



- (51) **International Patent Classification:**
H04L 29/06 (2006.01) *H04W 12/08* (2009.01)
- (21) **International Application Number:**
PCT/US2015/038239
- (22) **International Filing Date:**
29 June 2015 (29.06.2015)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/018,956 30 June 2014 (30.06.2014) US
14/753,146 29 June 2015 (29.06.2015) US
- (71) **Applicant:** UNISYS CORPORATION [US/US]; 801 Lakeview Drive, Suite 100, Blue Bell, PA 19422 (US).
- (72) **Inventors:** JOHNSON, Robert, A.; 2476 Swedesford Road, Malvern, PA 19355 (US). TROCKI, James; 2476 Swedesford Road, Malvern, PA 19355 (US). VALL-EVAND, Mark, K.; 2476 Swedesford Road, Malvern, PA 19355 (US). RAJCAN, Steven, L.; 2476 Swedesford Road, Malvern, PA 19355 (US).
- (74) **Agent:** GREGSON, Richard, J.; Unisys Corporation, 801 Lakeview Drive, Suite 100, Blue Bell, PA 19422 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) **Title:** SECURE NETWORK COMMUNICATIONS IN A MOBILE DEVICE OVER IPSEC

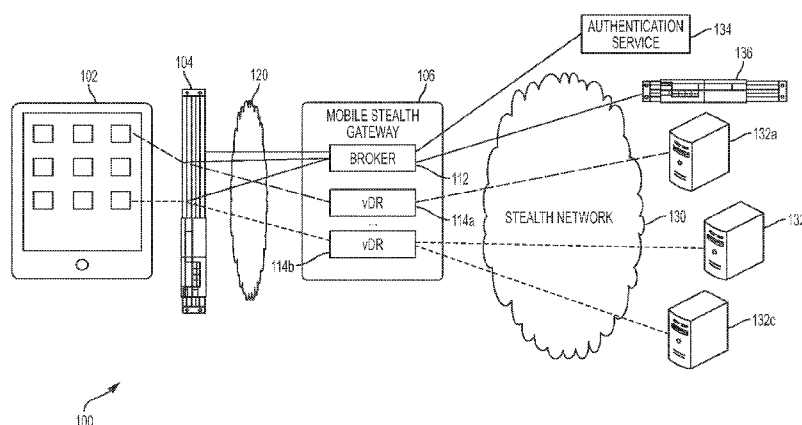


FIG. 1A

(57) **Abstract:** Methods and systems of communicating with secure endpoints included within a secured network from a mobile device external to the secured network is disclosed. The method includes initiating a VPN-based secure connection to a VPN appliance (104), and initializing a stealth-based service on the mobile device (102). The method further includes transmitting user credential information from the mobile device to a Virtual Device Relay, VDR, broker (112) via the VPN appliance, and receiving status information from the VDR broker identifying a VDR (114) associated with the mobile device and providing a connected status. The method also includes communicating with one or more secure endpoints (132) within the secured network (130) via a VPN connection to the VDR via the VPN appliance and through the VDR to the one or more secure endpoints within a community of interest based on the user credential information transmitted to the VDR broker.



SECURE NETWORK COMMUNICATIONS IN A MOBILE DEVICE OVER IPSEC

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority from U.S. Provisional Patent Application No. 62/018,956, filed on June 30, 2014, Attorney Docket No. TN624.P, the disclosure of which is hereby incorporated by reference in its entirety.

[0002] The present application is also related to, and claims priority from the following related and commonly assigned U.S. Patent Applications:

[0003] 1. U.S. Provisional Patent Application entitled: Distributed Security on Multiple Independent Networks using Secure “Parsing” Technology, by Robert Johnson, Attorney Docket No. TN400.P, Serial No. 60/648,531, filed 31 January, 2005;

[0004] 2. U.S. Patent Application entitled: Integrated Multi-Level Security System, by Robert Johnson, Attorney Docket No. TN400.US, Serial No. 11/339,974 filed 26 January 2006 claiming the benefit of the above provisional applications;

[0005] 3. U.S. Patent Application entitled: Integrated Multi-Level Security System, by Robert Johnson et al., Attorney Docket No. TN400.USCIP1, Serial No. 11/714,590 filed 6 March 2007 which is a continuation-in-part of U.S. Application 11/339,974;

[0006] 4. U.S. Patent Application entitled: Integrated Multi-Level Security System, by Robert Johnson et al., Attorney Docket No. TN400.USCIP2, Serial No. 11/714,666 filed 6 March 2007 which is a continuation-in-part of U.S. Application 11/339,974; and

[0007] 5. U.S. Patent Application entitled: Integrated Multi-Level Security System, by Robert Johnson et al., Attorney Docket No. TN400.USCIP3, Serial No. 11/714,598 filed 6 March 2007 which is a continuation-in-part of U.S. Application 11/339,974.

[0008] 6. U.S. Patent Application, Serial No. 12/272,012, entitled “Block Level Data Storage Security System”, filed 17 Nov 2008, Attorney Docket No. TN497. The present disclosure also claims the benefit of commonly assigned U.S. Patent Application, Serial No. 12/336,558, entitled “Data Recovery Using Error Strip Identifiers”, filed 17 Dec 2008, Attorney Docket No. TN494.

[0009] 7 U.S. Patent Application, Serial No.12/336,559 entitled “Storage Security Using Cryptographic Splitting”, filed 17 Dec 2008, Attorney Docket No. TN496; U.S. Patent Application, Serial No. 12/336,562, entitled “Storage Security Using Cryptographic

Splitting”, filed 17 Dec 2008, Attorney Docket No. TN496A; U.S. Patent Application, Serial No. 12/336,564, entitled “Storage Security Using Cryptographic Splitting”, filed 17 Dec 2008, Attorney Docket No. TN496B; and U.S. Patent Application, Serial No. 12/336,568, entitled “Storage Security Using Cryptographic Splitting”, filed 17 Dec 2008, Attorney Docket No. TN504A.

[0010] 8. U.S. Patent Application, Serial No. 12/342,636 entitled “Storage Communities Of Interest Using Cryptographic Splitting”, filed 23 Dec 2008, Attorney Docket No. TN498. U.S. Patent Application, Serial No. 12/342,575, entitled “Storage Communities Of Interest Using Cryptographic Splitting”, filed 23 Dec 2008, Attorney Docket No. TN498A, U.S. Patent Application, Serial No. 12/342,610, entitled “Storage Communities Of Interest Using Cryptographic Splitting ”, filed 23 Dec 2008, Attorney Docket No. TN498B.

[0011] 9. U.S. Patent Application, Serial No. 12/342,379, entitled “Secure Network Attached Storage Device Using Cryptographic Splitting”, filed 23 Dec 2008, Attorney Docket No. TN499.

[0012] 10. U.S. Patent Application, Serial No. 13/493,023, entitled “Software Handling Of Hardware Error Handling In Hypervisor-Based Systems”, filed 5 Sept 2012, Attorney Docket No. TN550.

[0013] 11. U.S. Patent Application, Serial No. 13/547,148, entitled “Automated Provisioning of Virtual Machines”, filed 12 July 2012, Attorney Docket No. TN565.

[0014] 12. U.S. Patent Application Serial No. 14/042,239, entitled “Negotiation of Security Protocols and Protocol Attributes in Secure Communications Environment”, filed 30 September 2013, Attorney Docket No. TN597B.

[0015] 13. U.S. Patent Application Serial No. 14/042,182, entitled “Secured Communications Arrangement Applying Internet Protocol Security”, filed 30 September 2013, Attorney Docket No. TN597.

[0016] The disclosures of each of these applications are hereby incorporated by reference in its entirety as if set forth in this application.

TECHNICAL FIELD

[0017] The present application relates generally to secured communications and storage systems, and in particular to secure network communications in a mobile device over IPSec.

BACKGROUND

[0018] Modern organizations generate store, and communicate large quantities of data. In many instances, organizations include individuals having different rights to data, or different rights to communicate with other individuals or access particular computing resources. It is frequently important that such organizations be able to quickly and securely access the data stored at the data storage system. In addition, it is frequently important that data stored at a data storage system, or communicated between computing systems, be recoverable if the data is communicated or written incorrectly or are otherwise intercepted or corrupted.

[0019] To address the above issues, Unisys Corporation of Blue Bell, Pennsylvania developed a Stealth solution that uses a kernel-level driver to implement end-to-end cryptographic connections for communication of data across public and private networks. This solution allows users to communicate with other users having common user rights, while segregating user groups by way of assignment of different cryptographic keys used for each user group, or “community of interest”. However, the Stealth solution has some drawbacks.

[0020] Internet Protocol Security (IPsec) is one such standards-based protocol suite used for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec is an end-to-end security scheme of the Internet Protocol Suite. As compared to other security systems, such as SSL, SSH, or TLS, IPsec operates in the Internet Layer rather than operating in the upper layers of the TCP/IP model. Hence, IPsec protects any application traffic across an Internet Protocol (IP) network. Applications do not need to be specifically designed to use IPsec, whereas TLS/SSL is required to be designed into an application to protect the application protocols. In addition, IPsec operates in both IPv4 and IPv6-enabled networks.

[0021] However, IPsec is not without drawbacks. Existing IPsec-enabled systems typically negotiate to create IPsec tunnels, or secure tunnels, on a point-to-point basis, rather than allowing for data access by multiple entities within the same “community of interest”. Furthermore, IPsec is only available on some modern computing systems, and may be limited in availability in different types of systems, such as mobile devices. Furthermore, different implementations of IPsec on different types of computing systems are handled differently, leading to inconsistencies in connection parameters. Additionally, IPsec is built based on a

premise that two computing systems can negotiate security parameters; when two such systems intend to form a secure tunnel, that tunnel is established through use of an IKE key exchange, which requires a response to an initial transmission. However, to accomplish perfect forward secrecy, such trading of security parameters may not be possible.

[0022] Still further issues arise in the context of mobile devices, which may be located external to the secure network to which such mobile devices wish to connect. Such devices may use operating systems that lack support for Stealth, and may lack support for IPsec entirely. Furthermore, because such devices are mobile, there is no reliable instance in which the device may have a dedicated secured connection either to or within a network. Accordingly, improvements in the various existing secured communications systems are desired.

SUMMARY

[0023] In a first aspect, a method of communicating with secure endpoints included within a secured network from a mobile device external to the secured network is disclosed. The method includes initiating a VPN-based secure connection to a VPN appliance, and initializing a stealth-based service on the mobile device. The method further includes transmitting user credential information from the mobile device to a VDR broker via the VPN appliance, and receiving status information from the VDR broker identifying a VDR associated with the mobile device and providing a connected status. The method also includes communicating with one or more secure endpoints within the secured network via a VPN connection to the VDR via the VPN appliance and through the VDR to the one or more secure endpoints within a community of interest based on the user credential information transmitted to the VDR broker.

[0024] In a second aspect, a method of enabling communication between a mobile device and one or more secure endpoints included within a secured network is disclosed. The method includes receiving user credentials from a mobile device at a VDR broker within a gateway, and allocating a VDR at the gateway. The method also includes retrieving a wrapping key associated with the VDR, and transmitting a tuples request to an authentication server from the VDR broker, the tuples request including the user credentials. The method further includes receiving from the authentication server COIs wrapped with the wrapping key associated with the VDR, the COIs based on the user credentials, and providing configuration information to the VDR.

[0025] In a third aspect, a system for enabling communication between a mobile device and one or more secure endpoints included within a secured network is disclosed. The system includes a mobile gateway communicatively connectable to a mobile device via a tunneled connection. The mobile gateway includes a VDR broker configured to allocate VDRs to mobile devices based on authentication credentials received from the mobile devices and obtain key information to provide to the allocated VDRs for use in secure communications within the secured network. The mobile gateway further includes one or more VDRs associated with the mobile device and providing proxied secure communications using the key information obtained from the authentication server based on the authentication credentials provided by the mobile device.

[0026] This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] Figure 1A illustrates a generalized network in which communication is enabled between a mobile device and one or more secure endpoints included within a secured network;

[0028] Figure 1B illustrates components of a VDR broker included in the mobile gateway illustrated in Figure 1A, and useable to establish a virtual data relay (VDR) useable to enable communication between a mobile device and one or more secure endpoints included within a secured network;

[0029] Figure 2 illustrates a state diagram showing connectivity states of a mobile gateway for a particular enabled network connection between a mobile device and one or more secure endpoints included within a secured network;

[0030] Figure 3 illustrates an arrangement allowing a mobile device to connect to a plurality of different communities of interest, according to an example embodiment;

[0031] Figure 4 illustrates a flowchart of a method for enabling communication between a mobile device and one or more secure endpoints included within a secured network;

[0032] Figures 5A-5B illustrate an event sequence occurring at a mobile gateway to establish a VDR used for communication between a mobile device and one or more secure endpoints included within a secured network, according to an example embodiment;

[0033] Figures 6A-6B illustrate a sequence of communications among devices in establishing communications between a mobile device and one or more secure endpoints within a secured network, according to an example embodiment;

[0034] Figure 7 illustrates a sequence of communications among devices in performing a logoff operation for a first user, and establishing communications between a mobile device and one or more secure endpoints within a secured network for a second user, according to an example embodiment;

[0035] Figure 8 illustrates a sequence of communications among devices in performing a connection process in which a VPN error occurs, according to an example embodiment;

[0036] Figure 9 illustrates a sequence of communications among devices in performing a connection process in which a Stealth tunnel error occurs and is closed, according to an example embodiment;

[0037] Figure 10 illustrates an arrangement of the network of Figure 1 according to a further example embodiment providing high-availability connection for mobile devices to a Stealth-enabled network;

[0038] Figure 11 illustrates an example computing system in which aspects of the present disclosure can be implemented;

[0039] Figure 12 illustrates an example virtualization environment implemented on a computing system, illustrating a mechanism by which private-domain and cloud-based virtual machines can be implemented; and

[0040] Figure 13 illustrates an example multi-user computing arrangement illustrating shared computing resources across different partitions and/or virtual machines, according to example embodiments.

DETAILED DESCRIPTION

[0041] Various embodiments of the present invention will be described in detail with reference to the drawings, wherein like reference numerals represent like parts and assemblies throughout the several views. Reference to various embodiments does not limit the scope of the invention, which is limited only by the scope of the claims attached hereto. Additionally, any examples set forth in this specification are not intended to be limiting and merely set forth some of the many possible embodiments for the claimed invention.

[0042] The logical operations of the various embodiments of the disclosure described herein are implemented as: (1) a sequence of computer implemented steps, operations, or

procedures running on a programmable circuit within a computer, and/or (2) a sequence of computer implemented steps, operations, or procedures running on a programmable circuit within a directory system, database, or compiler.

[0043] In general, the present disclosure relates to improvements to systems and methods for securing endpoints and communication channels, such as the Stealth secure communications and storage system of Unisys Corporation of Blue Bell, Pennsylvania. As is included in the existing Stealth system, data to be transmitted among endpoints (e.g., client or server computing systems) is encrypted such that (1) no computing system other than the sender and intended recipient can view the contents of the encrypted message(s), and (2) in some embodiments, the messages are configurable such that message packets themselves are split among different packets and optionally transmitted along different transmission paths between computing systems, to ensure receipt of the secured communications at a receiving endpoint. That receiving endpoint can then reconstruct the message based on one or more such received split and encrypted messages.

[0044] The present disclosure specifically describes aspects of secure communications and secure computing systems that provide for a flexible manner in which mobile devices external to a secured network, such as a network secured with Stealth technology, can remotely connect to and securely communicate with endpoints within that secured network. Furthermore, the present application describes methods and systems by which specific devices, users, or applications themselves may be specifically associated with a group of affiliated computing resources such that only those resources within the secured network are visible to that associated device, user, or application. Other endpoints or computing resources within the secured network remain present, but are entirely opaque to the mobile device if not within the same community of interest,. Accordingly, even specifically-addressed messages directed to such endpoints will not be responded to (even with a response denying connection) thereby avoiding potential security issues that may be caused by denial of service attacks or other potential security compromise situations that do not require establishment of a connection to interfere with network operations. Accordingly, the present disclosure provides an additional layer of security in addition to traditional VPN connectivity, which is traditionally controlled or secured only at the level of user/device.

[0045] Referring now to Figure 1A, a generalized network 100 in which communication is enabled between a mobile device and one or more secure endpoints included within a secured network is shown. The network 100 includes a mobile device 102 communicatively

connected, via a public network 110, to a VPN server 104 managed by a secured entity. The VPN server 104 allows for communication via a trusted subnet 120 to a mobile gateway 106.

[0046] The mobile device 102 generally corresponds to any type of mobile device, such as a mobile phone, tablet, laptop, or other type of mobile device which may be used to connect to a secured network from a variable location and/or subnetwork. In the case of mobile phone and tablet devices, such a device may be an iOS-based device provided by Apple Corporation of Cupertino, California, or an Android-based device provided by any of a number of equipment-manufacturers, and operating using a variant of the Android operating system provided by Google, Inc. of Mountain View, California. Other types of mobile operating systems could be used as well (e.g., Blackberry, Microsoft's Windows Phone OS, or other operating systems). In preferred embodiments, the mobile device 102 either has a native IPsec implementation allowing it to communicate with a VPN server via an IPsec-based connection, or is capable of having installed thereon an application that manages such a secured connection over a public network. Consequently, the VPN server 104 provides a location at which the mobile device 102 can establish a secure connection to the enterprise, and which relays messages to the mobile gateway which effectively proxies the mobile device within the secure network, as discussed in further detail below.

[0047] In example embodiments, the VPN server 104 connects to an external network which is also accessible by the mobile device 102. The VPN server 104 authenticates and establishes an IPsec tunnel between itself and the mobile device 102, assigning it an IP address and subsequently routing traffic to the trusted subnet 120.

[0048] The mobile gateway 106 generally receives messages from the VPN server 104, relayed from the mobile device 102, via a portion of the enterprise network shown as a trusted subnet 120, which is dedicated to secure message routing between one or more VPN servers 104 and mobile gateways 106. The trusted subnet 120 may pass messages in cleartext or encrypted form, but in a manner dedicated to such interface communications with devices located remotely from the enterprise. In example embodiments, the trusted subnet may be a physical network connecting devices or a virtual network connecting software within an OS instance or a combination of the two. In all cases the trusted subnet 120 is isolated from the outside network and the Stealth network 130. Accordingly, if so desired, the trusted subnet 120 can be clear-text and would support packet inspection, firewalling and similar features if desired.

[0049] The mobile gateway 106 is communicatively connected to a Stealth network 130. The Stealth network 130 generally corresponds to a network managed within an enterprise, and which includes a plurality of Stealth network endpoints 132a-c, an authentication server 134, and a licensing server 136. The Stealth network 130 generally implements Stealth-based communications among endpoints within the Stealth network 130, as discussed in the applications incorporated by reference above. In example embodiments, the Stealth network 130 can be implemented using one or both of an IPsec-based Stealth implementation and a multi-level secure tunneling protocol (MLSTP)-based Stealth implementation, as is also described in the applications incorporated by reference above.

[0050] In the embodiment shown, the mobile gateway 106 includes a VDR broker 112 and a plurality of VDRs 114a-b. The VDR broker 112 interacts with the VPN server 104 and an authentication server 134, and the resources which instantiate instances of a virtual data relay (VDR), to establish routing of traffic to effectively allow a mobile device to participate in the Stealth network 130.

[0051] The VDR broker 112 acquires a Stealth license; during the authentication and authorization process of each mobile endpoint, the authorization manager of the VDR broker 112 will identify itself to the authentication server 134 as a VDR broker 112 for a mobile device in an XML-based tuples request (discussed in further detail below), and identifies the authenticating user via HTTP. The authentication server 134 will then indicate to the VDR broker 112 that a Stealth Mobile license is available for use.

[0052] In general, to ensure security the VDR broker 112 will not service client connections from mobile devices without first securing appropriate licenses, from the authentication server 134 and/or licensing server 136.

[0053] The VDRs 114a-b operate as proxies for the mobile devices 102 with which they are associated. Generally, an instance of a VDR exists for each IPsec connection established by the VPN server 104. For example, if a secure connection is established on a per-device basis, each device will be associated with a different VDR 114. In the example shown, different applications on the mobile device 102 are each associated with different VPN-based connectivity, and have different security credentials. Accordingly, in such an example embodiment, different VDRs (shown as VDRs 114a-b) are associated with different applications on the same mobile device 102. Generally, each VDR 114 hosts a Stealth network endpoint. The endpoint has been authenticated by the authentication server 134. Traffic routes are established allowing traffic to flow between a stealth network endpoint 132

and the mobile device 102, based on the stealth network endpoint and the associated application (or device, or user, based on the level of granularity of security authorization as implemented). In particular embodiments, application-level authentication is used to the exclusion of device-level authentication, requiring a user to authenticate himself/herself within each application seeking a secured connection to Stealth network endpoints 132.

[0054] In example embodiments, and as discussed further below, the IPsec-based Stealth solution can be employed in either an entirely IPsec-based secure network, or within an existing Stealth network employing a traditional bit-based splitting and encrypting/decrypting arrangement, which utilizes an existing multi-level secure transport protocol (MLSTP) secure communications construct. In both configurations, all endpoints in the Stealth network are required to be licensed with a Stealth license that supports earlier versions of the Stealth security protocol. In addition, a Stealth appliance may be used, and all licensing and logging is provided through the Stealth appliance (or team of appliances). However, it is noted that a mixed Stealth configuration may be required when the IPsec-based system is deployed in an existing Stealth network in which endpoints are already running a previous Stealth configuration, or when the existing (or new) Stealth network must support otherwise unsupported endpoints (e.g., Windows XP, Windows 2003).

[0055] The VPN server 104 will perform the IPsec authentication and tunnel address assignment with participation by the VDR broker 112. Accordingly, mobile device applications will connect to the VPN server 104 using a user ID for an IPsec authentication, which will also subsequently be used for Stealth authentication via the authentication server 134.

[0056] Although in the embodiment shown a single mobile device is illustrated, it is understood that this is intended as exemplary; however, in typical embodiments the mobile broker will manage connections associated with a plurality of different mobile devices, mobile device applications, and/or users.

[0057] Referring now to Figure 1B, details of the VDR broker 112 included within the mobile gateway 106 are provided, according to an example embodiment. In example implementations the VDR broker 112 operates on an enterprise Linux-based system, with each of a plurality of managers instantiated thereon executing as separate programs in separate processes. In example implementations, the VDR broker 112 can be deployed as a bootable image that can be deployed on a bare metal computing system or virtual machine guest on a computing device, such as the devices illustrated in Figures 11-13, below. Various messages handled by the VDR broker 112, and in particular the managers included therein,

can be implemented using named pipes, with messages represented in structures that are decodable to function parameters that can be consumed by the event managers. In the example shown, the VDR broker 112 includes an authentication manager 113, a VPN manager 115, a VDR manager 116, a client application manager 117, an event manager 118, and a license manager 119.

[0058] The authentication manager 113 operates to, in example embodiments, authenticate VPN user and client application credentials with the Stealth-enabled network, for example by connecting to the authentication server 134. The authentication manager 113 can do so, for example in response to a request generated by the event manager 118. The authentication manager can further obtain Stealth authentication and authorization key materials, and return them to the event manager 118. Additionally, to the extent various versions of the Stealth service are provided within the Stealth network 130, the authentication manager 113 is configured to abstract such communication systems into a single, unified view presented to the mobile device 102. In some embodiments, an API library can be used to connect to the authentication server 134 to authenticate user/application credentials.

[0059] The VPN manager 115, in the embodiment shown, is configured to receive client tunnel connection indications from the VPN server 104, and reports the information to the event manager 118. The VPN manager is configured to receive client tunnel disconnection indications from the VPN server 104 and reports them to the event manager 118 as well. The VPN manager 115 is also configured to close a client tunnel in the VPN concentrator upon request from the event manager 118, and manages different types of VPN and abstracts them into a single view for management purposes. In example embodiments, an SSH-based library can be used by the VPN manager 115 to issue command line operations to the VPN server 104, to explicitly issue connection closures to mobile devices connected via such a VPN server.

[0060] The VDR manager 116, in the embodiment shown, is configured to start and shut down VDRs 114, as well as handling requests from the broker. The VDR manager 116 is further configured to create new VDR 114 and return its IP addresses. The VDR manager 116 is also configured to delete old VDRs, and manage an available VDR pool, to the extent a maximum number or available number of VDRs is provided at the mobile gateway 106. In example embodiments, to manage a pool of available VDRs, the VDR manager 116 creates and/or starts new VDRs 114 when needed and assigns IP addresses and other configuration

parameters to those VDRs. The VDR manager also manages different versions of VDRs, for example based on types of connectivity, and abstracts them into a single view.

[0061] In example embodiments, the VDR manager 116 is instantiated using a shell script within the VDR broker 112, and initiates a container having a configuration file. The VDR manager 116 can be initialized to instantiate a master VDR as well as one or more internal VDR pools and lists, and initialize individual VDRs for use. The VDR manager 116 can associate IP addresses, hardware addresses, and other physical resources (routing, packet forwarding parameters) to the various VDRs. The VDR manager 116 maintains a set of life-cycle states of VDRs, including a starting state, a running state, a freezing state, a frozen state, an unfreezing state, a stopping state, and an error state. The starting state represents a VDR cloned from a master VDR, which initializes hardware resources and causes the VDR to join a pool as a running VDR. The VDR is then initialized as useable within a stealth network, and enters a freezing state, which places the VDR in the pool of available VDRs (discussed below), in a frozen state. When a VDR is allocated, the VDR manager 116 indicates that the VDR is in an unfreezing state. The stopping state manages client requests to stop a VDR, which corresponds to the termination occurring in Figure 2 (and tracked by the event manager 118) below. An error state indicates that an uncorrectable error has occurred within the VDR, causing it to be terminated and ceasing to exist (allowing a new VDR to be re-instantiated).

[0062] The client application manager 117, in the embodiment shown, is configured to receive Stealth user credentials from a mobile client application, and receives status update requests from such an application. Likewise, the client application manager 117 can be configured to send status update requests to an application on a mobile device, and manage different types of client applications for abstracting to a single view for management purposes as well.

[0063] The event manager 118, in the embodiment shown, is configured to manage the state of each client connection. Example states of client connections are described in an example embodiment below, in connection with Fig. 2. The event manager 118 is further configured to receive and act upon events posted by the other modules, as also described below.

[0064] The license manager 119, in the embodiment shown, is configured to obtain a fixed count of Stealth Mobile licenses from a Stealth license gateway, and maintain a license tunnel to the license gateway on behalf of each of the VDRs 114 at the mobile gateway 106.

The license manager 119 is further configured to report license tunnel and license allocation status to the event manager 118.

[0065] In example embodiments, the event manager 118 manages a VDR table 131 that tracks a state of each client connection. The VDR table 131 can include, for example, various user and connectivity parameters, such as a VPN User ID, a VPN assigned IP address, a VPN Session ID, a VDR Session ID, a VDR IP address, a Stealth User ID, a start time, a keep alive (last received) time, a state (e.g., pending, open, close, error), and a list of IDs for communities of interest associated with the particular VDR, defining the endpoints with which that VDR can connect or to which the VDR (and associated mobile device 102) is visible.

[0066] In general the VDR broker 112 manages a plurality of events and associated states for each connection to a mobile device application. Events can include, for example, an access request message receipt, a VPN tunnel up or down message, a VDR down event, a Stealth tunnel down event, a Stealth TUN down event, or a license lost event. Such events can be triggered, typically, by external systems transmitting messages to the VDR broker 112. Correspondingly, the VDR broker 112 can take a plurality of different actions relative to such messages received, such as adding a new VDR, deleting an old VDR, performing a status query, generating an administrative notification, retrieving a wrapping key from an active VDR, or sending community of interest (COI) keys to a VDR. Furthermore, the VDR broker 112 manages VDR states for each VDR, as noted below.

[0067] Referring now to Figure 2, a state diagram 200 is illustrated showing connectivity states of a mobile gateway for a particular enabled network connection between a mobile device and one or more secure endpoints included within a secured network. VDR states can include, for example, a null session state 202 (referred to as SESS_NONE), a VDR request state 204 (SESS_REQ_VDR), an assigned VDR state 206 (SESS_ASSIGNED_VDR), a VDR provisioning request state 208 (SESS_COI_PROV_REQ), and a VDR active state 210 (SESS_COI_ACTIVE). Generally the null session state 202 represents a VDR in an available pool and lacking any routing or association with a VPN IP address. Such VDRs have a service key loaded and an associated IP address. The VDR request state 204, or starting state, generally has no routing, and is not associated with a VPN IP address. Rather, in this starting state the VDR broker 112 can create or start a container and start a Stealth service key mode, allowing the VDR to be allocated from the available pool.

[0068] The assigned VDR state 206 still has no routing, but has a service key loaded and includes IP addresses. The assigned VDR state 206 is associated with a VPN IP address, corresponding that VDR with a particular secure connection to a mobile application. However, a VDR in the assigned VDR state still has no community of interest material (keys, etc.) assigned, so communication by the mobile device within the Stealth network 130 is not yet enabled. In the VDR active state 210, the VDR broker 112 has assigned the VDR 114 with routing information, an associated VPN IP address, and community of interest material. Furthermore, the VDR broker 112 has opened a license tunnel, allowing for validation of the COI material within the Stealth network 130.

[0069] In operation, the event manager 118 of the example embodiments described above tracks state transitions among the various states 202-210, which may transition based on actions taken by the VDR broker 112. Various actions may be performed. In example embodiments, actions can include:

- a session creation action 220 (ACT_CREATE_SESSION), which creates a session entry and assigns a session ID;
- a request VDR action 222 (ACT_REQ_VDR), which corresponds to a VDR request received at the VDR manager from a VPN server 104, and including a Client IP address and session ID. The request VDR action 222 triggers a VPN_CONNECTION_START event passing a username and IP address of the mobile endpoint from the VPN server 104 to the VDR broker 112.
- a VDR assignment action 224 (ACT_VDR_ASSIGN_COMPLETE), which reassigns a state to assign the VDR;
- a VDR provisioning action 226 (ACT_PROV_VDR), which sends a provision request to the VDR manager;
- a VDR provisioning verification action 228 (ACT_PROV_COMPLETE), which resets a state of the VDR to active, as noted below; and a VDR discarding action 230 (ACT_VDR_DISCARD), which issues a VDR discard request to the VDR manager; and
- a cleanup action 232 (ACT_CLEANUP), which issues a VDR discard request to the VDR manager and frees session resources for reuse.

[0070] In the null session state 202, receipt of a start connection request from a VPN server 104 (shown as VPN_CONNECTION_START) will cause the VDR broker 112 to perform a session creation action 220, transitioning the VDR to the VDR request state 204.

Receipt of a vdr assignment response (VDR_ASSIGN_RSP), which indicates that a VDR has been allocated, can trigger the VDR assignment action 224, and, upon a VDR assignment action 224 (ACT_VDR_ASSIGN_COMPLETE), transition to the assigned VDR state 206. The VDR assignment response can include, for example, a VDR ID, parser public key, and VDR IP addresses (with different IP addresses facing networks 120, 130, as seen in Figure 4).

[0071] An authentication completion indication (AUTH_COMPLETE_IND), corresponding to a message from the authentication manager that a Stealth user has been authenticated by the authentication server 134, includes a username, gateway, and COI response from the authentication server, and triggers the VDR provisioning action 226, which in turn transitions the VDR to a VDR provisioning request state 208. From the VDR provisioning request state 208, a VDR provisioning verification action 228 will transition the VDR to a VDR active state 210, upon occurrence of a verification message (VDR_PROV_COMPLETE) from the VDR manager. From the VDR active state 210, a connection stop message (VPN_CONNECTION_STOP) received from the VPN server 104 indicating that a VPN tunnel has closed will cause transition to return to a VDR provisioning action 226, triggering attempts to re-provision the VDR with the associated mobile device upon reconnection of the VPN tunnel.

[0072] Additionally, when in any of states 206-212, performance of a cleanup action 232, or in states 208-212 performance of a VDR discarding action 230, will transition the VDR to a null session state 202, returning the VDR to an available pool by turning off all routing, disabling workgroups, and disassociating a VPN IP address (thereby disassociating the VDR from the mobile device and associated application). Such terminations may occur, for example, in response to a termination message received from the authentication manager (referred to in Figure 2 as CLIENT_STEALTH_TERM).

[0073] Referring to Figure 2 generally, it is noted that although a particular set of states and state transitions are disclosed, other states or transitions may be provided as well, for example to accommodate tracking of different types of VDR connections, VPN connections, or to further define instances in which terminations occur to determine a cause of such terminations.

[0074] Referring now to Figure 3, a particular arrangement 300 is shown, allowing a mobile device to connect to a plurality of different communities of interest, according to an example embodiment. The arrangement 300 illustrates connectivity within a broker host 302, which generally represents a computing system hosting the VDR broker 112 of Figure 1.

[0075] In the embodiment shown, a mobile device 102 can connect to a VPN gateway 304 (e.g., corresponding to VPN server 104 of Figure 1) via a public network 310. The connection between the mobile device 102 and VPN gateway 304 can be a tunneled, IPsec-based secure connection. In the embodiment shown, this connection is shown as accessible to the mobile device via address 10.99.95.1/24 (by way of example only). The VPN Gateway communicates with the broker host 302 via a network 320, at which it exposes a second IP address by which it communicates. In the example shown, the VPN gateway 304 is accessible using IP address 10.98.0.4.

[0076] Within the broker host 302, a plurality of VDRs are established by the VDR broker (not shown here, but as discussed above). In this example, the mobile device 102 can communicate separately with two different VDRs, given IP addresses 10.97.0.1 and 10.97.0.2. Accordingly, a first application at the mobile device 102 may have a first secure connection to a first VDR 314a (accessing at 10.97.0.1), while a second application at the mobile device 102 may have a second, separate secure connection to a second VDR 314b (accessing at 10.97.0.2). Such different VDRs may be assigned different COI credentials, allowing the first VDR 314a to connect to a first set of endpoints within a first community of interest 312a (shown as “Blue COI”), while a second VDR 314b can connect to a second set of endpoints within a second community of interest 312b (shown as “Red COI”).

[0077] Additionally, an authentication server 334 can be presented either at network 320 or network 330, and is accessible within the local subnet to pass COI credentials to the VDRs based on a request received from the VDR broker at the broker host 302. A licensing tunnel can be established to a licensing gateway 336 (analogous to licensing server 136) at network 320 or network 330 as well, and can connect to a licensing VDR 333 via an address within subnets facing either network 320 or 330 (subnets 10.97.0.x or 10.1.1.x) at a known address to allow for establishing and monitoring a licensing connection at the broker host 302.

[0078] Referring now to Figure 4 generally, a flowchart of a method 400 for enabling communication between a mobile device and one or more secure endpoints included within a secured network is shown. The method 400 can be performed within a network such as network 100, to initialize and perform communications between a mobile device (e.g., mobile device 102) and an endpoint within a secure network (e.g., Stealth network endpoints 132a-b within an allocated COI). Generally, the method 400 is performed based on selecting an appropriate VPN client and connection that is configured for connection to a VPN server

affiliated with a secured network, such as VPN server 104 associated with a Stealth network 130 of Figure 1.

[0079] In the embodiment shown, the method 400 includes initiating a VPN connection from the mobile device (step 402). This can include enabling the VPN client, and prompting a user of the VPN client to connect to the VPN server, for example using a username/password or other authentication credentials. Upon establishment of the VPN connection the mobile device will have a working network path to the VPN server and an associated VDR broker, but cannot yet access a Stealth-based intranet or associated services.

[0080] In some embodiments, initiating a VPN connection from the mobile device can include starting a Stealth-specific mobile application (step 404) and initializing a Stealth connection at the mobile device. Such embodiments, which may be required by some operating systems that do not enable IPsec-based connections natively, may require additional connection parameters (e.g., a passphrase or other secure communication credentials) which allow the user to open an SSL connection between the VPN server and the VDR broker. The user can then enter his or her username and password information to allow for a logon connection to the VDR broker.

[0081] In the embodiment shown, the method 400 further includes the VDR broker interacting with an authentication server (e.g., authentication server 134 of Figure 1A, or authentication server 334 of Figure 3) to pass the user's credentials to the authentication server for authentication (step 406). The VDR broker transmits a tuples request to the authentication server and obtains a public certificate from the authentication server. The authentication manager (e.g., authentication manager 113 of Figure 1B) creates an event to add a new VDR, and an event to obtain a wrapping key from the VDR. The wrapping key obtained from the VDR is then returned to the authentication server, which (upon positive authentication) returns the response to the tuples request including COI information (including COI keys) wrapped with the VDR's wrapping key.

[0082] In the embodiment shown, the method 400 also includes the VDR broker starting the VDR associated with the COI information (step 408). This includes the VDR broker building a stealth configuration based on the returned tuples request results from the authentication server, establishing routing, and awaiting a license tunnel to open. The VDR broker then passes the COI key IDs, appliance IP addresses, key status, and other connection information to the VDR.

[0083] The mobile application further includes, in some example embodiments, the mobile application receiving an answering response based on the authentication request transmitted by the mobile device (step 410), indicating to the mobile device the success or failure of establishing a secure connection to the desired Stealth-enabled network (specifically, the assigned COIs within that network).

[0084] Referring now to Figures 5A-5B, 6A-6B, and 7-8, various messaging and events are described illustrating example connection and disconnection sequences occurring between a mobile device and a Stealth-enabled network (by way of a mobile gateway and associated VDR broker). Figures 5A-5B illustrate an event sequence 500 occurring at a mobile gateway to establish a VDR used for communication between a mobile device and one or more secure endpoints included within a secured network, according to an example embodiment. In the embodiment shown, operational event sequences occur among an event manager, an authentication manager, a VPN manager, and a VDR manager, examples of which are discussed above in connection with Figure 1B.

[0085] In the example shown, a VPN manager (e.g., VPN manager 115) indicates an initialized VPN connection to a mobile device. The event manager (e.g., event manager 118) creates a table entry using the VPN IP parameters, and logs that event. The event manager then sends a VDR request to the VDR manager, and indicates a state should be set at SESS_REQ_VDR (e.g., VDR request state 204), indicating to request a VDR to be allocated. The event manager passes a message to VDR manager (e.g., VDR manager 116), which shuts down a VDR if a maximum number of VDRs has been reached, or otherwise allocates a new VDR. The event manager receives confirmation of the allocated VDR, and updates a table entry in VDR table 131 with a requestID, VPN IP, resultcode, and result text. The event manager also logs the allocation of the VDR. The event manager returns a message to the VPN manager.

[0086] The authentication manager (e.g., authentication manager 113) receives a login request from a mobile application, and event manager transmits a VDR assignment to the VDR manager. The VDR manager assigns a VDR and returns an assigned VDR, routing information, and a wrapping key. The event manager updates a table to indicate a state of the VDR as an assigned VDR state 206 (SESS_ASSIGNED_VDR) and stores a stealth user name, wrapping key, requestID, and VPN IP in the VDR table 131. The event manager then provides to the authentication manager a message, causing the authentication manager to transmit a tuples request to the authentication server (e.g., authentication server 134 or 334 of

Figures 1A, 3). The tuples request can include, for example, a username, password, and public key, and a response to the tuples request can be received that includes the request ID, VPN IP address, sessionID, and a tuples XML file including COI information wrapped with the wrapping key of the VDR. The event manager updates a state of the VDR (to the VDR provisioning request state 208, SESS_COI_PROV_REQ), and logs the information retrieved. The event manager passes the received information to the VDR manager which provisions the VDR instance with the various information (COI information in the form of the tuples XML file, as well as username information and session information). The VDR manager starts the Stealth service, and the event manager updates the state of that VDR to SESS_COI_ACTIVE (VDR active state 210). The authentication manager then passes a status of authentication back to the mobile device, confirming successful authentication.

[0087] Figures 6A-6B illustrate a sequence of communications 600 among devices in establishing communications between a mobile device and one or more secure endpoints within a secured network, according to an example embodiment. The sequence of communication 600 can occur among a mobile device (e.g., mobile device 102), a VPN appliance (e.g., VPN server 104), a VDR broker (e.g., VDR broker 112 at mobile gateway 106), a VDR (e.g., VDR 114), and an authentication server (e.g., authentication server 134).

[0088] In the embodiment shown, a mobile device starts a secure application and provides a certificate, username, and password to the VPN appliance. The VPN appliance authenticates the mobile device and establishes a secure (e.g., IPsec-based tunneled) connection between the mobile device and VPN appliance. The VPN appliance transmits a session ID and VPN IP address to the VDR broker, which allocates a VDR and sends an acknowledgement back to the VPN appliance. The mobile device then transmits a login request to the VDR broker, which obtains a wrapping key from an allocated VDR and builds a tuples request. The VDR broker transmits the tuples request to the authentication server, which includes the wrapping key and the user's login credentials. The authentication server authenticates the user based on the login credentials, and returns that user's COI keys wrapped with the VDR wrapping key to the VDR broker as a tuples XML response. The VDR broker sends a Stealth configuration to the VDR, which opens a license tunnel to a home appliance, and returns status information to the VDR broker. The VDR broker in turn optionally returns the status information to the mobile device for confirmation.

[0089] As seen in Figure 6B, the established tunnel can be closed by the mobile device transmitting a tunnel close message to the VPN appliance, which stops the VPN connection

and transmits a stop message, alongside a session ID and the VPN IP address, to the VDR broker. Based on that information, the broker updates and deallocates the VDR, and confirms with the VPN appliance. A VDR shutdown message is transmitted to the VDR associated with the VPN IP address and session ID, and the VDR returns a shutdown confirmation message upon shutdown to the VDR broker.

[0090] Figure 7 illustrates a sequence of communications 700 among devices in performing a logoff operation for a first user, and establishing communications between a mobile device and one or more secure endpoints within a secured network for a second user, according to an example embodiment. The sequence of communications 700 as shown generally occurs among the same devices, or types of devices, as discussed above in connection with Figures 6A-6B.

[0091] In the embodiment shown, the mobile device transmits a logoff message associated with a first user and session (shown as User X and Session ID). The VDR broker transmits a stealth service key state message to the VDR, which returns an acknowledgement and the service key state to the VDR broker. A subsequent login message from the mobile device, associated with a different user (User Y) is received at the VDR broker, which obtains the wrapping key from the VDR, and builds a tuples request. As in Figs. 6A-6B, the VDR broker retrieves COI information associated with the user (in this case User Y) retrieved from the authentication server wrapped in the wrapping key. The VDR broker then configures the VDR, which opens a license tunnel and initiates communication. The VDR broker transmits an updated status indicating successful connection to the mobile device, which optionally displays status information indicating successful connection.

[0092] Referring now to Figures 8-9, example connection sequences are illustrated depicting failed connections. Figure 8 illustrates a sequence of communications 800 among devices in performing a connection process in which a VPN error occurs, according to an example embodiment. In this embodiment, upon occurrence of a VPN error, the VPN appliance will close a VPN tunnel and indicate to the VDR broker that the tunnel has closed. The VDR broker will close the Stealth connection and transmit a message to the VDR associated with the mobile device to close all tunnels. The VDR will return an acknowledgement to the VDR broker, which disables routing, shuts down the VDR, and updates its state tables. The mobile device, which has an application status connection, will identify the failed VPN connection and display an indication of failed connectivity.

[0093] Similarly to Figure 8, Figure 9 illustrates a sequence of communications among devices in performing a connection process in which a Stealth tunnel error occurs and is closed, according to an example embodiment. In this sequence of communications 900, because it is the Stealth connection which fails (e.g., due to dropping a license tunnel), the VDR transmits a notification to the VDR broker, which updates the VDR table 131, setting a status to offline. The mobile device will request an application status from the VDR broker, and, upon finding that a status of the VDR is “offline”, will turn off Stealth and turn it back on, attempting reconnection. The VDR broker will try to reopen the license tunnel, and, upon successful reopening of the license tunnel from the VDR, the VDR broker will update status and return that status to the mobile device for display.

[0094] Referring now to Figure 10, an arrangement 1000 of the network of Figure 1 according to a further example embodiment providing high-availability connection for mobile devices to a Stealth-enabled network is shown. The arrangement 1000 ensures availability of a VDR by establishing redundant mobile gateways. In the embodiment shown, three client device connections 1002a-c are shown, connecting to two different mobile gateways 1006 (via VPN appliances, not shown). In this instance, VDR instances 1014 are redundant across the gateways and pooled between switches 1020, allowing for shared usage of VDRs across the mobile gateways. Accordingly, the client device connections 1002a-c can be made to either mobile gateway, with an L2 switch cluster communication module 1015 managing communication therebetween. Within a Stealth-enabled network 1030 (connected by switch 1020), cluster nodes 1022a-c are provided in which additional VDR instances are provided at cluster nodes, and are connected in a redundant, star-configuration to the Stealth-enabled network.

[0095] Referring to Figures 11-13, example details regarding computing systems in which aspects of the present disclosure can be implemented are provided. Such computing systems represent optional emulated environments in which the methods and systems of the present disclosure can be implemented, for example using the hardware systems disclosed above in connection with Figures 1, 3, and 10.

[0096] Figure 11 illustrates a computer system 1100 adapted according to certain embodiments of the gateway computing device, server and/or the user interface device. The central processing unit (“CPU”) 1102 is coupled to the system bus 1104. The CPU 1102 may be a general purpose CPU or microprocessor, graphics processing unit (“GPU”), and/or microcontroller. The present embodiments are not restricted by the architecture of the CPU

1102 so long as the CPU 1102, whether directly or indirectly, supports the operations as described herein. The CPU 1102 may execute the various logical instructions according to the present embodiments.

[0097] The computer system 1100 also may include random access memory (RAM) 1108, which may be synchronous RAM (SRAM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), or the like. The computer system 1100 may utilize RAM 1108 to store the various data structures used by a software application. The computer system 1100 may also include read only memory (ROM) 1106 which may be PROM, EPROM, EEPROM, optical storage, or the like. The ROM may store configuration information for booting the computer system 1100. The RAM 1108 and the ROM 1106 hold user and system data, and both the RAM 1108 and the ROM 1106 may be randomly accessed.

[0098] The computer system 1100 may also include an input/output (I/O) adapter 1110, a communications adapter 1114, a user interface adapter 1116, and a display adapter 1122. The I/O adapter 1110 and/or the user interface adapter 1116 may, in certain embodiments, enable a user to interact with the computer system 1100. In a further embodiment, the display adapter 1122 may display a graphical user interface (GUI) associated with a software or web-based application on a display device 1124, such as a monitor or touch screen.

[0099] The I/O adapter 1110 may couple one or more storage devices 1112, such as one or more of a hard drive, a solid state storage device, a flash drive, a compact disc (CD) drive, a floppy disk drive, and a tape drive, to the computer system 1100. According to one embodiment, the storage device 1112 may be a separate server coupled to the computer system 1100 through a network connection to the I/O adapter 1110. The communications adapter 1114 may be adapted to couple the computer system 1100 to the network 1208, which may be one or more of a LAN, WAN, and/or the Internet. The communications adapter 1114 may also be adapted to couple the computer system 1100 to other networks such as a global positioning system (GPS) or a Bluetooth network. The user interface adapter 1116 couples user input devices, such as a keyboard 1120, a pointing device 1118, and/or a touch screen (not shown) to the computer system 1100. The keyboard 1120 may be an on-screen keyboard displayed on a touch panel. Additional devices (not shown) such as a camera, microphone, video camera, accelerometer, compass, and or gyroscope may be coupled to the user interface adapter 1116. The display adapter 1122 may be driven by the CPU 1102 to control the display on the display device 1124. Any of the devices 1102-1122 may be physical and/or logical.

[00100] The applications of the present disclosure are not limited to the architecture of computer system 1100. Rather the computer system 1100 is provided as an example of one type of computing device that may be adapted to perform the functions of a server and/or a user interface / client device. For example, any suitable processor-based device may be utilized including, without limitation, personal data assistants (PDAs), tablet computers, smartphones, computer game consoles, and multi-processor servers. Moreover, the systems and methods of the present disclosure may be implemented on application specific integrated circuits (ASIC), very large scale integrated (VLSI) circuits, or other circuitry. In fact, persons of ordinary skill in the art may utilize any number of suitable structures capable of executing logical operations according to the described embodiments. For example, the computer system 1100 may be virtualized for access by multiple users and/or applications.

[00101] Figure 12 is a block diagram illustrating a server hosting an emulated software environment for virtualization according to one embodiment of the disclosure. An operating system 1202 executing on a server includes drivers for accessing hardware components, such as a networking layer 1204 for accessing the communications adapter 1114. The operating system 1202 may be, for example, Linux. An emulated environment 1209 in the operating system 1202 executes a program 1210, such as CPCCommOS. The program 1210 accesses the networking layer 1204 of the operating system 1202 through a non-emulated interface 1206, such as XNIOP. The non-emulated interface 1206 translates requests from the program 1210 executing in the emulated environment 1209 for the networking layer 1204 of the operating system 1202.

[00102] In another example, hardware in a computer system may be virtualized through a hypervisor. Figure 13 is a block diagram illustrating a server hosting an emulated hardware environment according to one embodiment of the disclosure. Users 1252, 1254, 1256 may access the hardware 1260 through a hypervisor 1258. The hypervisor 1258 may be integrated with the hardware 1260 to provide virtualization of the hardware 1260 without an operating system, such as in the configuration illustrated in Figure 11. The hypervisor 1258 may provide access to the hardware 1260, including the CPU 1102 and the communications adapter 1114.

[00103] If implemented in firmware and/or software, the functions described above may be stored as one or more instructions or code on a computer-readable medium. Examples include non-transitory computer-readable media encoded with a data structure and computer-readable media encoded with a computer program. Computer-readable media includes

physical computer storage media. A storage medium may be any available medium that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to store desired program code in the form of instructions or data structures and that can be accessed by a computer. Disk and disc includes compact discs (CD), laser discs, optical discs, digital versatile discs (DVD), floppy disks and Blu-ray discs. Generally, disks reproduce data magnetically, and discs reproduce data optically. Combinations of the above should also be included within the scope of computer-readable media.

[00104] Computer storage media generally includes at least some tangible, non-transitory media and can, in some embodiments, exclude transitory wired or wireless signals. Communication media may be embodied by 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 information delivery media. The term “modulated data signal” may describe a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media may include wired media such as a wired network or direct-wired connection, and wireless media such as Wi-Fi, acoustic, radio frequency (RF), infrared, and other wireless media. In accordance with the present disclosure, the term computer readable media as used herein may include computer storage media, but generally excludes entirely transitory embodiments of communication media, such as modulated data signals.

[00105] In addition to storage on computer readable medium, instructions and/or data may be provided as signals on transmission media included in a communication apparatus. For example, a communication apparatus may include a transceiver having signals indicative of instructions and data. The instructions and data are configured to cause one or more processors to implement the functions outlined in the claims.

[00106] Although the present disclosure and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the disclosure as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the present invention, disclosure, machines, manufacture,

compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present disclosure. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

[00107] Referring to Figures 1-13 overall, it is noted that in addition to the above functionality, it is apparent that specific applications may be made available using the methods and systems discussed herein for providing mobile connectivity to a Stealth-enabled network. For example, application-level connectivity and security can be provided, allowing for different access by different applications to different endpoints within different communities of interest, with dedicated VDRs for each community of interest and/or application connection made. Furthermore, based on the flexibility of communication connections of mobile devices, VDRs can be dynamically allocated, either at a particular mobile gateway or within a high availability environment including redundant and fault-tolerant networks of mobile gateways. Other advantages are provided as well, as are apparent from the above disclosure.

[00108] 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:

1. A method of communicating with secure endpoints included within a secured network from a mobile device external to the secured network, the method comprising:
 - initiating a VPN-based secure connection to a VPN appliance;
 - initializing a stealth-based service on the mobile device;
 - transmitting user credential information from the mobile device to a VDR broker via the VPN appliance;
 - receiving status information from the VDR broker identifying a VDR associated with the mobile device and providing a connected status; and
 - communicating with one or more secure endpoints within the secured network via a VPN connection to the VDR via the VPN appliance and through the VDR to the one or more secure endpoints within a community of interest based on user credential information transmitted to the VDR broker.
2. The method of claim 1, wherein the community of interest includes a user of the mobile device and the one or more secure endpoints but excludes one or more second endpoints within the secured network, wherein the one or more second endpoints are obscured to the user of the mobile device while the mobile device has the connected status.
3. The method of claim 1, wherein the mobile device includes a mobile security application installed thereon.
4. The method of claim 1, wherein the mobile device includes a first application and a second application installed thereon, and wherein the user credential information is collected by the first application.
5. The method of claim 4, wherein communicating with one or more secure endpoints comprises initiating communication from the first application, wherein the second application is excluded from the community of interest and lacks access to the one or more secure endpoints.

6. The method of claim 4, further comprising:
 - transmitting second user credential information from the second application on the mobile device to the VDR broker;
 - receiving status information from the VDR broker identifying a second VDR associated with the mobile device and providing the connected status; and
 - communicating with one or more second secure endpoints within the secured network via a VPN connection to the second VDR via the VPN appliance and through the second VDR to the one or more second secure endpoints within a second community of interest based on the second user credential information.
7. The method of claim 1, further comprising transmitting a tunnel close command to the VDR broker via the VPN appliance.
8. The method of claim 7, wherein transmission of the tunnel close command causes the VPN appliance to close a VPN tunnel and causes the VDR broker to shut down the VDR associated with the mobile device.
9. A method of enabling communication between a mobile device and one or more secure endpoints included within a secured network, the method comprising:
 - receiving user credentials from the mobile device at a VDR broker within a gateway;
 - allocating a VDR at the gateway;
 - retrieving a wrapping key associated with the VDR;
 - transmitting a tuples request to an authentication server from the VDR broker, the tuples request including the user credentials;
 - receiving, from the authentication server, one or more COIs wrapped with the wrapping key associated with the VDR, the one or more COIs based on the user credentials;
 - and
 - providing configuration information to the VDR.
10. The method of claim 9, further comprising the VDR opening a license tunnel to a home stealth appliance.

11. The method of claim 9, further comprising receiving status information from the VDR at the VDR broker.

12. The method of claim 9, wherein the wrapping key is provided to the VDR broker by the VDR.

13. The method of claim 9, further comprising returning status information regarding the VDR to the mobile device.

14. A system for enabling communication between a mobile device and one or more secure endpoints included within a secured network, the system comprising:

a mobile gateway communicatively connectable to the mobile device via a tunneled connection, the mobile gateway including:

a VDR broker configured to allocate VDRs to mobile devices based on authentication credentials received from the mobile devices and obtain key information to provide to the allocated VDRs for use in secure communications within the secured network;

one or more VDRs associated with the mobile device and providing proxied secure communications using the key information obtained from an authentication server based on the authentication credentials provided by the mobile device.

15. The system of claim 14, further comprising the mobile device, wherein the mobile device includes a Stealth connectivity application installed thereon.

16. The system of claim 15, further comprising a VPN appliance connected between the mobile device and the mobile gateway.

17. The system of claim 14, further comprising the authentication server, wherein the authentication server is within the secured network communicatively connected to the mobile gateway.

18. The system of claim 14, wherein the mobile gateway manages a plurality of VDR connectivity states for each VDR connection, the plurality of VDR connectivity states including:

- an inactive state;
- a request VDR state;
- an assigned VDR state;
- a provisioning request state; and
- a COI active state.

19. The system of claim 14, further comprising a licensing VDR at the mobile gateway configured to maintain a licensing tunnel to a licensing server within the secured network, wherein, upon failure of the licensing tunnel, each of the VDRs allocated at the mobile gateway are interrupted.

20. The system of claim 14, wherein the key information is associated with a community of interest of which the mobile device is a member based on the received authentication credentials.

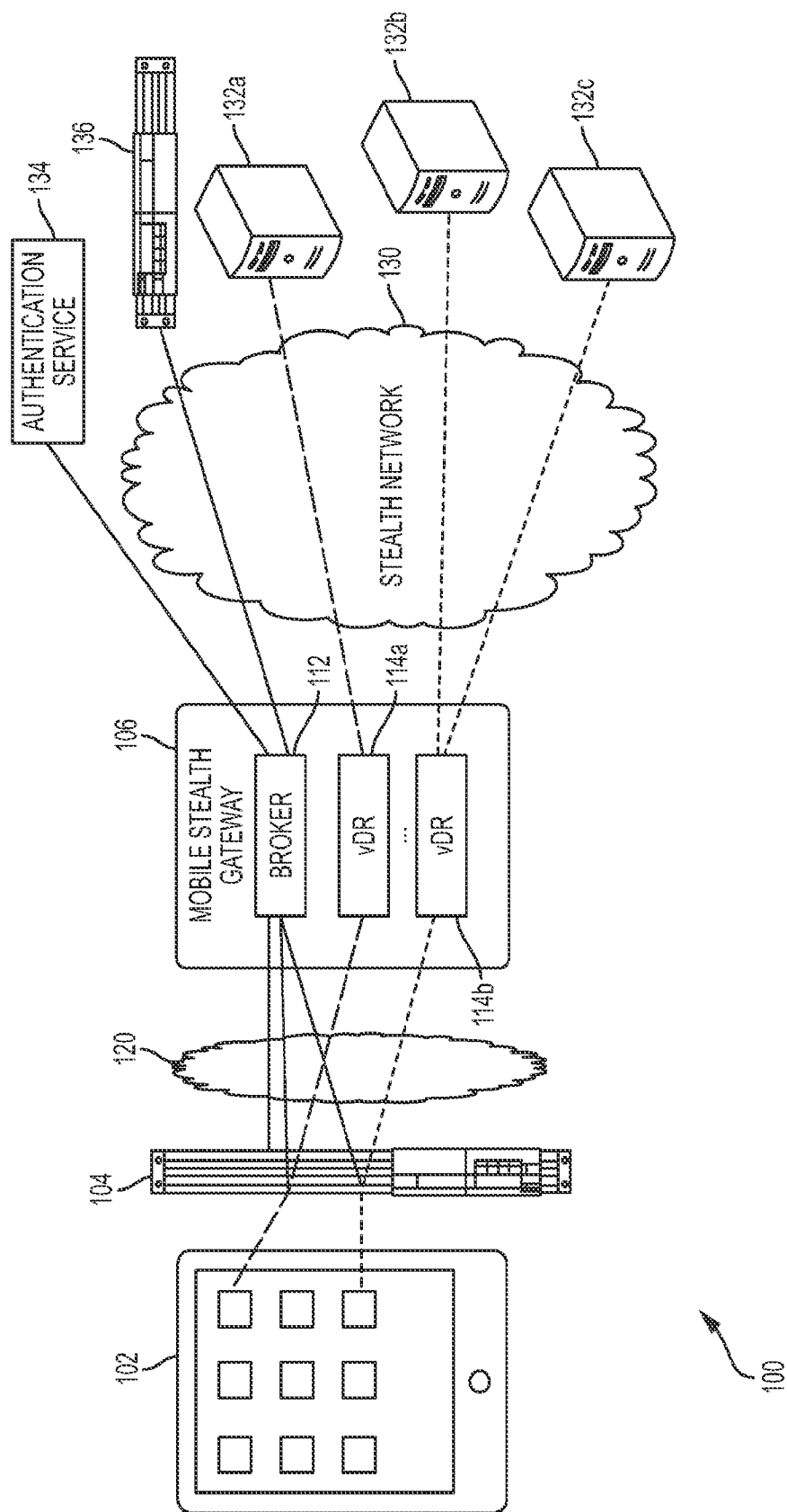


FIG. 1A

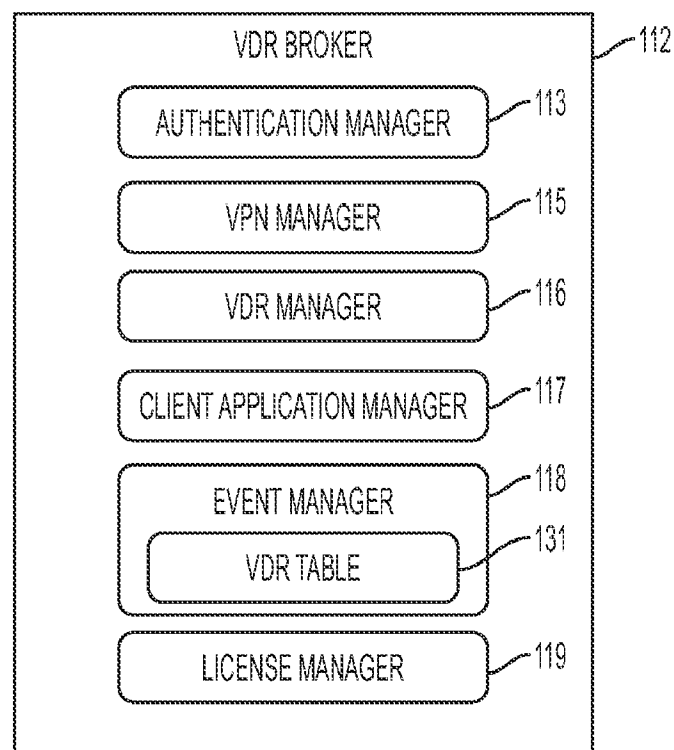


FIG. 1B

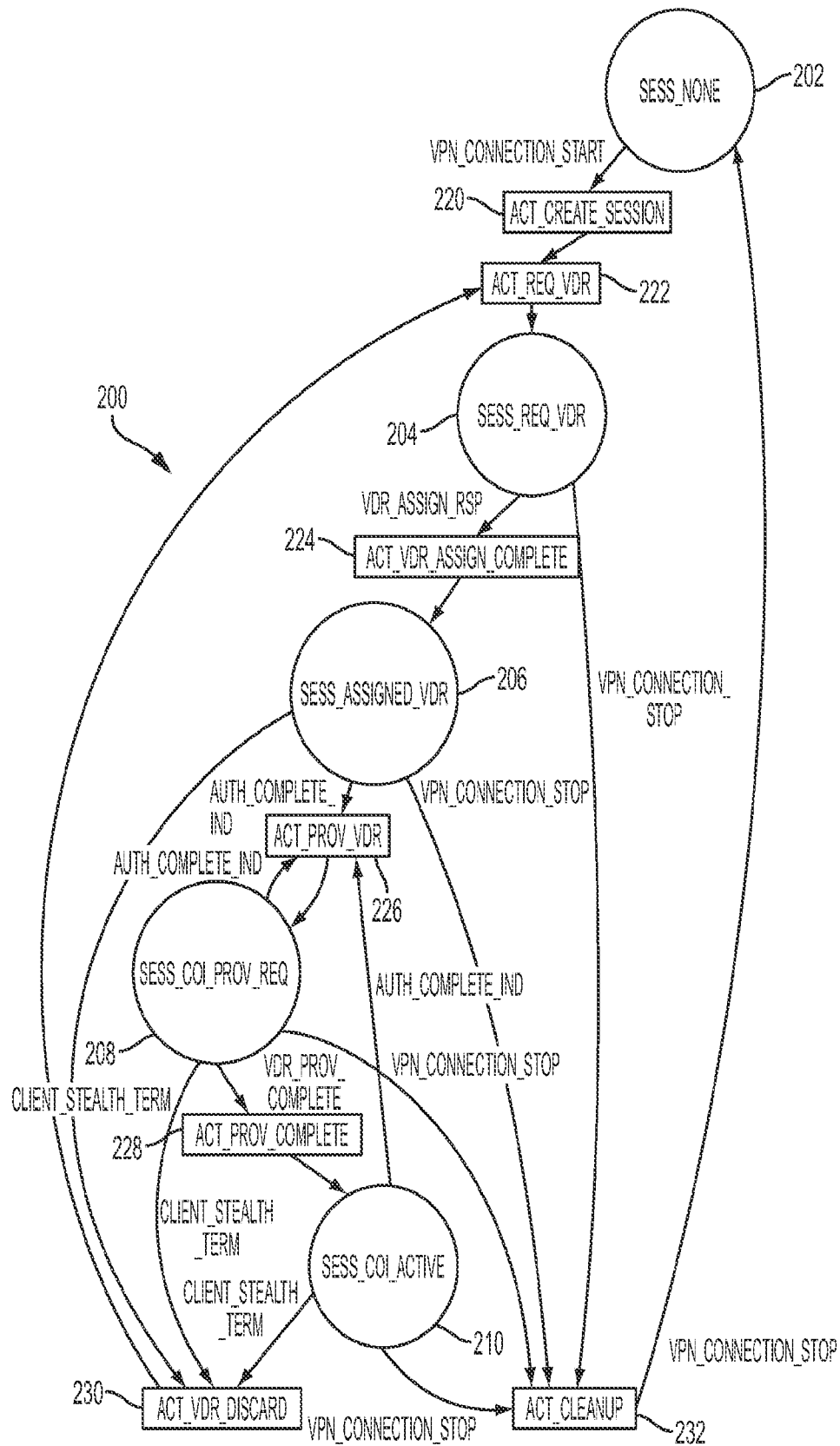


FIG. 2

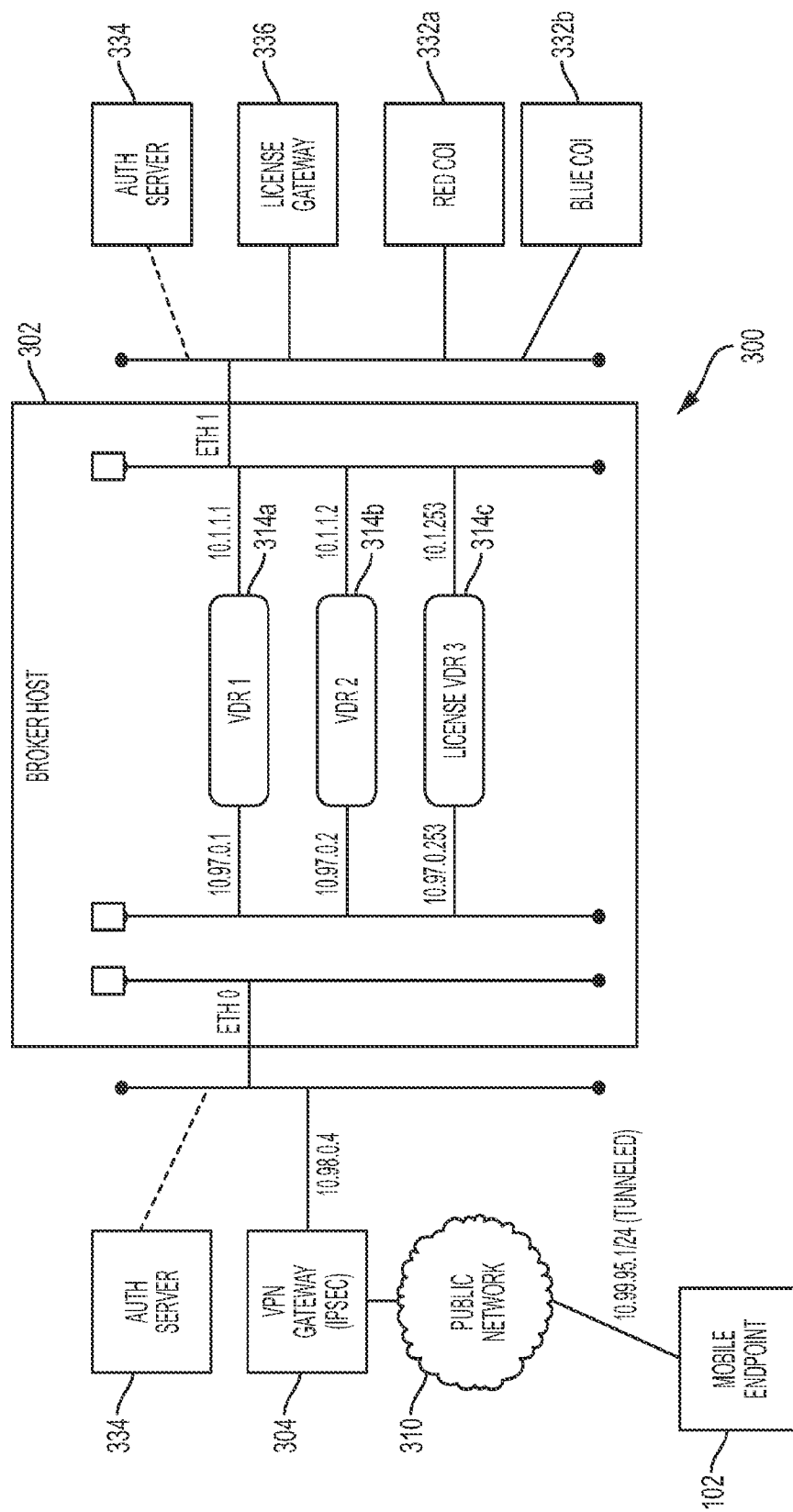


FIG. 3

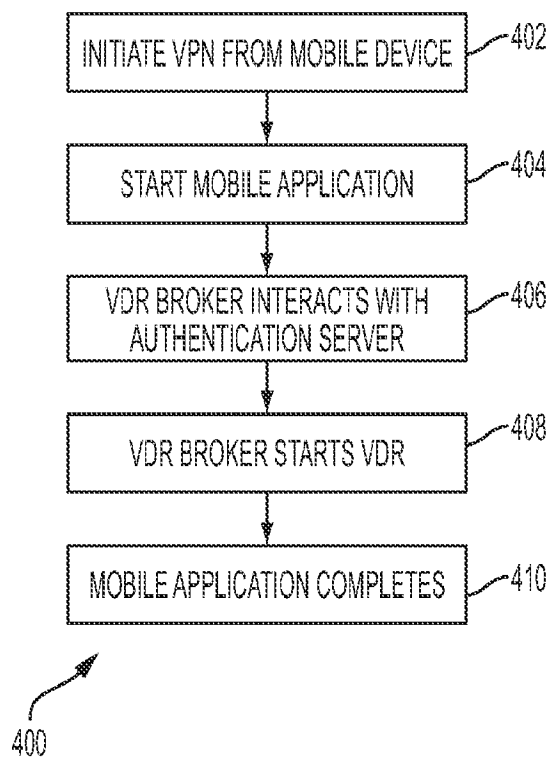


FIG. 4

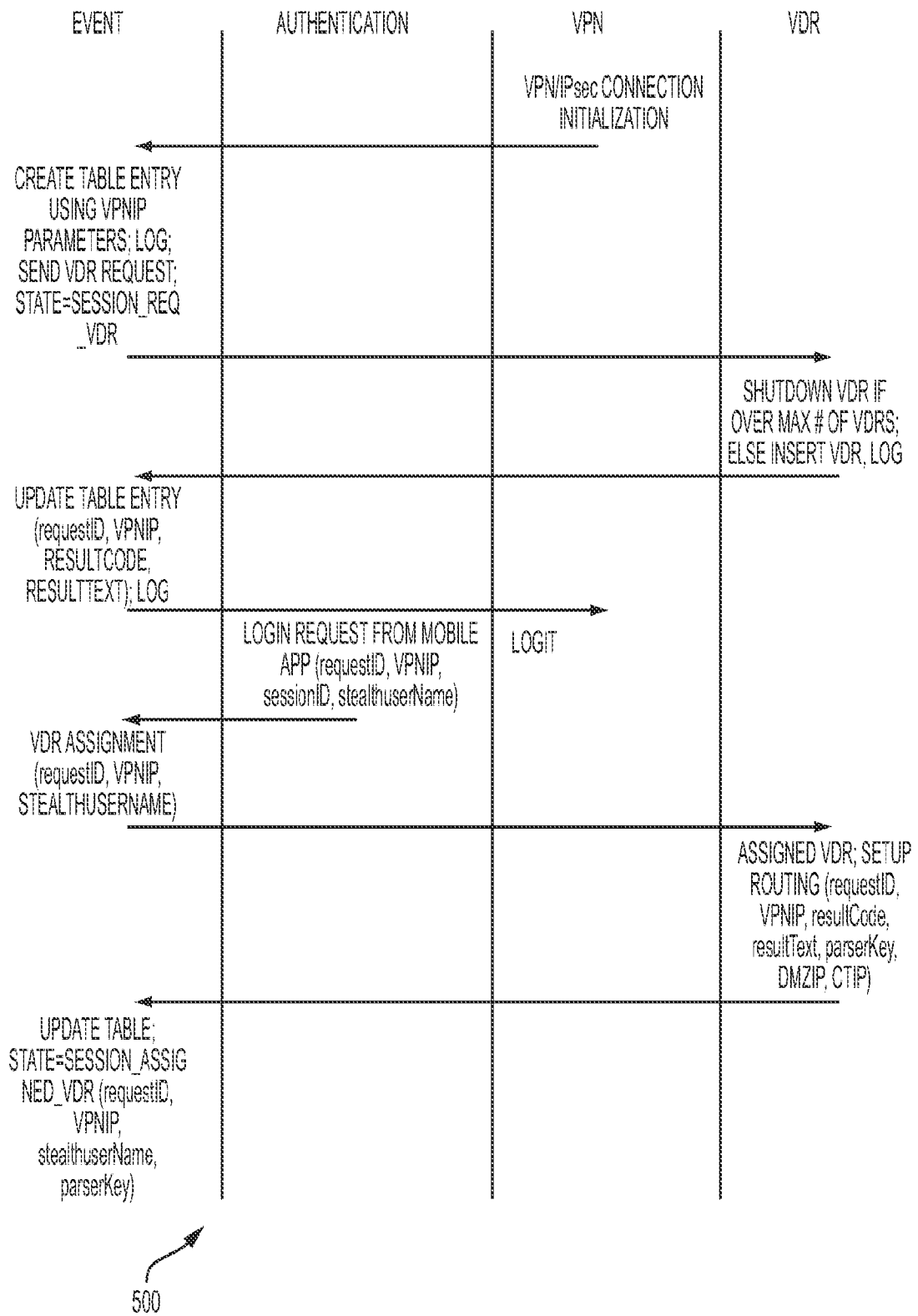
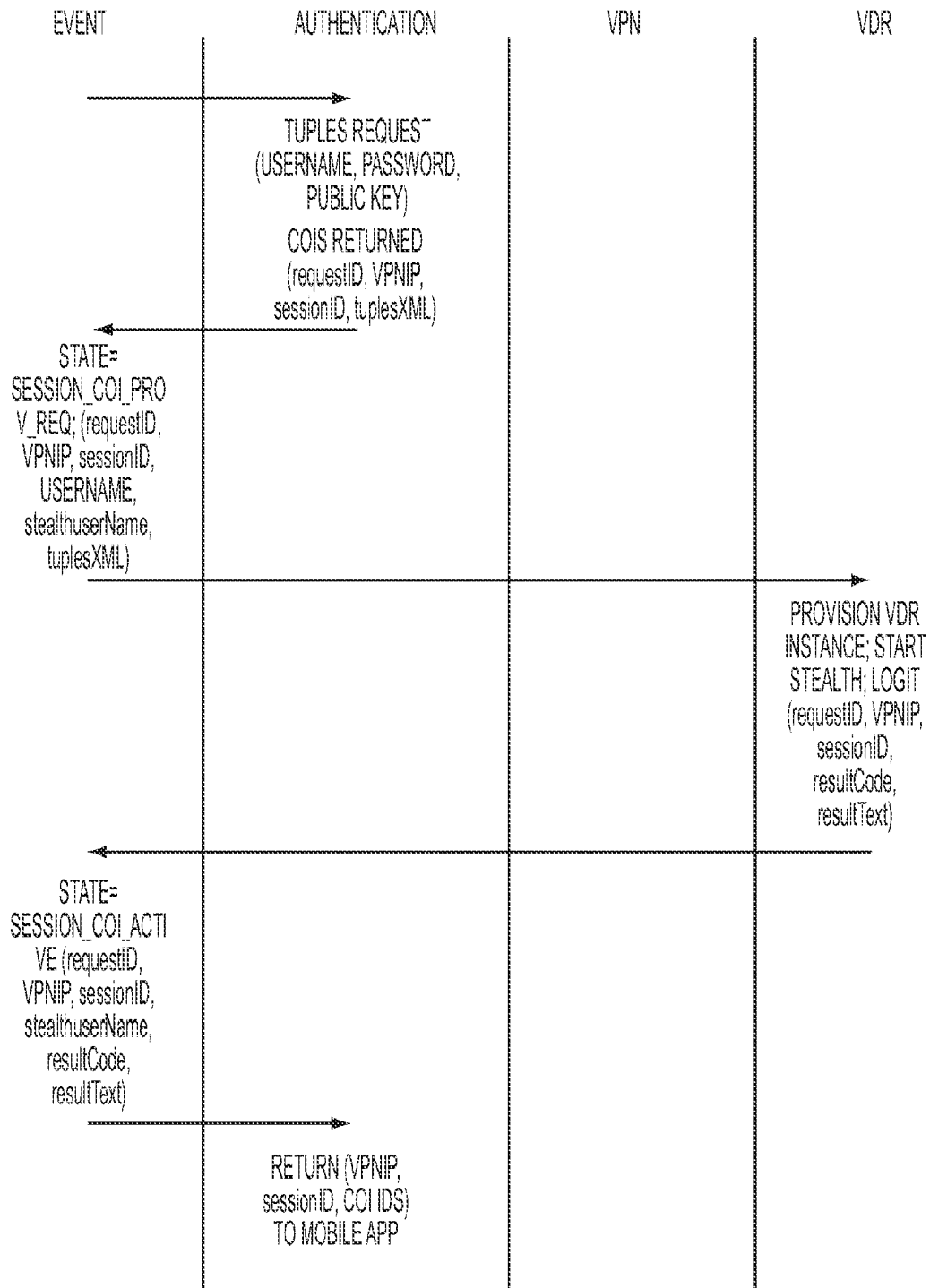


FIG. 5A



500

FIG. 5B

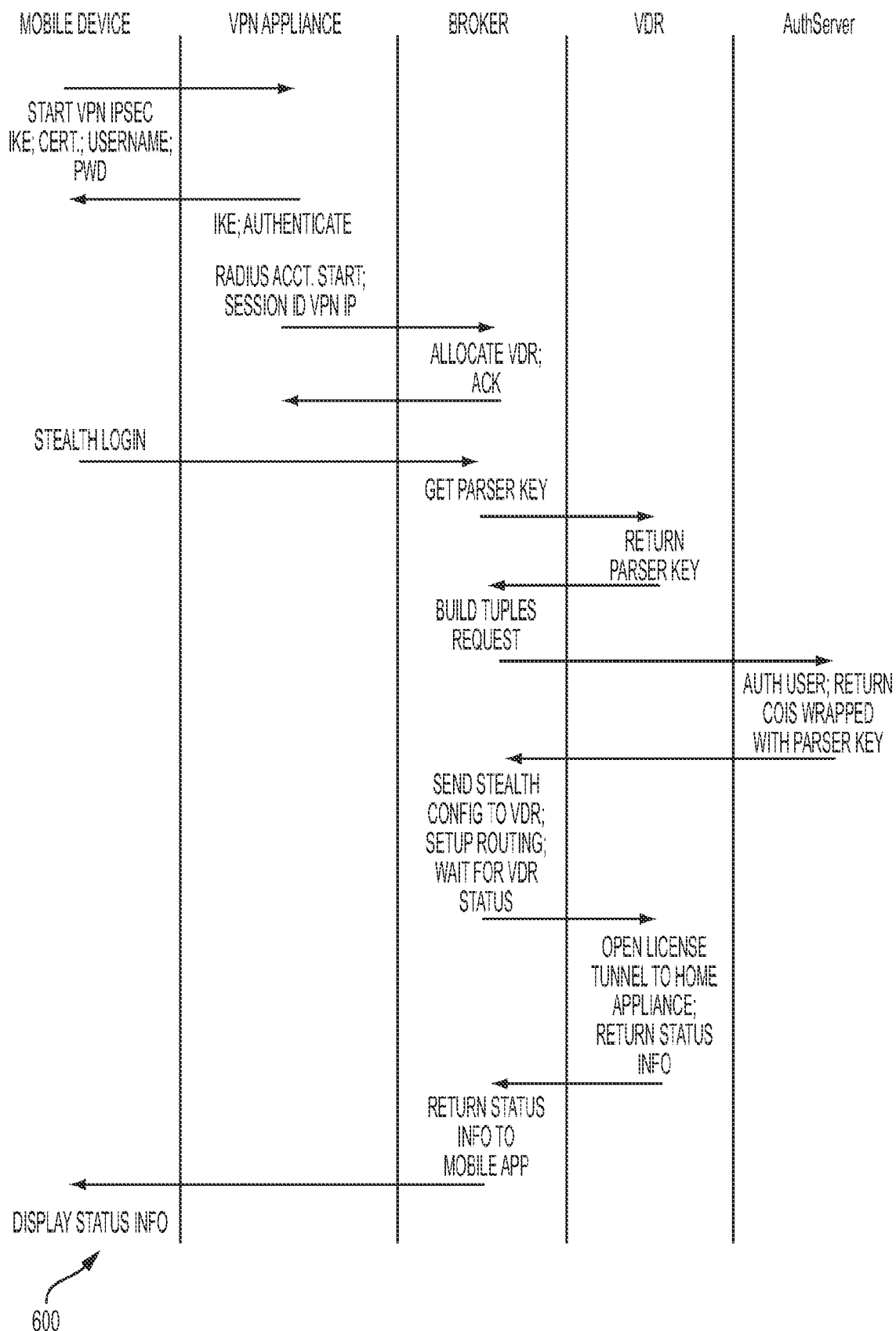


FIG. 6A

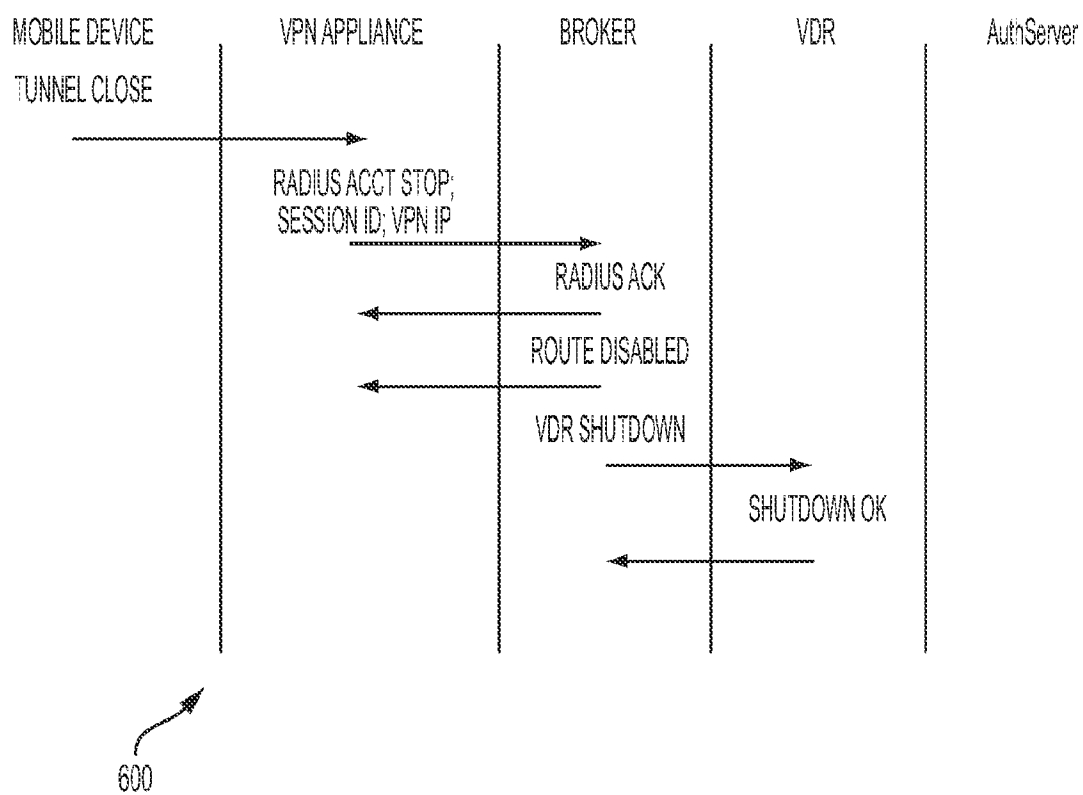


FIG. 6B

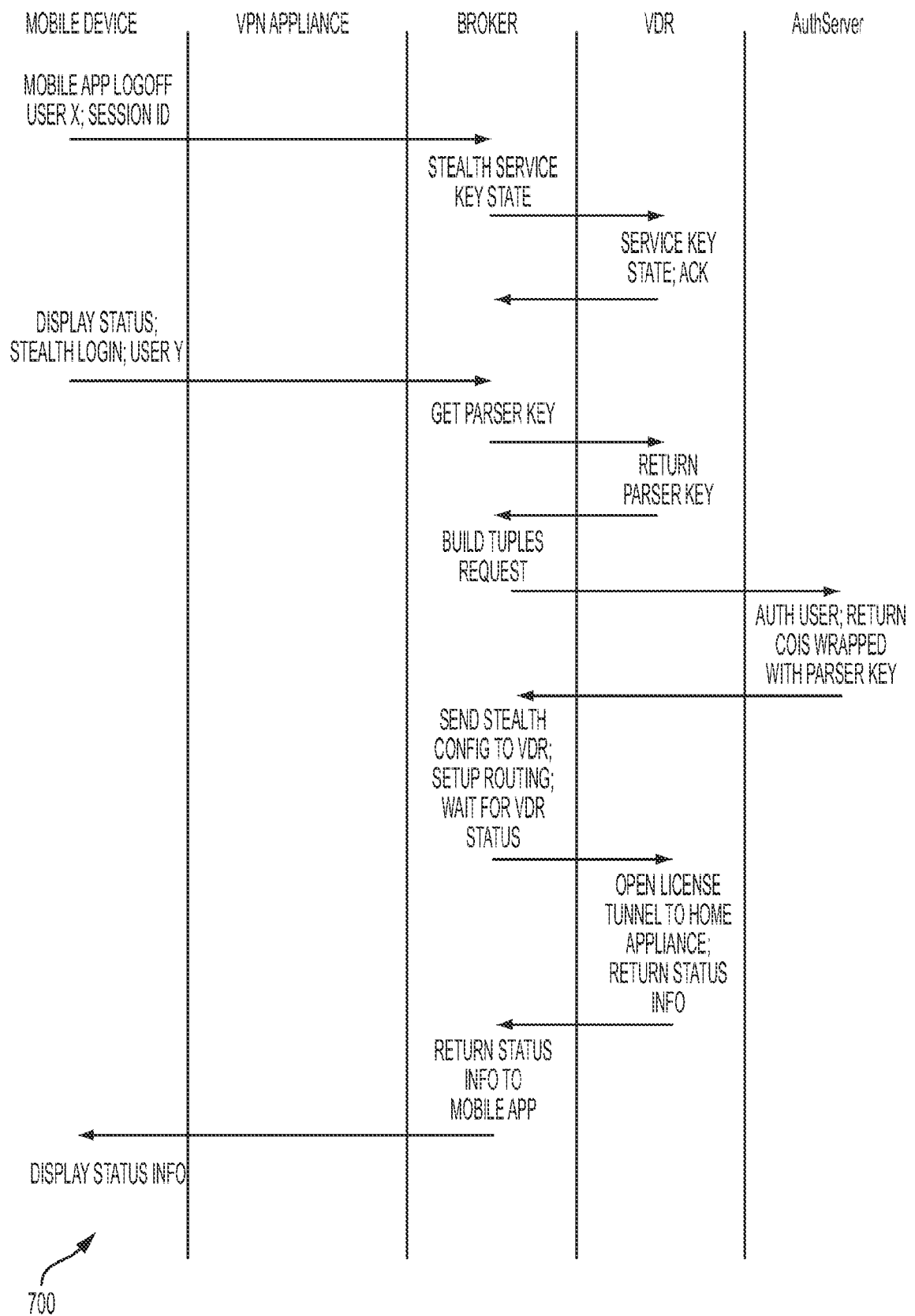


FIG. 7

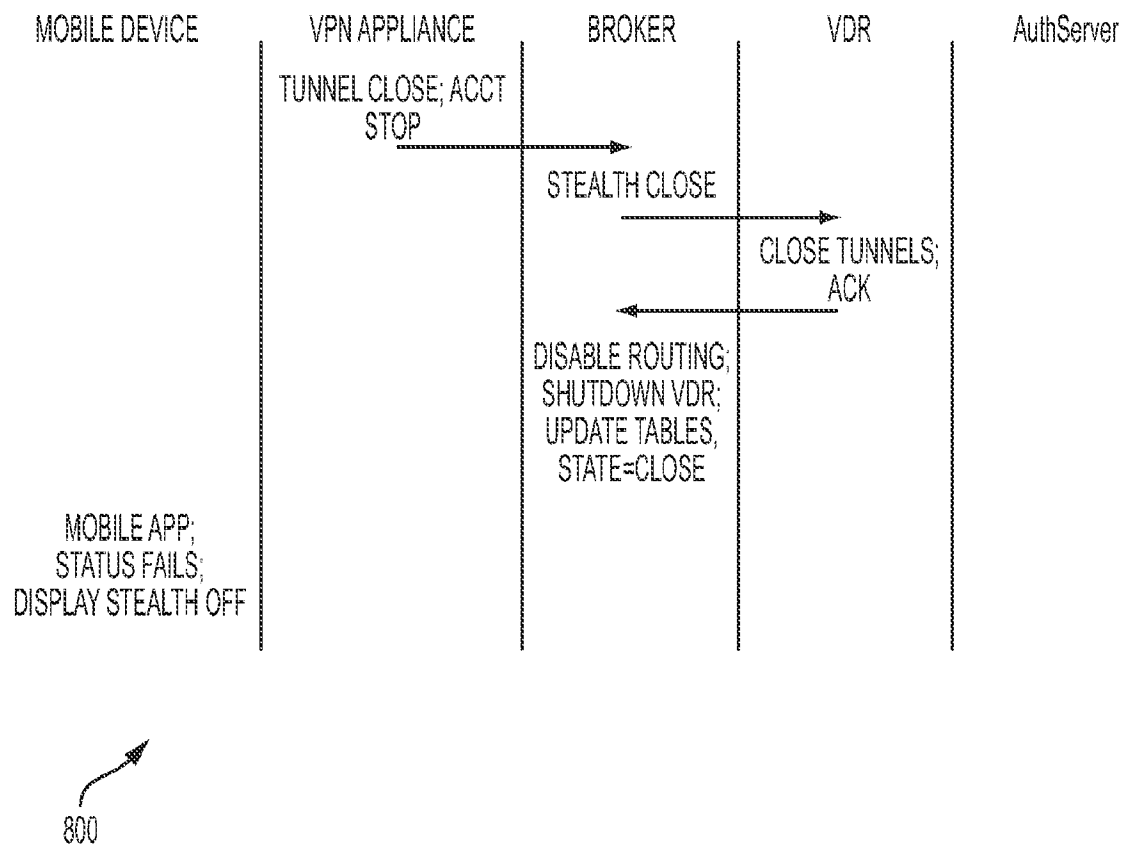


FIG. 8

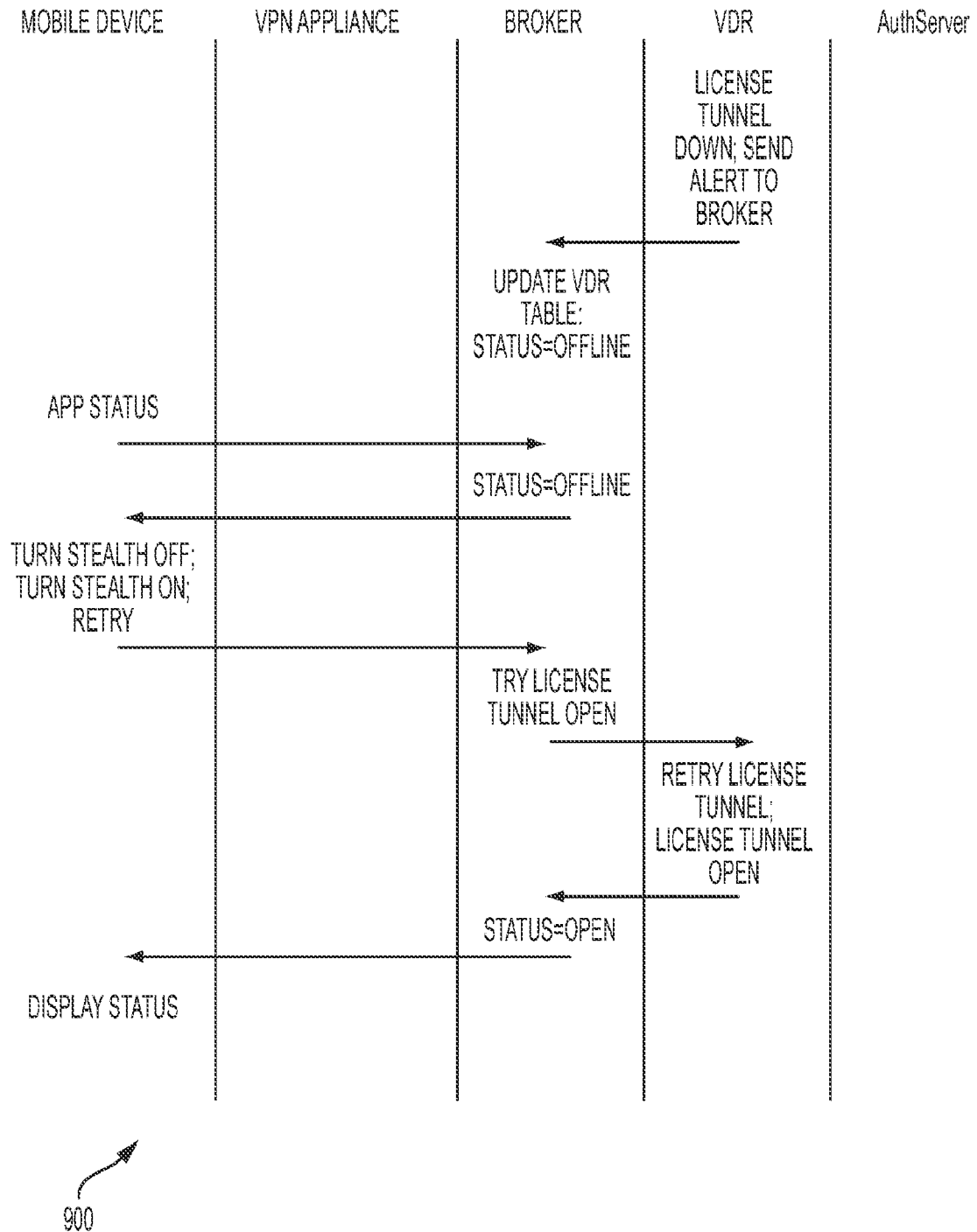


FIG. 9

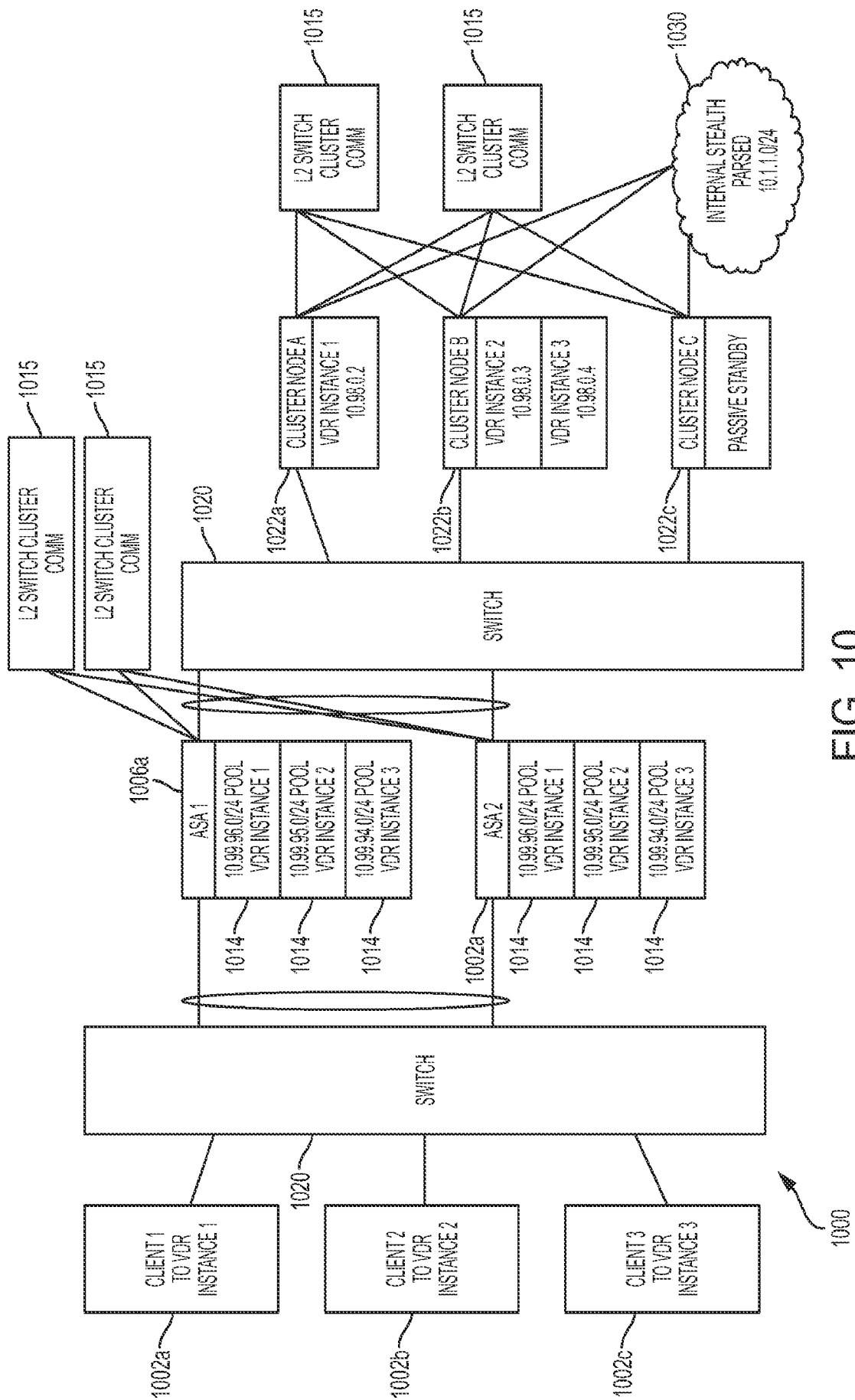


FIG. 10

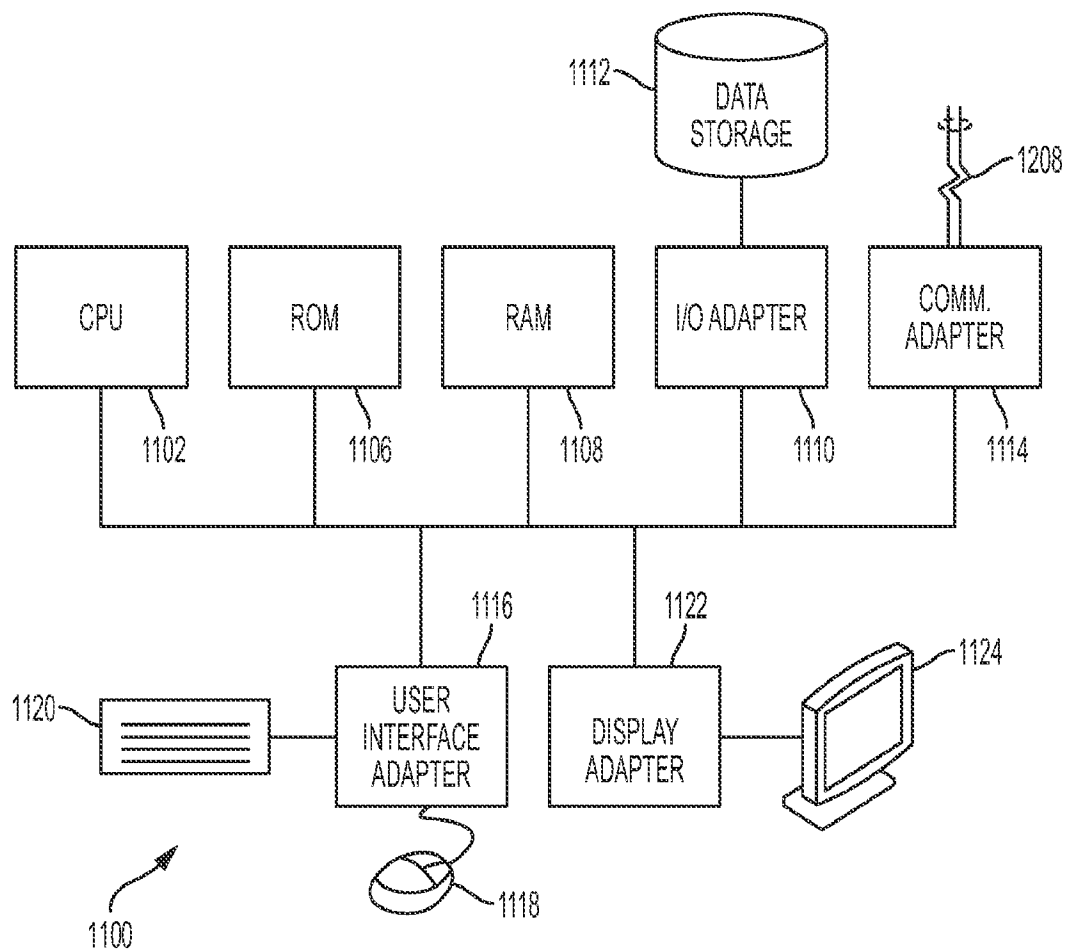


FIG. 11

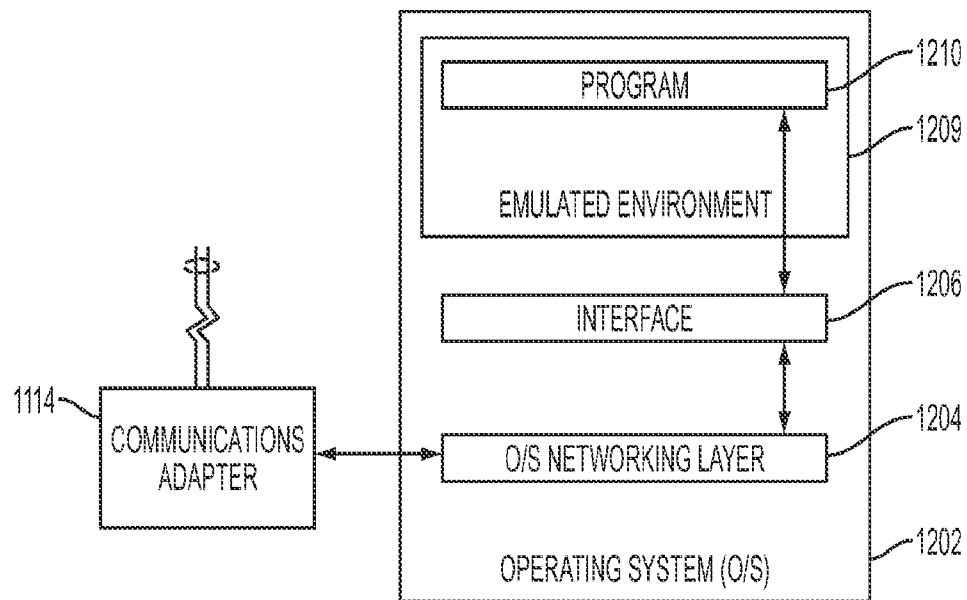


FIG. 12

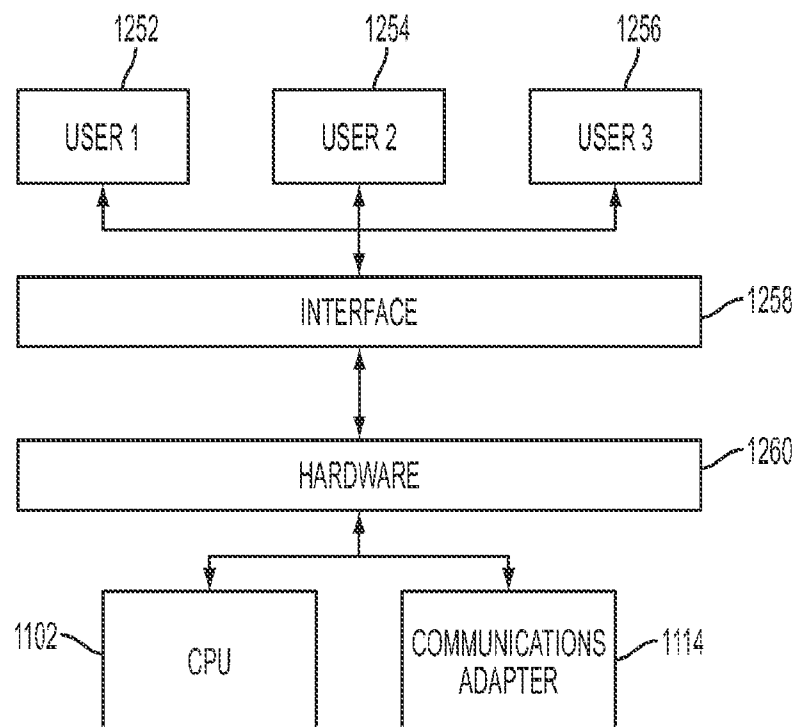


FIG. 13

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/038239

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/08
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/123268 A1 (FARINA RALPH [US] ET AL) 1 May 2014 (2014-05-01)	1-3,7-20
Y	paragraph [0006] - paragraph [0044] figures 3,4	4-6
Y	----- US 2013/133043 A1 (BARKIE ERIC J [US] ET AL) 23 May 2013 (2013-05-23) paragraph [0059] - paragraph [0062] -----	4-6
A	US 2013/291086 A1 (PONTILLO MICHAEL SCOTT [US] ET AL) 31 October 2013 (2013-10-31) paragraph [0055] -----	4-6



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 September 2015

Date of mailing of the international search report

07/10/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ströbeck, Anders

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2015/038239

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014123268 A1	01-05-2014	US 2014123268 A1 WO 2014070815 A1	01-05-2014 08-05-2014
US 2013133043 A1	23-05-2013	NONE	
US 2013291086 A1	31-10-2013	NONE	