122**, the IDM server **120**, may instead include one of the switch **108**, the SNAC registration server **122**, or the IDM server **120** without the other components.

It may further be appreciated that certificate authority **160** may be hosted on the SNAC registration server **122**, for example, managed by the same entity that manages the SNAC registration server, or may be a separate server remote from the SNAC registration server **122** that is managed by a different entity that manages the SNAC registration server **122**.

It should be further noted that the boundaries of the system **102**, as suggested by the outlined area in FIG. **1**, are example boundaries only. For example, the Active Directory **136** and/or the Guest Directory **142** may be considered part of the system **102**.

Various manners in which a simplified network access control management operation may be implemented are discussed with respect to the methods **200**-**600** and **800**, respectively depicted in FIGS. **2**-**6** and **8**. It should be readily apparent that the methods **200**-**600** and **800** depicted in FIGS. **2**-**6** and **8** represent generalized illustrations, and that other processes may be added or existing processes may be removed, modified or rearranged without departing from the scope and spirit of the methods **200**-**600** and **800**.

Generally speaking, the various operations depicted and discussed with respect to FIGS. **2**-**6** and **8** may be implemented by at least one of the components of the system **102** depicted in FIG. **1**. Thus, for instance, the switch **108**, the SNAC registration server **122**, or the IDM server **120**, or a combination of these components may implement each of the operations depicted in FIGS. **2**-**6** and **8**. In this regard, the methods **200**-**600** and **800** may comprise machine-readable instructions stored on any one or more of the switch **108**, the SNAC registration server **122**, the IDM server **120**, and a combination of these components. In addition, or alternatively, the methods **200**-**600** and **800** may comprise machine-readable instructions stored on a non-transitory computer readable storage medium that is implemented or executed by any one or more of the switch **108**, the SNAC registration server **122**, the IDM server **120**, and a combination of these components.

With reference first to FIG. **2**, there is shown a flow diagram of a method **200** for managing access to a network **110**, according to an example. At block **202**, a user **104** is enabled to self-register a user device **106** into a database of authorized users **128** to access the network **110** in response to the user **104** being listed as a valid user in a directory of active network users **136**, **142**. According to an example, the self-registration is enabled through a MAC based authentication operation. Various manners in which the self-registration operation may be implemented are described in greater detail herein below with respect to the method **300** in FIG. **3**.

At block **204**, the directory of active network users **136**, **142** is monitored for modification of information pertaining to the users listed in the directory of active network users **136**, **142**. As discussed above, the directory of active network users may comprise one or both of the active directory **136** and the guest directory **142**. In addition, various manners in which the directory of active network users **136**, **142** may be monitored are described in greater detail herein below with respect to the method **400** in FIG. **4**.

At block **206**, the database of authorized users **128** is modified in response to a determination that the user information pertaining to at least one user listed in the directory of active network users **136**, **142** that affects the database of authorized users **128** has been modified. Various manners in which the database of authorized users **128** maybe modified based upon modifications to the directory of active network users **136**, **142** that affect the user information contained in the database of authorized users **128** are also described in greater detail herein below with respect to the method **400** in FIG. **4**.

Turning now to FIG. **3**, there is shown a flow diagram of a method **300** for enabling a user to self-register a user device into a database of authorized users **128** to access the network **110**, according to an example. The method **300** generally comprises a more detailed description of the operations that may be performed at block **202** in FIG. **2**.

At block **302**, user device information **106**DI of the user **104** requesting access to the network **110** is received. The user device information **106**DI may be, for instance, the MAC address of the user device **106**. In addition, the user device **106** may automatically communicate the user device information **106**DI to the switch **108** when the user device **106** is coupled to the switch **108**, for instance, during a handshake operation between the switch **108** and the user device **106**.

More generally, the user device information **106**DI may comprise a set of data associated with the user device **106** and may serve to uniquely identify the user device **106** to the network **110**. In some cases, redundant or additional information may be employed, or added, in order to further identify the user device **106** or to limit, control, or constrain the association of the user device **106** with the network **110**. For example, a port identifier on the switch **108** may be combined with the MAC address of the user device **106** to form a combined or multi-signature user device information **106**DI. Similarly, a specific frequency or channel may be associated with a wireless device in order to form a combined or multi-signature user device information **106**DI. In some cases, however, some leeway may be granted in assigning a user device information **106**DI. For example, a wireless user device **106** may still be granted access to the network **110** if it is associated with two or more wireless access points (that is, wireless switches **108**), provided those multiple access points are substantially in proximity to each other.

At block **304**, a determination as to whether the database of authorized users **128** includes the user device information **106**DI is made. As shown in FIG. **1**, and according to an example, the switch **108** is to implement the RADIUS server **112** ("MAC-AUTH" line) in making the determination as to whether the database of authorized users **128** includes the user device information **106**DI. Alternatively, however, the SNAC registration server **122** and/or the IDM server **120** may make this determination.

In response to a determination that the database of authorized users **128** does include the user device information **106**DI, access to the network **110** is granted to the user **104** through the user device **106**, as indicated at block **306**. Specific access and control rights may be determined by IDM agent **116** in conjunction with IDM policy database **124**. However, if a determination that the database of authorized users **128** does not include the user device information **106**DI, at block **308**, user information **104**UI is received. More particularly, for instance, the user **104** may be prompted to input the user information **104**UI, such as, a user name, user identification, password, and/or other credentials, and the user **104** may input the requested user information **104**UI. In addition, the switch **108** may redirect the user information **104**UI to the SNAC registration server **122** as indicated by the line labeled "MAC-AUTH-FAILURE-REDIRECT".

At block **310**, a determination as to whether the user information **104**UI is valid in the directory of active network users **136**, **142** is made, for instance, by the SNAC registration server **122** following receipt of the user information **104**UI. Thus, for instance, a determination as to whether the user information **104**UI is contained in the directory of active network users **136**, **142** is made and if so, whether the user **104** has inputted the correct credentials, for instance, the correct password, and is enabled to access the network **110** is made. By way of example, and as shown in FIG. **1**, the active directory table **138** contained in the active directory **136** shows that the user "Jane Doe" is enabled to access the network **110** and that here password is "123RF34". It will be noted that the Active Directory **136**, Guest Directory **142**, or similar directories of active network users are typically populated, maintained, and updated by an authorized administrator or other person(s) responsible for ensuring legitimate network access. For example, an authorized organizational staff member may be designated to populate Guest Directory **142** with names and other identifying information **104**UI for network users **104** who will be guests, and who will therefore be permitted guest or temporary access to the network **110**.

In response to a determination that the user information **104**UI supplied by the user at block **308** is invalid, access to the network **110** is denied as indicated at block **312**. Thus, if the user information **104**UI is not contained in the directory of active network users **136**, **142**, if the user information **104**UI, for instance, the password, does not match the user information **104**UI contained in the directory of active network users **136**, **142**, and/or if the user's **104** network access has been disabled, access to the network is automatically denied at block **312**. In addition, suitable additional steps may be taken. For example, a user **104** may prompted to re-enter user information **104**UI (on the possibility that the information was entered incorrectly a first time), or an alert may be sent to an administrator or designated organizational administrator. Policies for responding to an incorrect or erroneous user information **104**UI may be defined in IDM policy database **124**, and implemented by processes such as RADIUS server **112** and/or IDM agent **116**.

In response to a determination that the user information **104**UI supplied by the user at block **308** is valid, the user information **104**UI is registered into the database of authorized users **128**, as indicated at block **314**. In other words, the user information **104**UI is automatically populated into the list of authorized users **130** in the database of authorized users **128**. In this regard, the user **104** may be granted access to the network **110** through the user device **106** without requiring the direct support or intervention of an administrator. From the perspective of the user **104**, the self-registration operation of the method **300** may be implemented via a log-in process and log-in displays.

In addition, along with the user information **104**UI, and associated with it, is added the user device information **106**DI for the device **106**. If the user **104** is already present in the list of authorized users **130** (indicating another user device **106** is already associated with the user **104**), then newly added

device **106** and its user device information **106**DI may also be associated with the same user **104**. In an example, when the user information **104**UI is added to the list of authorized users **130**, all of the provided user information **104**UI is added. In another example, when the user information **104**UI is added to the list of authorized users **130**, only a subset of the user information **104**UI is added.

In addition, the user **104** is granted access to the network **100** as indicated at block **306**, which has been described herein above.

By way of particular example, once the user's credentials are verified and the user **104** is determined to be a valid user at block **310**, the SNAC registration server **122** adds the user information **104**UI to the IDM server **120**. In addition, the IDM server **120** pushes the user information **104**UI to all of the IDM agents **116**. An IDM agent **116** registers the user information **104**UI into the database of authorized users **128** as discussed above. Subsequent access to the network **110** through the user device **106** will now occur automatically as the user **104** is immediately allowed access with the appropriate access rights based on the their IDM group, profile, etc. In addition, from this point forward, the user **104** is unaware that SNAC is being implemented since the user's **104** access to the network **110** through the user device **106** is transparent to the user **104**. As discussed in greater detail below with respect to the method **400** in FIG. **4**, when the user's access rights changes, such as, when the user leaves a company, that change is automatically reflected in the database of authorized users **128** since the IDM server **120** is monitoring the directory of active network users **136**, **142** for changes.

With reference now to FIG. **4**, there is shown a flow diagram of a method **400** for ongoing management of a user **104** and user device **106** already granted access to a network **110** as per the method **200** discussed above. The method **400** generally comprises a more detailed description of the operations that may be performed at blocks **204** and **206** in FIG. **2**. In this regard, the method **400** may be implemented following implementation of block **202**. In addition, the method **400** may involve a single process, or may involve multiple processes occurring substantially in parallel or in alternating sequence. FIG. **4** depicts two processes. According to an example, the SNAC registration server **122** and/or the IDM server **120** implements various operations in the method **400**.

In a first process starting at block **402**, the directory of active network users **136**, **142** is monitored in substantially real time, on a substantially continuous or frequent basis. At decision block **404**, a determination is made as to whether a user **104** has been deleted from the directory of active network users **136**, **142**. Such a deletion may be made by an administrator or other person or entity authorized to control access to the network **110**.

If a user **104** has been deleted, at block **406**, any record or similar listing of the user **104** in the database of authorized users **128** is deleted, as is the listing of any associated user device information **106**DI from the listing of authorized users **130**. This effectively prevents these user devices **106** from logging into the network **110** in the future, as per methods **200**/**300** discussed above. In addition, if any of the deleted user devices **106** are currently connected to the network **110**, their network connection may be terminated.

If, however, at decision block **404**, a determination is made that the user **104** is still listed in the directory of active network users **136**, **142**, at block **408**, a determination is made if the user **104** has been disabled in the directory of active network users **136**, **142**. Such a status may be set by an administrator or other person or entity authorized to control access to the network **110**.

If a user **104** has had their activity status set to disabled, at block **410**, a determination is made if any user devices **106** for the user **104** are currently contained in the database of authorized users **128**. If yes, at block **412**, and according to an example, if any such user devices **106** currently have active network connections, their network connection is terminated. In addition, the user information **104**UI and user device information **106**DI are deleted from the list of authorized users **130** contained in the database of authorized users **128**. In another example, instead of the user information **104**UI and user device information **106**DI being deleted from the database of authorized users **128**, a flag may be set in the list of authorized users **130** indicating that the user device(s) **106** are not currently authorized to access the network **110**. This may prevent the user devices **106** from being logged into the network **110** during the method **200** and may trigger the self-registration process of the method **300**. If, however, at block **410**, the user **104** is not listed in the database of authorized users **128**, then no specific action is required with respect to the database of authorized users **128**, and monitoring continues as per block **402**.

If at decision block **408**, a determination is made that a user **104** remains active in the directory of active network users **136**, **142**, at block **414**, a determination is made as to whether any other aspects of parameters for the user **104** have been changed in the directory of active network users **136**, **142**. If yes, at block **416**, appropriate changes are made to the database of authorized users **128**, and user device **106** network access or network privileges may be modified as appropriate. For example, network access privileges may be increased or decreased, access domains changed, network control authority changed, and other changes made as appropriate. Some changes may be determined based on changes in the directory of active network users **136**, **142** in conjunction with policies set in IDM policy database **124**, as appropriate.

In an example second process starting at block **418**, a user time limit and/or date limit set in the directory of active network users **136**, **142** is noted, and the appropriate time and or date is monitored. For example, a date limit may indicate that a user **104** is only entitled to access to the network for a specific date, such as May 1. The current date is determined, as well as whether or not the corresponding user device **106** is in use.

At decision block **420**, a determination is made if the user time limit or user date boundaries have been exceeded. If yes, then at block **422** network access through the user device **106** is terminated by removing the user information **104**UI and the associated user device information **106**DI are deleted from the list of authorized users **130** in the database of authorized users **128**, preventing future logins through the user device **106**.

It may be appreciated that, in some embodiments, alternative to removing the user and associated devices from the database of authorized users and terminate/deny network access, the user and associated devices may be put into a less privileged access profile or group.

In general, the methods **200**-**600** and **800** may be implemented to determine if more than one user device **106** with a same user device information, or a single device with an erroneous user device information, attempts to connect to the network **110**. In such cases, an alert may be sent to an administrator indicating that an attempt at device spoofing may be in progress, and one or more user devices **106** may be denied access or have existing access challenged. Specific policies to detect spoofing and other erroneous self-identifications may be defined on IDM policy database **124**, and implemented by IDM agent **116**.

Some or all of the operations set forth in the methods **200-600** and **800** may be contained as a utility, program, or subprogram, in any desired computer accessible medium. In addition, the methods **200-600** and **800** may be embodied by computer programs, which may exist in a variety of forms both active and inactive. For example, they may exist as machine-readable instructions, including source code, object code, executable code or other formats. Any of the above may be embodied on a computer readable storage medium.

Examples of non-transitory computer readable storage media include conventional computer system RAM, ROM, EPROM, EEPROM, and magnetic or optical disks or tapes. Concrete examples of the foregoing include distribution of the programs on a CD ROM or via Internet download. It is therefore to be understood that any electronic device capable of executing the above-described functions may perform those functions enumerated above.

FIGS. **5**A-**5**B depicts an example flow diagram of a method **500** for registering a user device. As shown in FIGS. **5**A-**5**B, a server may receive information related to a user **502**, for example, a user name, password, etc. The received information is verified with user information stored, as noted above, to determine if the received user information is correct **504**. If the user information is not correct (**504**, NO), then access to the network is denied **506**. If the received information is verified (**504**, YES), additional information is received **508**. This information may be received from an active directory, as discussed above. Additional information may be received at the server from the user device, for example the MAC address of the user device **510**. The server may determine whether the received MAC address is stored in the database **512**. If the MAC address is present in the database of authorized users (**512**, YES), then access to the network is denied **506**. If the MAC address is not present in the database (**512**, NO), then the server registers the user information in the database of authorized users **514**.

A public/private key pair is generated by the certificate authority based on the MAC address of the user device **516**. As discussed herein, the public/private key pair may be, for example, asymmetric keys such that information that is encrypted by one key can be decrypted only by the other key. The certificate authority may generate, for example, an X.509 digital certificate containing the public key. In the certificate extension, the certificate authority may embed the MAC address of the user device. The domain user name may further be the subject name of the certificate. By providing the MAC address in the certificate and the domain name user as the subject name, the user identity is bound to the MAC address of the user device.

The MAC address is stored in the database **518**, for example, associated with the access policy group to which the active directory domain the user belongs. The generated key pair is transmitted to the user device **520**. The key pair may be transmitted, for example, in the form of a .pfx file to the user device with a "registration success" message.

It may be appreciated that the registration server may allow the user device to generate the key pair. Along with the success message, the registration server may also give an option to the user to download and install an agent software on the user device, for example, ActivClient Agent from ActiveIdentity Inc., Cisco Trust Agent from Cisco, Inc., etc. The private key may be stored on the user device, on external storage, etc.

FIG. **6** depicts an example flow diagram of a method **600** for determining whether a user and a user device are permitted access to a network. As shown in FIG. **6**, the certificate and digital signature are received from a user device requesting access to the network **602**. The digital signature is analyzed to determine if it is a valid digital signature of the user requesting access to the network **604**. If the digital signature is not valid (**604**, NO), access will be denied to the user device. If the digital signature is valid (**604**, YES), then the MAC address is determined from the certificate **606**. In addition, the MAC address of the user device requesting access to the network is determined **608**. In one example, the MAC address may be retrieved from the RADIUS attribute calling-station-id in the form of an access-request message per RFC 2865/2866 sent by the switch to the RADIUS server. The MAC address from the certificate is compared with the MAC address of the user device requesting access to the network (**610**). If the MAC addresses match (**610**, YES), access may be granted to the network **612**. If the MAC addresses do not match (**610**, NO), access may be denied. If access is denied, an event may be triggered reporting an improper access to the network was attempted. This event may be an alert, a message to one of the servers in the system, etc.

It may be appreciated that, according to one or more examples discussed herein, additional checks may be performed to ensure the user and/or user device is authorized to access the network. For example, additional steps may be taken to extract the subject name from the certificate, and compare the extracted name with the user name associated with the MAC address from the policy database. If the names do not match, then access may be denied. Additionally or alternatively, the issuer of the certificate may be checked to determine if the issuer is a trusted authority, based on a comparison of a list of stored trusted authorities. If the issuer is not a trusted authority, access may be denied. Additionally, or alternatively, the certificate may be checked to determine if it is valid with respect to status and/or expiry. If the status is not valid, or the certificate expired, access may be denied.

It may be appreciated that the process described, for example, with respect to FIG. **6** may be implemented utilizing different protocols. For example, within the context of IEEE 802.1x port-based network access control, an authentication mechanism is provided. An agent may be installed on the user device to facilitate communication between the user device and one or more servers in the network. When a user device is connected to a switch port, the user device sends a connection request to a switch. The switch may send an extensible authentication protocol (EAP) EAP-request message to the user device where the user devices supplies user device identifying information to the switch. The switch sends the user device identifying information to the RADIUS server in the form of, for example, a RADIUS access request packet. The RADIUS server may send a RADIUS access-challenge packet to the switch to start a EAP-TLS (transport layer security) handshake process. The user device may transmit a ClientHello message to the RADIUS server. The RADIUS server may reply with a ServerHello, its digital certificate, ServerKeyExchange, a request to the user device to supply its digital certificate, and the ServerHelloDone. The user device verifies the server's certificate. The user device sends its digital certificate along with other information, for example, the ClientKeyExhange, CertificateVerify, ChangeCipherSpec, and TLSFinished. The RADIUS server may verify the user device's certificate and digital signature. The MAC address may be determined from the certificate and the user device's identity may be verified as the user device that is authorized to access the network. If the MAC address was spoofed by another device, the credentials from the digital certificate and the MAC address embedded in the certificate would reveal that a spoofing device is attempting to gain access to the network. Also, the digital signature generated

using a spoofing device's private key cannot be decrypted by the legitimate user's public key thereby failing the digital signature verification.

In another example, MAC authentication may be utilized. After the user device has successfully registered, the registration server may provide agent software to be downloaded and installed on the user device. The user device may install the agent software. The agent software may capture information of the user device, for example, MAC address, digital certificate, the digital signature, etc. As the device is successfully registered through registration (after verifying its domain credentials against Active Directory), the user device is provided network access using MAC authentication where only the MAC address is sent to the authentication/RADIUS server in the access request. The information of the user device such as the switch's IP to which it is connected, port to which the user device is connected, device's MAC address, the session information like Session ID, etc. is stored in the policy database. The authentication server sends a request message to the agent running on the user device for further identity information. This may be accomplished, for example, by sending a CoA (Change of Authorization) message per RADIUS protocol extension—RFC 3576 (superseded by RFC 5176) to the switch/user device. Alternatively, the registration server may send an event message to the user device requesting for further identity information without using RFC 3576. The agent running on the user device then responds with the digital signature, MAC address, digital certificate, etc. The RADIUS server or the registration server may execute the method described in FIG. **6**, where, in step **608**, the MAC address is provided via the agent software running on the user device.

It may be appreciated that when the user registered the user device through registration process as discussed herein, its domain name/user name was stored in the policy database. It may be compared against the subject name field in the digital certificate. This may be used to confirm that device is used by the legitimate user.

In one example, if the agent software is not installed on the user device, and the agent software is required to be installed on the user device, then access to the network may be terminated as the message request from the server will not obtain any response from the user device.

By providing for verification of a digital signature and the validation of the MAC address as discussed herein, the identity of the user and the user device may be confirmed as legitimate. If a MAC address is spoofed by a spoofing device, the spoofing device may not have access to the private key of the legitimate user. Thus, even if a spoofing device spoofs a MAC address of a legitimate user device, as discussed herein, the MAC address present in the certificate will not match the MAC address present in the RADIUS access request packet, and/or the digital signature verification will fail as the illegitimate user cannot get an access to the legitimate user's private key and will thereby reject the authentication.

FIG. **7** depicts an example database of authorized users according to an example of the present disclosure. As noted above the database of authorized users **700** may include information associated with users that are authorized to access the network. The database of authorized users may include fields for storing information associated with an authorized user. For example, the database a user name **702**, a MAC address **704**, a user group **706**, and a duration of network access **708**.

In addition, database **700** may further include a re-verification timer **710**. This re-verification timer may be set, for example, when the user is registered in the database **700**. The re-verification timer is a pre-determined time that defines when a re-verification process may be initiated where the user may be requested to supply the user credentials to the system in order to be re-verified. The re-verification timer may be set automatically, for example, based on the user group that the user belongs to; may be set based on a default value applied to all users; may be set based on access policies; may be set ad hoc by an administrator, etc. The re-verification time may decrement in coordination with the system time clock such that when the time reaches zero, the timer times out and the re-verification process is initiated. If the user is re-verified in accordance with the re-verification process, the re-verification timer may be reset to the initial time value. Alternatively, the re-verification timer may be reset to a different value as determined by, for example, a network administrator.

Database **700** may further include the date/time of the last verification **712**. This information may be used in order to determine when the re-verification process may take place.

Optionally, database **700** may further include an indication whether an agent was downloaded to the user device **714**. If the agent was downloaded to the user device, then communication between, e.g., SNAC registration server **122** and the user device **104** may be expected. For example, if the agent was downloaded to the user device, and there is no communication between the agent at the user device and the SNAC registration server, then access to the network may be denied.

It may be appreciated that the information stored in database **700** may be stored in a single database, or in multiple databases at the same device or at difference devices. It may further be appreciated that additional information related to the user and the user device may be stored in database **700**.

It may further be appreciated that, alternatively, the database **700** may store information relating to how much time is left until the re-verification process is initiated.

FIG. **8** graphically illustrates an example flow diagram of a re-verification process. When a user device sends a request for network access to the SNAC registration server, the user information and/or user device information may be compared with information stored in the database of authorized users. If the information is stored in the database of authorized users (**802**, YES), access is granted to the network **804**.

Alternatively, if the information is stored in the database of authorized users, an additional check may be made to determine if a re-verification timer is enabled. If the re-verification time is not enabled, then access may be granted to the network **804**. However, if the re-verification timer is enabled, a check may be made to determine if an agent is installed on the user device. If the agent is installed on the user device access may be granted to the network. If the agent is not installed, an appropriate agent may be selected based on the type of user device, based on a finger print process to determine the type of user device, transmitted to the user device, and the user may be prompted to install the user agent. Once the user agent is installed, the database of authorized users may be updated to indicate that the agent is installed on the user device and access may be granted to the network.

As shown in FIG. **8**, if the database of authorized users does not include the user (**802**, NO), the system accepts user credentials **806**, e.g., user name and password, these credentials will be verified against organization's Active Directory as discussed above.

If the user information is not valid in the Active Directory (**808**, NO), access to the network is denied **810**. If the user credentials are correct (**808**, YES), the registration server may process the re-verification timer **812**. The re-verification timer may be processed by determining the value of the timer, e.g., the amount of time to pass until the re-verification process is initiated. As noted above, this value may be pre-

determined, for example, based on the group the user belongs to, etc. This value may be entered into the database of authorized users and associated with the user. In addition, the date and time of the user's last verification may be entered into the database of authorized users.

A determination is made whether the re-verification timer has timed out **814** based on the time stored in the database of authorized users. If the re-verification time has not timed out (**814**, NO), then access is granted to the network **816** until the re-verification time has timed out.

If the re-verification time has timed out (**814**, YES), then a request is sent to the user device requesting the user re-verify **818**. This request may be made in a manner such that a message appears on a display, e.g., in a pop-up window, of the user device requesting the user access, for example, a Uniform Resource Locator (URL) and enter the user credentials, e.g., user name, password, etc.

If an agent is installed on the user device, the message may be transmitted to the agent, where the agent may prompt the message to appear on the display of the user device.

Once the user credentials are received, a determination is made whether the re-verification was successful, e.g., the user credentials, when compared with information stored in the database of active users, are verified. If re-verification was not successful (**820**, NO), then access to the network may be denied **810**. If re-verification is successful (**820**, YES), then access to the network is granted **822** and the process proceed to **812** where the re-verification timer is processed. It may be appreciated that the re-verification process may include the method discussed with regard to FIG. **6**.

It may be appreciated that, alternatively, after it is determined that the user information is valid in the database of active users (**808**, YES), the SNAC registration server may select, based on a fingerprinting operation to determine the type of user device, an appropriate agent may be selected, transmitted to the user device, and the user may be prompted to install the user agent. Once the user agent is installed, the database of authorized users may be updated to indicate that the agent is installed on the user device. Processing may then proceed to step **812**.

It may be appreciated that the registration server allows a user to register multiple devices at the time of registration process. In this case only the device participating in the registration process may be prompted to download the user agent. The database of registered users may be appropriately updated indicating that only the device that downloaded and installed the agent includes the agent. For all the other user devices, the agent download status will be marked as false.

It may be appreciated that, in an embodiment where the agent is installed on the user device, the agent may be in constant communication with the SNAC registration server. In one embodiment, if the communication between the user device and the SNAC registration server is discontinued, the user of the user device may be prompted to either re-verify, or access to the network may be denied. Alternatively, if the user is prompted to re-verify based on the re-verification timer timing out, a check may be made to confirm that the agent is properly communicating with the SNAC registration server. If the agent is not communicating with the SNAC registration server, access to the network may be denied.

Turning now to FIG. **9**, there is shown a schematic representation of a computing device **900**, which may be employed to perform various functions of the servers **120**, **122** depicted in FIG. **1**, according to an example. Similar elements, possibly with some elements omitted or added, may also be employed within an intelligent switch, such as switch **108** in FIG. **1**. Computing device **900** includes a processor **902**; a display device **904**, such as a monitor; a network interface **908**, such as a Local Area Network LAN, a wireless 802.11x LAN, a 3G mobile WAN or a WiMax WAN; and a computer-readable medium **910**. Each of these components is operatively coupled to a bus **912**. For example, the bus **912** may be an EISA, a PCI, a USB, a FireWire, a NuBus, or a PDS.

The computer readable medium **910** may be any suitable non-transitory medium that participates in providing instructions to the processor **902** for execution. For example, the computer readable medium **910** may be non-volatile media, such as an optical or a magnetic disk; volatile media, such as memory; and transmission media, such as coaxial cables, copper wire, and fiber optics. Transmission media can also take the form of acoustic, light, or radio frequency waves. The computer readable medium **910** may also store other machine-readable instructions, including word processors, browsers, email, Instant Messaging, media players, and telephony machine-readable instructions.

The computer-readable medium **910** may also store an operating system **914**, such as Mac OS, MS Windows, Unix, or Linux; network applications **916**; and a network access management application/key generation **918**. The operating system **914** may be multi-user, multiprocessing, multitasking, multithreading, real-time and the like. The operating system **914** may also perform basic tasks such as recognizing input from input devices, such as a keyboard or a keypad; sending output to the display **904**; keeping track of files and directories on the computer readable medium **910**; controlling peripheral devices, such as disk drives, printers, image capture device; and managing traffic on the bus **912**. The network applications **916** include various components for establishing and maintaining network connections, such as machine-readable instructions for implementing communication protocols including TCP/IP, HTTP, Ethernet, USB, and FireWire.

The network access management application **918** provides various components for managing access to a network and implementing a re-verification process, as described above with respect to the methods FIGS. **2-6** and **8**. The network access management application **818**, when implemented, receives on a network device **108/120/122** a user device identification **106**DI from a user device **106** requesting access to the network **110**. The network access management application **818**, when implemented, further enables a user **104** to self-register the user device **106** into a database of authorized users **128** in response to the user being listed as a valid user in a directory of active network users **136**, **142**. In addition, the network access management application **818**, when implemented, monitors the directory of active network users **136**, **142** for modification of information pertaining to the users listed in the directory of active network users **136**, **142**. Moreover, the database of authorized users **128** is modified in response to a determination that user information pertaining to at least one user listed in the directory of active network users **136**, **142** that affects the database of authorized users **128** has been modified. In addition or alternatively, a re-verification process may be implemented where users may be prompted to re-verify their credentials in order maintain access to the network. In certain examples, some or all of the processes performed by the network access management application **818** may be integrated into the operating system **814**. In addition, or alternatively, a public/private key pair may be generated based on a MAC address of a user device as discussed herein. In certain examples, the processes may be at least partially implemented in digital electronic circuitry, or

in computer hardware, machine-readable instructions (including firmware and/or software), or in any combination thereof.

Although described specifically throughout the entirety of the instant disclosure, representative embodiments of the present disclosure have utility over a wide range of applications, and the above discussion is not intended and should not be construed to be limiting, but is offered as an illustrative discussion of aspects of the disclosure.

What is claimed is:

1. An apparatus comprising:

a memory, storing a set of instructions; and

a processor, to execute the stored set of instructions, to:

in a registration process of a user device in a network, generate a public/private key pair based on a media access control (MAC) address of the user device;

transmit the generated public/private key pair to the user device;

receive from the user device the generated public key and a user device digital signature, the user device requesting access to a network;

verify if the digital signature is valid;

determine the MAC address from a certificate extension of the public key;

compare the determined MAC address with a MAC address of the user device requesting network access; and

provide network access to the user device if the MAC address determined from the certificate extension is the same as the MAC address of the device requesting access to the network and if the digital signature is verified as valid.

2. The apparatus of claim **1**, wherein the processor is further to transmit, to the user device, an agent for installation on the user device.

3. The apparatus of claim **2**, wherein the agent, when installed on the user device, is to facilitate communication between the apparatus and the user device.

4. The apparatus of claim **1**, wherein the processor is further to provide the MAC address of the user device to a storage device for storage.

5. A method of managing access to a network, the method comprising:

implementing a media access control based authentication operation in determining whether to grant a user device of a user access to the network;

enabling the user to self-register the user device into a database of authorized users to access the network in response to the user being denied access to the network through the MAC based authentication operation and being listed as a valid user in a directory of active network users;

receiving a MAC address of the user device;

generating a public/private key pair for the user, the MAC address of the user device being embedded in the public certificate extension; and

transmitting the generated public/private key pair to the user device.

6. The method of claim **5**, further comprising:

storing the MAC address in association with the user, in a storage.

7. The method of claim **5**, further comprising:

setting a re-verification timer based on information associated with the user device in the database of authorized users.

8. The method of claim **7**, further comprising:

determining the re-verification timer has timed out; and

initiating a re-verification process to re-verify the user of the user device.

9. The method of claim **8**, wherein the re-verification process includes:

requesting reverification of the user at the user device for access to the network;

receiving a response to the request from the user device including a digital signature of the user and the public key; and

determining the digital signature is valid;

determining the MAC address embedded in the certificate extension of the public key;

comparing the determined MAC address from certificate extension with the MAC address of the user device requesting access to the network;

providing access to the user device if the determined MAC address from the certificate extension is the same as the MAC address of the user device requesting access to the network and the digital signature is valid; and

resetting the re-verification timer.

10. A non-transitory computer readable storage medium on which is embedded a computer program, said computer program implementing a method, said computer program comprising computer readable code to:

receive, from a user device requesting access to a network, a public key and a digital signature, the public key including a media access control (MAC) address;

verify if the digital signature is valid;

determine the MAC address from the public key;

compare the determined MAC address with a MAC address of the user device requesting access to the network; and

provide network access to the user device if the MAC address determined from the public key is the same as the MAC address of the user device requesting access to the network and if the digital signature is valid.

11. The non-transitory computer readable storage medium of claim **10**, the computer readable code to further:

in a self-registration process of a user device in a network, generate a public/private key pair based on the media access control (MAC) address of the user device;

transmit the generated public/private key pair to the user device, wherein the public/private key is to facilitate network access by the user device; and

provide the MAC address of the user device, associated with the user, to a storage device.

12. The non-transitory computer readable storage medium of claim **10**, the computer readable code to further:

set a re-verification timer based on information associated with the user device in the database of authorized users.

13. The non-transitory computer readable storage medium of claim **12**, the computer readable code to further:

determine the re-verification timer has timed out; and

initiate a re-verification process to re-verify the user of the user device.

14. The non-transitory computer readable storage medium of claim **13**, the computer readable code to further:

transmit to the user device a request for user credentials;

receive a response to the request, the response including user credentials including a digital signature and the public key;

determine the MAC address from the public key;

compare the determined MAC address with the MAC address of the user device reverifying;

if the MAC address from the public key and the MAC address of the user device reverifying match, continue to provide access to the network;

if the received credentials do not match the credentials stored in the database of authorized users, deny access to the network; and

reset the re-verification timer.

15. The non-transitory computer readable storage medium of claim **10**, the computer readable code to further:

extract a subject name from public key;

compare the extracted subject name with a user name associated with the MAC address;

deny access of the names do not match based on the comparison; and

grant access if the names match based on the comparison.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,270,454 B2
APPLICATION NO. : 13/600318
DATED : February 23, 2016
INVENTOR(S) : Kamat Maruti et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

In column 18, line 3, in Claim 9, delete “reverification” and insert -- re-verification --, therefor.

Signed and Sealed this
Twenty-first Day of June, 2016

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office