



(51) International Patent Classification:  
**G06F 15/16** (2006.01)

(21) International Application Number:  
PCT/IN2009/000486

(22) International Filing Date:  
3 September 2009 (03.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):  
**MCAFFEE, INC.** [US/US]; 3965 Freedom Circle, Santa Clara, California 95054 (US).

(72) Inventors; and

(71) Applicants : **NARASIMHAN, Srinivasan** [IN/IN]; 6th Main/341 MC Ramaiah City, JP Nagar 8th Phase, Bangalore 560076 (IN). **HEJMADI, Parthiv** [IN/IN]; 565/4, 6th Cross, 7th Main, HAL 2nd Stage, Bangalore 560008 (IN). **PORWAL, Vinod Kumar A.** [IN/IN]; G6 Sai Gokul Apartments, 14th Main, 4th Block Jayanagar, Bangalore 560011 (IN). **SREENATH, Sheshadri** [IN/IN]; 1490, Southbend B road, 9th Block Jayanagar, Bangalore 560069 (IN).

(74) Agents: **WILSON, Neeti** et al; Anand And Anand, B-41, Nizamuddin East, New Delhi 110013 (IN).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: NETWORK ACCESS CONTROL

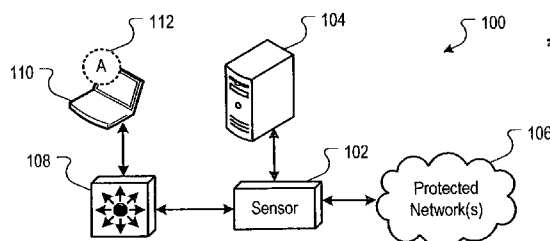


FIG. 1

(57) Abstract: Methods, systems, and apparatus, including computer programs encoded on a computer storage medium, for allocating probing responsibilities between a primary sensor and a secondary sensor. In one aspect, a method includes determining a first probe type, the first probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the primary sensor, determining a second probe type, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor, determining whether the second probe type is prioritized higher than the first probe type, and allocating probing responsibilities between the primary sensor and the second sensor based on the prioritization of the first probe type and the second probe type.



## NETWORK ACCESS CONTROL

### BACKGROUND

This specification relates to network access control.

5           Network access control involves regulating access to network resources based on a hosts' health, the identity of a user logged on to the host, or combination of both. As used herein, the term "host" refers to any computer device that is attempting to gain access to a protected network, or that has access to the protected network. A host can be a personal computer, a mobile communication device, a server computer in another network, or any  
10           other computer device capable of accessing the protected network. A network access control system protects a network by identifying, assessing, quarantining, and remediating host devices prior to network access and during network access.

          The network access control system includes network sensors that are deployed on  
15           the edge of a protected network or within the network, and one or more network access control servers in data communication with the network sensors. The sensors detect new host devices attempting to gain access to the network and monitor host devices that have been granted access to the network. The sensors report to the network access control server(s) when new host devices are attempting to gain access to the network, and report  
20           actions taken by the host devices. The sensors can take actions with respect to a host device immediately, or can take actions with respect to the host device as determined by the network access control server(s), depending upon the health of the host device and the identity of the user that is logged onto the host device.

25           When a host device is first attempting to join a network, a sensor must collect information about the host device. Such host information collection is conducted during a host information collection phase. Each sensor has at its disposal one or more information probes that can be used to collect information from a host device. Furthermore, if the host device has installed upon it a network access control agent, the network access control  
30           agent can periodically provide beacons that include information about the host device. As there are several different types of information probes that the sensor can use to collect

host information, determining how to effectively and efficiently send the information probes to the host device and process the replies can be challenging.

In addition, when a host device has been granted access to a network, the sensors  
5 monitor the host device for degradation of the host device health, for the logout of the user, and for when the host goes off-line and attempts to rejoin the network. Accordingly, the host device can go through multiple different states while attempting to access the network and after being granted access to the network. Determining how to manage the host device according to these various states is also challenging.

10 Additionally, in many network access control systems, sensors can be arranged in a failover configuration. In this failover configuration, a pair of peer sensors is used to control access to a network for host devices. One of the peer sensors is designated a primary sensor and the other peer sensor is designated a secondary sensor. To minimize  
15 network traffic, usually only one of the peer sensors is used to probe a host device, and the host status information received at the probing peer sensor is then provided to the non-probing peer sensor. However, one of the peer sensors may have a more reliable communication channel with the host device, or may have a communication channel that facilitates a more robust information probe than the other peer sensor. Accordingly,  
20 determining which of the peer sensors should be used to probe the host device can present the design challenge.

Furthermore, there are situations in which the probing peer sensor may be unable to communicate with the host device. For example, a firewall may be enabled that  
25 interferes with the probing peer sensors queries, or the host device may go off-line. How the pair of peer sensors responds to the probing sensor detecting the host going off-line can depend on the information probes that each peer sensor can use to probe the host device, and whether the primary peer sensor or the secondary peer sensor is the probing peer sensor. Accordingly, determining how the pair of peer sensors should respond to the  
30 probing peer sensor's failure to communicate with the host device should take into account these factors.

Each of the sensors stores a host table that includes a record for each host device that the sensor is monitoring. The record includes information such as the identity of the host, e.g., an IP address, or a MAC address, etc., the identity of the user logon to the host, e.g., a user identifier, and optionally other host device information. The host tables of the peer sensors are synchronized, as the probing peer sensor provides host device information to the non-probing peer sensor. In the event of one of the peer sensors failing, or in the event of a communication link between the peer sensors going down, the host tables of the peer sensors must be synchronized after recovery. As the status of the monitored host devices may have changed while a sensor was rebooting or while the communication link between the peer sensors was recovering, determining which host records in the host table need to be updated and which records do not need to be updated presents design challenges.

Finally, despite numerous security measures, there is always the potential for replay attacks. A replay attack is a form of a network attack in which information for credentials is delayed and/or fraudulently repeated at a later time. An attacker typically intercepts IP traffic to capture the credentials being transmitted from a host device, and then presents the credentials as their own. A common defense against a replay attack is the use of a nonce. For example, when a sensor provides an access portal to facilitate a user login from a host device, or queries an agent on the host device, the sensor will send a nonce to the host device when requesting authentication information, e.g., when requesting a user identifier and password within the HTTP 401 authentication realm, or provide a nonce with the agent query. The host device, in turn, sends a reply that includes an authentication code. When providing login credentials, such as a user identifier, the authentication code is a hash of the user's password and the nonce. The sensor then checks the authentication code by hashing the user's password and the nonce. Provided the hashes match, access is granted. Likewise, a reply to the agent query can include a hash that is, in part, based on the nonce. As the sensor provides a new nonce with each presentation of the access portal or with each agent query, replay attacks are thwarted.

Nonces are typically generated using pseudorandom number generators so that attackers cannot predict what the next nonce will be. However, use of pseudorandom

number generators can be processor intensive. Additionally, the sensor may handle many authentication requests, and thus generating a new random number for each authentication request can be expensive in terms of processing resources.

## SUMMARY

5           In general, one innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of receiving data at the data processing apparatus indicating a host device is connecting to a network; in response to the host device connecting to the network, initiating a host detection phase for the host device during which host attributes of the host are collected by the data processing  
10           apparatus and network access for the host device is restricted, and during the host collection phase for the host device: transmitting a plurality of information probes to the host device, the information probes including an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes requesting one or more other host attributes, monitoring for replies to the  
15           information probes from the host device during the host detection phase, ending the host detection phase in response to receiving a reply to the agent probe that includes the unique agent identifier, resending the plurality of information probes and incrementing a repeat counter in response to not receiving a reply to the agent probe after the expiration of a time period; and ending the host detection phase in response to a value of the repeat counter  
20           exceeding a maximum repeat value. Other embodiments of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

          Another innovative aspect of the subject matter described in this specification can  
25           be embodied in methods that include the actions of generating, by the data processing apparatus, a source value; hashing, by the data processing apparatus, the source value to generate a nonce; providing, by the data processing apparatus, the nonce with a query over a network; receiving, in response to the query, reply data and an authentication code; hashing a combination of the reply data and the nonce to generate a digest; and  
30           determining the reply is authentic if the digest matches the authentication code. Other embodiments of this aspect include corresponding systems, apparatus, and computer

programs, configured to perform the actions of the methods, encoded on computer storage devices.

Another innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of generating, by the data processing apparatus, a plurality of source values; hashing, by the data processing apparatus, the source values to generate hash values; generating, by the data processing apparatus, a nonce from the hash values; providing, by the data processing apparatus, the nonce with a query over a network; receiving, in response to the query, reply data and an authentication code; hashing, by the data processing apparatus, a combination of the reply data and the nonce to generate a digest; and determining, by the data processing apparatus, the reply is authentic if the digest matches the authentication code. Other embodiments of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

Another innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of storing in the memory of the data processing apparatus a host table, the host table including, for each of a plurality of host devices monitored on a network, a record including: an IP address field for storing an IP address assigned to the host device, an agent identifier field for storing an agent identifier of agent installed on the host device, and a time stamp field for storing a time stamp indicating the time that host attributes were stored in the record; receiving from a peer data processing apparatus, in response to a synchronization event, a peer record for a host device, the peer record comprising data for a record stored in a host table in the memory of the peer data processing apparatus; determining whether an IP address of the peer record is stored in a record in the host table; in response to determining that the IP address of the peer record is not stored in a record of the host table: determining whether the peer record includes an agent identifier; in response to determining that the peer record includes the agent identifier, determining whether the agent identifier of the peer record is stored in a record of the host table; in response to determining that the agent identifier of the peer record is stored in a record of the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the

time stamp of the records in the host table; and in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with data of the peer record. Other embodiments of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

Another innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of defining a state machine in a memory of the data processing apparatus, the state machine comprising a plurality of states, and wherein network access for a host device is controlled in each state according to one or more network access zones associated with the state, each network access zone defining network access capabilities for the host device; monitoring, by the data processing apparatus, host devices attempting to access the network and host devices that have access to the network; transitioning, for each host device, a state of the host based on the monitoring and a current state of the host; storing in the memory of the data processing apparatus, for each monitored host device attempting to access the network or that has access to the network: host attributes of the host device that identify the host, and the state of the host; and controlling network access of the host device according to the one or more network access zones associated with the state of the host device. Other embodiments of this aspect include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

Another innovative aspect of the subject matter described in this specification can be embodied in methods that include the actions of: in response to a detection of a host device attempting to access a network, transmitting, from each of a primary sensor and a secondary sensor, a plurality of information probes to the host device, each of the information probes being prioritized according to their probe types by the primary sensor in a descending priority order; determining, at the primary sensor, a first probe type, the first probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the primary sensor; determining, at the secondary sensor, a second probe type, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at

the secondary sensor; transmitting, from the secondary sensor, data indicating the second probe type to the primary sensor; determining, at the primary sensor, whether the second probe type is prioritized higher than the first probe type; in response to determining the second probe type is prioritized higher than the first probe type, transmitting, from the primary sensor, data indicating a probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor; and transmitting subsequent information probes to the host device from the secondary sensor.

The details of one or more embodiments of the subject matter described in this specification are set forth in the accompanying drawings and the description below. Other features, aspects, and advantages of the subject matter will become apparent from the description, the drawings, and the claims.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of an example deployment architecture of a network access control system.

Fig. 2 is a block diagram of another example deployment architecture of a network access control system.

Fig. 3 is a block diagram illustrating a system health based network access control process.

Fig. 4 is a block diagram illustrating an identity based network access control process.

Fig. 5 is a block diagram illustrating a host information collection phase in the network access control system.

Fig. 6 is a flow diagram of an example process of collecting host information from a plurality of information probes.

Fig. 7 is a state diagram for a host state machine that is used to control network access of the host device.

Fig. 8 is a block diagram of two sensors configured in a failover configuration.

Figs. 9A and 9B are flow diagrams of an example process for synchronizing host tables in a pair of peer sensors.

Fig. 10 is a flow diagram of an example process for allocating probing responsibilities among a pair of peer sensors.

Fig. 11 is a timing diagram of a nonce-based authentication process.

Fig. 12 is a flow diagram of an example process for generating a nonce.

5 Fig. 13 is a flow diagram of another example process for generating a nonce.

Like reference numbers and designations in the various drawings indicate like elements.

## DETAILED DESCRIPTION

### § 1.0 Network Access Control System Overview

10 A network access control system protects a network by identifying, assessing, quarantining, and remediating host devices prior to network access, and during network access. The network access control system includes network sensors that are deployed on the edge of a protected network or within the network, and one or more network access control servers in data communication with the network sensors.

15 As used herein, a sensor device, also referred to as a sensor, is a hardware device in a data communication path between a host device joining a network and the network resources that the host devices are attempting to access. An example sensor device includes one or more processors, a memory subsystem, and an input/output subsystem.

20 The one or more processors are programmed according to instructions stored in the memory subsystem, and monitor the network traffic passing through the input/output subsystem. The one or more processors are programmed to take one or more protective actions on their own, or to query the network access control server and take further actions as instructed by the network access control server.

25 The network access control server is one or more server computers, each of which include one or more processors, a memory subsystem, and an input/output subsystem. The network access control servers are programmed to communicate with the sensors and to determine actions to be taken based on the user that is logged onto the host device and

30 the health level of the host device, to provide configuration data to the sensor devices and updates to the sensor devices, and to query identity databases, such as an LDAP database.

These functions can be distributed among different servers running different software components, or can be consolidated in a single server.

In some implementations, network access zones that define network access capabilities for the host device can be employed, allowing different access capabilities for host devices. The access capabilities of a network access zone can depend upon the system health of the host device, the user identity of the user login using the host device, and other factors, such as whether the user has logged in through a virtual private network (VPN).

In some implementations, such as those described in the deployment architectures 100 and 200 of Figs. 1 and 2 below, a software agent of the network access control system can be installed on the host device to assess the health of the host device. As used herein, the health of host device, or health level of the host, refers to the configuration of the host with respect to a specification defining a minimum set of up-to-date security software in the host device. Depending on the differences between the configuration of the host device and this specification, the agent, or another process that receives data from the agent specifying the host device configuration, can classify the hosts into one of several health level categories. In some implementations, the health level category can be a binary category, such as healthy and unhealthy, or can have several levels of categories, such as healthy, fair, poor, serious, and critical. Finally, if the health level of the host device cannot be determined, the health level of the host device can be classified as unknown, or alternatively, can be classified according to the lowest health level, e.g., failing or critical. Depending upon the health level the host and, optionally, the identity of the user logged into the host, different network access capabilities can be provided to the host device.

The sensors are deployed in line, i.e., directly in the network traffic path, inspecting all traffic as it passes through the sensor. In this mode, packet inspection is performed in real-time, and intrusive or malicious packets are dropped as they occur. Furthermore, in this mode, the sensor can redirect traffic of a host device, or limit traffic of a host device.

### § 1.1 Layer 2 Deployment

Fig. 1 is a block diagram of an example deployment architecture 100 of a network access control system. This example deployment architecture is referred to as "Layer 2" or "L2" mode. The sensor 102 is connected to a host device 110 through a Layer 2 switch device 108. In this mode, the sensor 102 identifies a host device based on its MAC address, and collects information from a host device 110 by use of a network access agent 112. When the host device 110 attempts to connect to the network 106, the sensor 102 sends an information probe to the agent 112. The information probe is an agent query, and in response to the information probe, the agent 112 provides an agent identifier of the agent, the MAC address of the host device 110, user login information associated with the host device 110, and other information, such as data indicating a health level of the host device 110. In some implementations, the agent identifier is a unique identifier, i.e., each agent used by the network access control system has a unique identifier that is not used by other agents.

The sensor 102 is also in communication with a network access control server 104. As described above, the network access control server 104 is programmed to communicate with the sensors and to determine actions to be taken based on the user that is logged onto the host device and the health level of the host device, to provide configuration data to the sensor devices and updates to the sensor devices, and to query identity databases, such as an LDAP database. These functions can be also be distributed among two or more servers; however, to avoid congestion in the drawings, a single server 104 is shown.

Together the sensor 102 and the network access control server 104 provide protection and access control for one or more protected networks 106. Examples of such protected networks include corporate local area networks (LANs), corporate wide area networks (WANs), and other networks for which access to the network can be controlled.

### § 1.2 Layer 3 Deployment

Fig. 2 is a block diagram of another example deployment architecture 200 of a network access control system. This example network architecture is referred to as a "Layer 3" or "L3" deployment mode. In this mode, the sensor 102 detects a host device

based on the IP address of the host device. In this mode, host devices 110 can connect to the sensor by use of a Layer 2 switch 108, or a Layer 3 switch 109 and the router 120. Additionally, host devices 110 can also connect to the sensor 102 through a virtual private network. For example, a host device 110 can connect to the sensor 102 through the Internet 130 and a VPN concentrator 134. In this mode, layer 2 devices are also detected by their IP addresses, i.e., layer 2 devices are treated as layer 3 devices.

Because this mode is at the network layer, the sensor 102 can use additional information probes to collect information from host devices 110. For example, in addition to an agent query, the sensor 102 can also use NBTSTAT queries to collect information from a host. Additionally, the sensor 102 can use ICMP pings to determine if a host device is on-line or off-line.

Note, however, that the sensor 102 may not be able to use all of these information probes for all host devices 110, depending on the communication path in the session established for each host device 110. For example, a firewall 132 may interfere with one or more probe types.

Other deployments can also be used. For example, the sensor 102 can be configured to use both layer 2 and layer 3 detection modes. In this mode, the deployment architecture is similar to that of Fig. 2. MAC addresses and layer 3 devices, e.g., a router or firewall, are specified in the layer 3 device list. Traffic that has any the MAC addresses specified in the layer 3 device list is treated as coming from a remote network, and the layer 3 detection mode is used. Conversely, traffic that does not have any of the MAC addresses specified in the layer 3 device list is treated as coming from a local network. In this case, the layer 2 detection modes used.

### § 1.3 Health-Based Network Access Control

Fig. 3 is a block diagram illustrating a system health based network access control process 300. The sensor 102 detects a new host 110 joining the network, and the new host 110 is moved to a preadmission zone 302. In a preadmission zone, the network access control system determines the health level of the host device. Network access given to the

host device is limited to critical systems such as login portals and remediation portals, which are described in more detail below.

The sensor 102 queries the agent 112 on the host device 110. The agent 112, in turn, provides data to the sensor 102 for use in determining the health level of the host device 110. If the host device 110 has an agent 112 installed, the host device is considered a managed host device. Conversely, if the host device 110 does not have an agent 112 installed, it is considered an unmanaged host device. In some implementations, unmanaged hosts are redirected to a remediation portal 310 to download an agent 112. When the agent 112 is installed, the health level of the host 110 is determined and communicated back to the network access control server 104 and the sensor 102.

Once the health level of the host device 110 is determined, the sensor 102 maps the host device 110 to a network access zone. The particular network access zone can, for example, be dependent upon the health level of the host device 110. The sensor 102 then allows or drops traffic to and from the host device 110 given the network access zone assigned to the host device 110.

#### § 1.4 Identity-Based Network Access Control

Fig. 4 is a block diagram illustrating an identity based network access control process 400. The sensor detects a new host device 110 joining the network, and places the new host device in the preadmission zone until a user of the host device 110 is authenticated. In some implementations, the identity of the user can be implicitly authenticated, such as by sending a query to the agent 112, snooping traffic of the host device 110, by listening to beacons transmitted from the agent 112, or by examining VPN session data, such as capital RADIUS accounting messages. If the user identity cannot be authenticated implicitly, the sensor 102 redirects the host device to a client guest portal 410, where the user is prompted to submit login credentials for authentication.

Example user data and host information that the sensor 102 obtains can include the following: a user identifier, which is an identifier that is uniquely associated with a user; a source IP address, a MAC address, or a VLAN address, depending upon how the user is

connected to the network; and whether the host device 110 is a managed host or an unmanaged host.

Once the identity of the user is obtained, the user attributes and values are compared to attributes and values stored in a predefined directory, such as an LDAP database 412, e.g., implemented in an active directory server. Assuming the user is authenticated, identity-based policies are applied to the host device when the user is lagged in. For example, user identifiers are mapped to a user role associated with a corresponding network access zone, e.g., host devices 110 of users that are mapped to the role of network administrators may have applied to them a network access zone in which all network access capabilities are available. Conversely, host devices of users that are mapped to the role of salespersons may have applied to them a network access zone in which network access capabilities are restricted to certain parts of the network.

#### § 2.0 Host Information Collection

As described above, the sensor 102 and the network access control server 104 control the network access of a host device that joins the network. The access control is based on either the identity of the user who has logged on to that host device, the health of the host device, or both. Additionally, once the host device 110 is provided access to the network, the host device must be monitored for going offline, for IP address reassignments (e.g., the IP address being re-used by a different host device) and for other events or actions that may change the status of the host device.

The sensor 102 determines the identity and other critical information (e.g., a MAC address) describing the host device to facilitate implementing network access control. This is established during a "host information collection phase." In some implementations, the detection of a host device 102 is declared to the network access control server after completion of the host information collection phase.

Fig. 5 is a block diagram illustrating a host information collection phase 500 in the network access control system. As described above, the sensor 102 collects information from a host device 102 by way of information probes 502 and listening for replies 504 to

the information probes 502. Additionally, if an agent 112 is installed on a host device 110, the sensors 102 can listen for an agent beacon 506.

The types of information probes can vary based on the system architecture, operating system environment, and communication protocols supported. In some implementations, the sensor 102 can send an agent probe, an NBSTAT query, and an ICMP Ping. A response to the agent probe from the agent 112 provides the most detailed information about the host device 110. For example, in some implementations, the reply can provide the agent identifier, the MAC address, information about the user that is logged into the host device 110, the host name, and the network domain name. Additional information, such as health level information, can also be provide.

The agent beacon 506, in some implementations, also provides the same information as a reply to the agent probe. In other implementations, the agent beacon 506 can provide a proper subset of the information, such as the agent identifier and the MAC address.

The sensor 102 can also use an NBTSTAT query to request the MAC address and the host name of the host device 110. The ICMP ping is a probe that only provides the sensor 102 with confirmation that the host device is reachable over an IP network.

Due to various factors in the network, e.g., the firewall 132 not allowing agent queries, some of the information probes may not result in the sensor 102 collecting host device information, despite the host device 110 being capable of replying to these probes. To efficiently collect information, a host information collection algorithm is implemented in the sensor 102. Briefly, the sensor 102, when implementing the host information collection algorithm, begins a host information collection phase and sends all the probes to the host device 110 in response to detection of the host device 110 attempting to join the network.

If an identifier is obtained from a reply to the agent query the host info collection phase ends immediately. Conversely, if an agent identifier is not received after a timeout

period (e.g., 30 seconds, 1 minute, 5 minutes, or some other time period), all information probes that have not been responded to are resent. If, after a maximum number of retries, e.g., 3, the agent identifier is not provided to the sensor 102, the host info collection phase ends.

5

In some implementations, if an agent identifier is received from an agent beacon, the host information can also end immediately. For example, if the agent beacon sends the same information as a reply to the agent query, the agent beacon can be used to process the same information that is provided by the reply to the agent query.

10

Fig. 6 is a flow diagram of an example process 600 of collecting host information from a plurality of information probes. The process 600 can be implemented in the sensor 102.

15

The process 600 initiates a host detection phase (602). For example, in response to detecting a host device 110 attempting to join the network, the sensor 102 can initiate the host detection phase.

20

The process 600 transmits information probes to the host device (604). For example, the sensor 102 can transmit an agent query, and NBTSTAT query, and an ICMP ping to the host device 110.

25

The process 600 monitors for replies the information probes from the host device (606). For example, the sensor 102 listens for responses to the information probes. Additionally, the sensor 102 can also listen for agent beacons. If an agent 112 is installed on the host device 110, the agent will periodically send an agent beacon.

30

While monitoring, the process 600 determines if an agent identifier has been received (608). For example, the sensor 102 will determine if it has received a reply to an agent query, or if it has received an agent beacon, and if so, if the reply or the beacon include the agent identifier.

If an agent identifier is received, the process 600 ends the host detection phase (610). For example, the sensor 102 will notify the network access control server 104 of a new host device 110 joining network, and will initiate further network access control processing to join the host device 110 to the network (or preclude the host device 110 from joining the network, if necessary).

If, however, the agent identifier has not been received, then the process 600 determines if the timeout has occurred (612). For example, the sensor 102 will determine if a predefined time period, measured from when the information probes were sent, has expired.

If a timeout has not occurred, the process 600 returns to monitoring for replies (606); conversely, if a timeout has occurred, the process 600 increments a repeat counter (614) and determines if the repeat counter is greater than the maximum repeat value (616). For example, the sensor 102 can increment a repeat counter in memory and compare the value of the repeat counter to a maximum repeat value.

If the repeat counter is greater than the maximum repeat value, the process ends the host detection phase (610). For example, sensor 102 will end the host detection phase if the repeat counter exceeds the maximum repeat value. Depending on the information received from the host device 110, the sensor 102 can initiate further network access control processing to join the host device 110 to the network, providing only limited network access to the host device, or preclude the host device from joining the network. For example, if the host device 110 does not have an agent 112 installed, the host device may be redirected to client portal to install an agent 112. Optionally, the host device 110 may be redirected to a guest access portal to allow the user to provide user credentials to gain access to the network, or portion of a network.

Conversely, if the repeat counter is not greater than the maximum repeat value, then the process 600 retransmits information probes to the host device (618), and returns to monitoring for replies (606).

### S 3.0 Host State Machine

As the host device 110 connects to the network, it goes through a series of health assessments and/or identity authentications before it is allowed to join the network. Additionally, the host device 110 has a network access zone applied, depending on the health of the host device 110 and the identity of the user of the host device. As described above, when the identity of the user cannot be established implicitly, or when the system health can not be determined, traffic for the host device 110 is redirected to a guest portal 410 or a remediation portal 310, respectively. Once the identity is established through the guest portal 410 and/or the system health is established through the remediation portal 310,\* the sensor 102 will provide the host device 110 with the appropriate network access.

The phase where the identity and/or the system health are determined is referred to as a "preadmission" phase. The phase where network access is provided to the host device 110 is referred to as a "post admission" phase. While in the post admission phase, the host can go back to the preadmission phase based on a change in health, a change in user identity, an IP address reassignment, or by going off-line and attempting to rejoin the network. Furthermore, in each of the preadmission and post admission phases, different states occur. For example, during preadmission, the host device 110 goes through a host information collection phase, and may need to go through a login phase or a remediation phase. The choice of subsequent phases is dependent on the current state of the host device 110, the health level of the host device 110, and the identity of the user of the host 110 (if identity-based network access control is being used).

Thus, to effectively maintain an entry for the host device 110 in the sensor and take appropriate actions on the traffic from the host device 110, i.e., redirecting or dropping traffic, the sensor 102 needs to know the current state of the host device 110. Accordingly, each sensor device 102 implements, in memory, a state machine that includes a plurality of states and for which network access for the host device 110 is controlled in each state according to one or more network access zones associated with the state.

Fig. 7 is a state diagram for a host state machine 700 that is used to control network access of the host device. Each large oval represents a state in which a host

device 110 may be transitioned to, and each arrow represents a transition from one state to another state. Each transition condition is numbered on its respective arrow and described below.

5 The sensor 102 monitors each host device 110 for which it is responsible and transitions each host device to a state based on the monitoring and a current state of the host device. In some implementations, these states are recorded in a host table that stores data for each host device 110 being monitored by the sensor 102. By monitoring host  
10 -attributes of the host device that identify the host device, traffic to and from the host device, and the state of the host device, the sensor 102 can control network access of the host device according to the one or more network access zones associated with the state of the host device.

15 In the description that follows, each state and the actions that are taken during each state are described. Thereafter, the transitions from states are described, as are the transition conditions that cause the transitions.

### § 3.1 States

20 In some implementations, the states include an initial preadmission admission state 740, a host detection preadmission state 742, a user detection preadmission state 744, a post admission state 746, a secure guest preadmission state 748, a remediate preadmission state 750, a post boot admission state 752, and a quarantine post admission state 754. Additional states can be implemented, or, alternatively, fewer states can be implemented, depending on the network access control solution desired. For example, if network access control is based solely on the health level of a host device 110, then the secure guest  
25 preadmission state 748 and the user detection preadmission state 744 can be omitted, as these states are transitioned to when an identity-based network access control solution is employed.

30 The initial preadmission state 740 is a state during which the sensor 102 sends host information collection queries to the host device to receive host attributes from the host device in response. In some implementations, the host device is quarantined and a preadmission network access zone that prevents redirection of host device traffic is

applied. The sensor 102 sends information probes to the host device 110 in an attempt to identify the host device 102.

The host detection preadmission state 742 is a state during which the sensor 102 determines a host status based on the host attributes of the host. In this state, the sensor 102 sends a host detection event message to the network access control server 104, and, in some implementations, the preadmission network access zone still applies.

The user detection preadmission state 744 is a state during which a user identifier associated with the host device is mapped to a user role associated with a corresponding network access zone. In this state, the sensor 102 has determined a user identifier for the host device 110, and a user detection event is sent to the network access control server 104 to map the user identifier to a specific role defined for the user identifier. In some implementations, the preadmission network access zone still applies in this state.

The post admission state 746 is a state during which the host device is granted access to the network according to one of a plurality of network access zones. In this state, the host device 110 has been granted network access in accordance with the network access zone that is dependent on the health level of host device 110. In some implementations, the network access zone dependent on health level the host device 110 is applied only if the host device 110 was an unmanaged host, i.e., a host device 110 that did not have an agent 112 installed when it initially attempted to join the network.

In some implementations, if identity-based network access control is not enabled, and if the host device 110 is a managed host device, then full network access is provided.

During the post admission state 746, the sensor 102 monitors the host to determine if it remains online, and to detect possible IP address reassignments. Other events can also be monitored, such as a user logging out of the host device 110, and a new user logging into the host device 110.

The secure guest preadmission state 748 is a state during which HTTP traffic from the host device is directed to a guest access portal managed by the sensor 102 and which causes the host device to generate a user login and password prompt and. The sensor

receives a user identifier and password in response to user input. In this state, traffic from the host device 110 is redirected to a secure guest access portal 410. The user is prompted for a login name and password credentials. Upon receiving these login credentials, the sensor 102 passes the login credentials to the network access control server 104, and the network access control server 104 authenticates or rejects the login.

The remediate preadmission state 750 is a state during which HTTP traffic from the host device is directed to a remediate portal managed by the sensor 102 and which causes an agent to be downloaded to the host device. Only unmanaged host devices 110 are transition to this state. Traffic for the host device 110 is redirected to a remediation portal 310 and an agent is downloaded onto the host device 110. When the agent 112 is installed, the health level of the host device 110 is determined and communicated to the network access control server 104 and the sensor 102. In some implementations, the preadmission network access zone applies.

The post boot admission state 752 is a state in which all host devices are in after a sensor 102 reboot. The host attributes of all hosts stored in a persistent memory prior to a reboot of the sensor 102 are copied into a host table after the sensor 102 reboot, and the sensor 102 sends information probes to determine if one or more attributes of each host device 110 has changed. For example, prior to a reboot, the states of the host devices 110 and the host table have been persisted to a persistent memory, such as a flash memory. Upon reboot, information probes are sent to the host devices 110 to determine if IP addresses have been reassigned. Depending on the response to these information probes, a host device 110 may go into the post admission state 746, or may revert to the initial preadmission state 740.

The quarantine post admission state 754 is a state during which network access for the host is limited to a quarantine zone. In this state, access is restricted to a quarantine network access zone. Network access capabilities available to the host device 110 can, for example, be based on the severity of the attack that caused the transition to the state. The host device 110 remains in the state until a message is received from the network access control server 104 informing the sensor 102 of the change in the health level of the host

device. In some implementations, the host device 110 can remain in this state until a quarantine period timeout occurs.

### § 3.2 Transition Events

When a sensor 102 detects a new host device 110 attempting to join the network,  
5 the sensor populates its host table with a record for the host device 110 and initially places the host device in an unknown state. For example, the sensor 102 can receive a packet from a host device 110 for which there is no entry in the host table. Alternatively, for a host device 110 attempting to join a VPN, a RADIUS "accounting start" message can also create a host entry in the host table. The condition 702 of a host device 110 being listed in  
10 the host table with an unknown state causes the host device to transition to the initial preadmission state 740.

The state of the host device 110 can also transition to the initial preadmission state 740 from the post admission state 746 upon an IP address being reassigned to the host  
15 device 110, an information probes failing to receive a response after a maximum number of retries, or a RADIUS "accounting stop" message being received for the host device 110 (condition 730).

The state of the host device 110 can also transition to the preadmission state 740  
20 from the post boot admission state 752 in response to one or more of the host attributes in an information probe reply received by the sensor 102 not matching the attributes of the host device 110 as stored in the host table (condition 736).

The state of the host device 110 can transition to the user detection preadmission  
25 state 744 from the secure guest preadmission state 748 when the user identifier is determined. For example, if identity-based network access control is enabled, the user identifier can be determined implicitly, as described above, or explicitly by use of the guest access portal 410 (condition 708).

30 The state of the host device 110 can transition to the user detection preadmission state 744 from the host detection preadmission state 742 when an identity-based access

control process is enabled for the host device and a user identifier for the host device has been determined. For example, when the network access control server 104 returns the identity of the user of the host device 110, the state of the host device 110 can transition from the host detection preadmission state 742 to the user detection preadmission state 744 (condition 724).

The state of the host device 110 can transition to the user detection preadmission state 744 from the initial preadmission state 740 when an identity-based access control process is enabled for the host device and a user identifier for the host device has been determined. For example, the sensor 102 and/or the network access control server 104 can determine the user identifier for the host device 110 by parsing host device traffic capturing the user identifier information, e.g., by processing RADIUS AUTH packets, by agent queries sent to the host device 110, or by listening to agent beacons sent from the host device 110 (condition 706).

The state of the host device 110 can transition to the user detection preadmission state 744 from the post admission state 746 when a user logout of the host device is detected. For example, the user logout can be detected by the sensor 102, the network access control server 104, by a response to an agent query, or by listening to an agent beacon (condition 728).

The state of the host device 110 can transition to the secure guest preadmission state 748 from the initial preadmission state 740 when an identity based network access-control process for the host device is enabled and the host attributes received for the host device indicate that the host device is not a member of a predefined directory, or a user identifier for the host is not determined from the received host attributes. For example, a reply to an agent query with may indicate that the user identifier of the host device 110 is not a member of an active directory domain, or the host information collection phase fails to determine a user identifier for the host device 110 (condition 704).

The state of the host device can transition from the initial preadmission state 740 to the host detection preadmission state 742 when the identity-based access control process is

enabled for the host device and host attributes of the host are not received in response to host information collection queries (e.g., an agent query timeout), or a MAC address is received in a data link layer (L2) detection mode (condition 712).

5           The state of the host device can transition from the user detection preadmission state 744 to the host detection preadmission state 742 when the user identifier is mapped to a user role and further network accesses control for the user role is enabled (condition 710). For example, a particular user role for which the health level of the host device 110 must be determined can cause a transition from the user detection preadmission state 744  
10           to the host detection preadmission state 742.

          The state of the host device can transition from the host detection preadmission state 742 to the remediate preadmission state 750 when the host is determined to be an unmanaged host with an unknown health level (condition 714). For example, the sensor  
15           102, or the network access control server 104, can determine that the host is unmanaged and has an unknown health level based on the absence of an agent 112 being installed on the host device 110.

          To state the host device can transition from the user detection preadmission state 744 to the remediate preadmission state 750 when the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is enabled (condition 726). For example, the user may be  
20           authenticated through the user detection preadmission state 744, and the role of the user (e.g., a guest) requires that the health level of the host device 110 be determined.

25           The state of the host device can transition from the host detection preadmission state 742 to the post admission state 746 when the host is determined to be a managed host or the host is determined to be an unmanaged host with a pre-determined health level that is acceptable for transition to the post admission state (condition 718).

30           The state of the host device can transition from the remediate preadmission state 750 to the post admission state 746 when the host device 110 is determined, from the

health data provided by the agent, to have a health level that is acceptable for transition to the post admission state (condition 716).

5 The state of the host device can transition from the user detection preadmission state 744 to the post admission state 746 when the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is disabled (condition 722).

10 The state of the host device can transition from the post boot admission state 752 to the post admission state 746 when the host attributes of the host device received after the reboot match the host attributes of the host device stored in the persistent memory and copied into the host table (condition 734). For example, the sensor 102 or the network access control server 104 can determine that host attributes, such as the agent identifier, user identifier, IP address and MAC address, received in information probe replies match  
15 the attributes in a record in a host table for the host device 110. Thus, if the state of the host has not changed since prior to the reboot, the host device state is transitioned to the post admission state 746.

20 The state of the host device can transition from the post admission state 746 to the quarantine post admission state 754 when an attack is detected for the host device 110 (condition 732). For example, the sensor 102 can detect an attack from monitoring the network traffic of the host device 110, or the agent 112 can notify the sensor 102 of attack. Attacks can be detected by monitoring the behavior of the host device, and/or by comparing the traffic to and from the host device 110 to malware and/or virus signature  
25 data.

30 The state of the host device can transition from the quarantine post admission state 754 to the post admission state 746 until the sensor 102 receives a message from the network access control server 104 informing the sensor 102 of a change in the health level the host device 100, or, optionally, until a quarantine period timeout occurs (condition 733).

#### § 4.0 Failover Configuration

In some implementations, the sensors 102 can be deployed in a failover configuration. Fig. 8 is a block diagram of two sensors 102-A and 102-B configured in an example failover configuration 800. In this configuration, one sensor is designated a primary sensor (102-A), and the other sensor is designated a secondary sensor (102-B). As will be explained below, either the primary sensor 102-A or the secondary sensor 102-B is responsible for probing a host device 110.

As depicted in Fig. 8, the primary sensor 102-A is responsible for probing the host device 110-A, and the secondary sensor is initially responsible for probing the host device 110-B. Together the sensors 102-A and 102-B form a pair of peer sensors configured to control host device 110 access to a network.

Each sensor 102 stores a host table 810 that includes, for each of the host devices 110 monitored on the network by the peer sensors, a record including fields for host attributes ("HA"), a primary sensor probe type ("PSPT") and a secondary sensor probe type ("SSPT"). As will be explained in more detail in section 4.2 below, the primary and secondary probe types are the probe types of the highest priority information probe for which a reply from the host device was received at the primary sensor and the secondary sensor, respectively.

Example host attributes include an IP address of the host device 110, a MAC address of the host device 110, an agent identifier of an agent 112 installed on the host device 110, a user identifier of a user logged into the host device 110, and one or more timestamp fields for storing a timestamp indicating the time that the host attributes were stored the record.

#### § 4.1 Host Table Synchronization

When in a failover configuration, the host tables 810 in the sensors 102 are synchronized so that they are identical (except for the time stamps). In normal operations, the sensors are connected through a interconnect link 812 to maintain synchronization of the host tables 810. However, when a peer sensor 102 in a failover configuration goes

offline, or if the interconnect link 812 goes down, the host tables stored in both sensors need to be synchronized upon recovery of the interconnect link 812, or upon the peer sensor 102 coming back online.

5 In some implementations, each record includes a separate timestamp for each of a user identifier attribute, a MAC address attribute, an agent identifier attribute, and a host name attribute. Each timestamp measure the time that the record was last updated for its respective attribute. In other-implementations, each record includes only one timestamp that measure when the record was last updated for any attribute.

10 In some implementations, the timestamps are based on unsynchronized system clocks. Unsynchronized system clocks are clocks that are not synchronized to a reference time, such as GMT, or synchronized to each of the other sensor clocks. As the time stamps for records cannot be compared in absolute values, they are compared relative to the time they were entered in the host tables 110 to determine which record in the tables is most recent. For example, if one record in host table 810-A for host device 110-A was updated 10 minutes ago, relative to the system clock of the sensor 102-A, and a corresponding record in host table 110-B for the host device 110-A was updated one minute ago, relative to the system clock of the sensor 102-B, the latter is determined to be the most recent record.

15 In some implementations, when the record is transmitted to a peer sensor, the timestamp field of the data being transmitted is updated based on the following calculation:

20 system clock time - last update time

For example, assume the MAC address field in a first peer sensor memory was updated at a system clock time of 1000, and that the record is provided to a second peer sensor at a system clock time of 1100 in the first peer sensor. For the record data transmitted to the second peer sensor, the timestamp of the MAC address is 100 (1100 — 1000).

Alternatively, the receiving sensor 102 can communicate with its peer sensor over the link 812 to obtain the peer sensor's clock value to determine how long ago the peer record was updated. Likewise, the receiving sensor can compare its own clock value to the timestamp of the record in its own host table to determine how long ago the record in its own host table was updated.

In other implementations, the timestamps can be synchronized, i.e., the clocks for all sensors can be synchronized to each other to a known reference time, e.g., Greenwich mean time (GMT). In these implementations, the timestamp that is most recent is the most current.

In some implementations, the IP address of the host entries are used as a key to synchronize the host tables 810. To synchronize, the timestamps are used to determine when the Agent identifier, MAC address, user information, and other host attributes were updated, as well as the probe type that was used to collect the information that resulted in the most recent update.

For example, during synchronization, a sensor, e.g., 102-A, receives a peer record for a host entry from its peer sensor, e.g., 102-B. Assume the peer record from host table 810-B corresponds to the host device 110-B, and that the sensor 102-A is coming back online. If the peer record identifies a completely new entry (i.e., there is no entry in the host table 810-A for the IP address listed in the peer record), then subsequent searches are done in the host table 810-A based on the agent identifier and then on the MAC address, if necessary.

If there is an entry in the host table 810-A with the agent identifier that is provided in the peer record, and if the peer record is more recent than the record in the host table 810-A (e.g., for a record with only one time stamp, the time stamp of the peer record indicates that the record was updated more recently in the host table 110-B than the record in the host table 110-A, or, for a record with a separate timestamp for each of the agent identifier, MAC address, user identifier and host name attributes, the time stamp of the peer record indicates the agent identifier is more recent than the agent identifier of the

record stored in the host table 810-A), then an IP address reassignment occurred for the host device 110-B. The corresponding record in the host table 810-A is updated, and the network access control server 104 is notified.

5           If any of the above conditions are not met, however, then the host table 810-A is searched based on the MAC address of the peer record. If there is an entry in the host table 810-A with the MAC that is provided in the peer record, and if the peer record is more recent than the record in the host table 810-A (e.g., for a record with only one time stamp, the time stamp of the peer record indicates that the record was updated more  
10           recently in the host table 110-B than the record in the host table 110-A, or, if multiple time stamps are used, the time stamp of the peer record indicates the MAC address is more recent than the MAC address of the record stored in the host table 810-A), then an IP address reassignment occurred for the host device 110-B. The corresponding record in the host table 810-A is updated, and the network access control server 104 is notified.

15           Otherwise, the host device 110-B is a new host device, and a new host detected event with all appropriate information available from the peer record is sent to the network access control server 104.

20           If the peer host record includes an IP address that is already in the host table 810-A, then the agent identifiers, the MAC addresses, user and host information, and the probe types are compared, if necessary.

25           For example, if the agent identifier of the host record in the host table 810-A does not match the agent identifier in the peer record, and if the peer record is more recent than the host record in the host table 810-A, then the host device 110-B is a new host using the same IP address that is stored in the host table 810-A. The host record in table 810-A is deleted and a new host device detection event is generated by the sensor 102-A.

30           If, however, the agent identifiers match, then the MAC addresses are compared. If the MAC addresses differ, and if the peer record is more recent than the host record in the host table 810-A, then the host device 110-B is a new host using the same IP address that

is stored in the host table 810-A. The host record in table 810-A is deleted and a new host device detection event is generated by the sensor 102-A.

If the MAC addresses also match, then the user information and host information of the host device 110-B is compared (if identity based network access control is implemented). If the user information and the host information are different, and if the peer record is more recent than the host record in the host table 810-A, then a new user has logged onto the host device 110-B. The contents of the peer record are copied into the host record in table 810-A, and a new user detection event is generated.

Finally, if the MAC addresses match and identity-based network access control is not implemented, the probe types are compared. If the probe types are different, and if the peer record is more recent than the host record in the host table 810-A, the contents of the peer record are copied into the host record in table 810-A and the probe type of the secondary sensor is used for subsequent probes.

Figs. 9A and 9B are flow diagrams of an example process 900 for synchronizing host tables in a pair of peer sensors. The process 900 can be implemented in any peer sensor of a pair of sensors 102 configured in a failover configuration. The process steps depicted in Fig. 9A occur when the IP address of the peer record is not stored in the host table of the sensor receiving the peer record, and the process steps depicted in Fig. 9B occur when the IP address of the peer record is stored in a host table record of the host table of the sensor receiving the peer record.

The process 900 receives peer record data from a peer sensor (902). For example, the primary sensor 102-A can receive a record from the secondary sensor 102-B.

The process 900 determines if an IP address of the peer record is stored in a host table record of the host table of the sensor executing the process (904). For example, the primary sensor 102-A searches the host table 810-A based on the IP address in the peer record.

If an IP address of the peer record is not stored in the host table of the sensor executing the process, then the process 900 determines if an agent identifier of the peer record is stored in a host table record of the host table executing the process (906). For example, the sensor 102 can determine if there is an agent identifier stored in the peer record, and if so, can use the agent identifier to search the host table 810-A.

If agent identifier of the peer record is stored in a host table of the sensor executing the process, then the process 900 determines if the peer record is more recent than the host table record (908). For example, the primary sensor 102-A can communicate with the secondary sensor 102-B to obtain the secondary sensor 102-B clock value to determine how long ago the peer record was updated. Likewise, the primary sensor 102-A can compare its own clock value to the timestamp of the record in the host table 810-A to determine how long ago the record in the host table 810-A was updated. Based on these determinations, the primary sensor 102-A determines which of the two records is the most recent.

If the peer record is more recent than the host table record, then the process 900 executes an IP reassignment process (910), as described above. If, however, the peer record is not more recent than the host table record, or if the agent identifier of the peer record is not stored in the host table, then the process 900 determines if the MAC address of the peer record is stored in a host table record of the sensor executing the process (912). For example, the sensor 102 can determine if there is a MAC address stored in the peer record, and if so, can use the MAC address to search the host table 810-A.

If the MAC address of the peer record is stored in the host table the sensor executing the process, the process 900 determines if the peer record is more recent than the host table record (914), as described above.

If the peer record is more recent than the host table record, then the process 900 executes an IP reassignment process (910), as described above. If, however, the peer record is not more recent than the host table record, or the MAC address of the peer record is not stored in the host table, then the process 900 sends a new host device detected message (916). The new host device detected message is sent to the network access control server 104, which, in turn, provides instructions to the sensor 102. Although the

network access control server 104 may be aware of the new host device from the monitoring provided by the other peer sensor, the peer sensor that is being updated with the peer record may, in some implementations, need additional direction from the network access control server 104 to determine the correct state of the host device 110 (e.g.,  
5 receive identification-related information from the network access control server 104, etc.).

Returning to step 904, if the process 900 determines that the IP address of the peer record is stored in the host table, then the process 900 determines if the agent identifier the  
10 peer record matches the agent identifier of the host table record in the host table of the peer sensor executing the process (918).

If the agent identifiers do not match, then the process 900 determines if the peer record is more recent than the host table record (920), as described above.

15 If the peer record is more recent than the host table record, then the process 900 sends a delete event for the current host device in the host table record and sends a host detected event for a new host device (922), as the host device 110-B is a new host device using an IP address that was previously assigned to another host device 110, and for which  
20 a reassignment occurred when the primary sensor 102-A was off-line or when the interconnection link 812 was down.

If the peer record is not more recent than the host table record, or if the agent identifiers do match, then the process 900 determines if the MAC address of the peer  
25 record matches the MAC address of the host record (924). If the MAC addresses do not match, then the process 900 determines if the peer record is more recent than the host table record (926), as described above.

30 If the peer record is more recent than the host table record, then the process 900 sends a delete event for the current host device in the host table record and sends a host detected event for a new host device (922), as this again is the case in which the host

device 110-B is a new host device using an IP address that was previously assigned to another host device 110.

5 If the peer record is not more recent than the host table record, or if the MAC addresses do match, and if identity-based network access control is enabled, then the process 900 determines if the user identifier and host information in the peer record match the user identifier host information in the host table record (928).

10 If the user identifiers and host information do not match, then the process determines if the peer record is more recent than the host table record (930), as described above.

15 If the peer record is more recent than the host table record, then the process 900 copies the peer record contents to the host table record in the host table, and sends a new user detected event for new user (932), as this is the case in which a new user has logged onto the host device 110-B. In some implementations, only the user identifier and host name information are copied.

20 If, however, identity-based network access control is not enabled, or if the user identifier and host information do match, or if the peer record is not more recent than the host table record, then the process 900 determines if the probe type of the probe used to collect the information in the peer record matches the probe type of the probe used to collect information in the host table record (934).

25 If the probe types do not match, then the process 900 determines if the peer record is more recent than the host table record (936), as described above.

30 If the peer record is more recent than the host table record, then the process 900 copies the peer record contents to the host table record and uses the probe type of the peer record for subsequent probes (938). If, however the peer record is not more recent than the host table record, or if probe types do match, then the process 900 ends (940).

#### § 4.2 Information Probe Allocation

As described above, both of the peer sensors are able to probe the host device with information probes. However, only one of the peer sensors is needed to probe any particular host device at any particular time.

5

In some cases, when the primary sensor 102-A sends information probes, there may not be any reply from the host device 110; however, if the secondary sensor 102-B sends an information probe, the secondary sensor 102-B can receive a reply to the information probes. This may occur due to network topology differences and changes between the primary sensor, the secondary sensor, and the host device that is monitored by the primary sensor and the secondary sensor, e.g., by the establishment of a firewall, the temporary failure of a switch, etc.

10

15

In some implementations, information probing is allocated among peer sensors so that only one peer sensor is responsible for probing a host device. The probing sensor copies the replies received in response to the queries to the non-probing sensor. The initial allocation of the probing sensor among the primary sensor 102-A and the secondary sensor 102-B depends on the replies received to initial information probes at both of sensors. Additionally, whether a host device is determined to be offline in response to a failure to receive a reply to an information probe, and whether to hand over probing responsibilities, depends on the initial probing allocation and the probe types determined by both the primary sensor 102-A and the secondary sensor 102-B.

20

25

For example, initial allocation of probing responsibilities between the primary sensor 102-A in the secondary sensor 102-B depends on the information probes that replied to both the primary sensor 102-A in the secondary sensor 102-B. Additionally, whether a host device, such as host device 110-A, is categorized as being off-line in response to failure to receive a reply to an information probe, or whether probing responsibilities are handed over to a peer sensor, can also depend on the information probes that replied to both the primary sensor 102-A in the secondary sensor 102-B.

30

Fig. 10 is a flow diagram of an example process 1000 for allocating probing responsibilities among a pair of peer sensors. The portions of the process 1000 under the heading "Primary Sensor" are performed in the primary sensor, and the portions of the process under the heading "Secondary Sensor" are performed in the secondary sensor.

5

In the primary sensor, the process 1000 transmits information probes to a host device (1002). Likewise, in the secondary sensor the process 1000 transmits information probes to the host device (1050). The primary and secondary sensors transmit information probes in response to detecting a new host device attempting to join the network.

10

In some implementations, all information probes available to the sensors 102 are used, e.g., an agent query, NBTSTAT, and an ICMP Ping. Additionally, the information probes are prioritized according to their probe types in a descending priority order. In one example participation, the agent query is prioritized higher than the NBTSTAT query, and the NBTSTAT query is prioritized higher than the ICMP Ping.

15

In the primary sensor, the process 1000 determines a first probe type (1004). The first probe type is the probe type of the highest priority information probes for which a reply from the host device was received at the primary sensor. Likewise, in the secondary sensor, the process 1000 determines a second probe type (1052). The second probe type is the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor.

20

In the secondary sensor, the process 1000 transmits the second probe type to the primary sensor (1054), and in the primary sensor, the process 1000 determines if the second probe type is greater than the first probe type (1006).

25

If a second prototype is greater than the first probe type, then the process 1000 transmits a probe handover to the secondary sensor (1008). For example, in Fig. 8, the dashed arrow 820 represents the probe handover, which allocates probing responsibility to the secondary sensor 102-B.

30

In response to receiving the probe hand over at the secondary sensor, the process 1000 monitors the host device (1056). For example, the secondary sensor 102-B issues information probes and listens for agent beacons.

5           At the secondary sensor, the process 1000 determines if the host device is off-line (1058). For example, the secondary sensor 102-B listens for replies to the information probes and/or the agent beacons. As long as replies are received, the secondary sensor 102-B continues to monitor the host device (1056).

10           If, however, the process 1000 determines of the host devices off-line, then the process 1000 deletes the record for the host device in the host table of the secondary sensor, and transmits the deletion data to the primary sensor (1060). At the primary sensor, in response to receiving the deletion data from the secondary sensor, the process 1000 deletes the record for the host device in the host table (1018).

15           Thus, in response to the secondary sensor 102-B having a probe type higher priority than the primary sensor 102-A, the secondary sensor will not request the primary sensor 102-A to try and probe the host device 110 again, as it is very likely that the host device 110 will also not respond to information probes from the primary sensor 102-A.

20           Returning to step 1006, if the process 1000 determines that the second probe type is not greater than the first probe type, then the process 1000 monitors the host device using the primary sensor (1010). At the primary sensor, the process 1000 determines if the host device is off-line (1012). For example, the primary sensor 102-A listens for replies to the information probes and/or the agent beacons. As long as replies are received, the  
25           primary sensor 102-A continues to monitor the host device (1010).

          If, however, the process 1000 determines the host device is off-line, then the process 1000 determines if the second probe type is equal to the first probe type (1014). If the second probe type is equal to the first probe type, then the process 1000 transmits a  
30           probe hand over to the secondary sensor (1008). Thereafter, the secondary sensor monitors the host as described above.

If, however, the second probe type is not equal to the first probe, then the process 1000 deletes the record for the host device the host table, and transmits deletion data to the secondary sensor. At the secondary sensor, in response to receiving deletion data from the primary sensor, the process 1000 deletes the record for the host device in the host table the  
5 secondary sensor (1062).

In some implementations, the process 1000 also transmits the first probe type to the secondary sensor. Although in the process 1000 above the secondary sensor does not make a determination based on the probe types in response to failing to receive replies from a host device, there is the possibility that the roles of the secondary sensor and the  
10 primary sensor can be reversed, i.e., the secondary sensor can be designated the primary sensor, and the primary sensor can be designated the secondary sensor. In the event of such re-designation, the decision process of the primary sensor takes into account the probe types of the primary and secondary sensor. In variations of this implementation, the probe types are re-determined when the re-designation occurs, i.e., upon re-designation,  
15 process steps 1002, 1004, 1050, 1052 and 1054 are repeated for the newly-designated primary and secondary sensors.

#### § 5.0 Nonce Authentication

Fig. 11 is a timing diagram 100 of a nonce-based authentication process. As a sensor 102 often queries a host device 110, or often redirects host devices 110 to a guest  
20 access portal, there is the potential for replay attacks. To guard against replay attacks, the sensor 102 can implement a nonce-based authentication.

For example, when a sensor 102 provides an access portal to facilitate a user login from a host device, the sensor will send a nonce to the host device when requesting  
25 authentication information, e.g., when requesting a user identifier and password within the HTTP 401 authentication realm. The host device, in turn, sends a reply that includes a login credential, such as a user identifier, an authentication code that is a hash of the user's password and the nonce

30 Likewise, when a sensor 102 queries an agent, the sensor 102 can include a nonce with the agent query. The agent 112, when replying to the agent query, also provides an

authentication code with the reply. The authentication code can, for example, be a hash of the reply and the nonce, such as a hash generated by use of the MD5 hash algorithm (or any other suitable hash algorithm, such as a hash algorithm of the SHA series, RIPEMD series, etc.). The sensor 102 then checks the authentication code by hashing the reply and the nonce. Provided the hashes match, the reply is deemed authentic.

As the sensor provides a new nonce with each presentation of the access portal or for each agent query, replay attacks are thwarted.

In some implementations, the sensor 102 maintains nonce counter that is initialized from the sensor 102 system clock. Each time a nonce is generated, the counter value is passed to a hash function and incremented. In some implementations, only the hash of a single count value is used as a nonce. In other limitations, two different counter values are hashed and combined to form the nonce. As the hash function returns a completely different hash value for each unique counter value, the hash function effectively randomizes the nonce so that predicting the next nonce is impractical for a replay attack.

#### § 5.1 Nonce Generation

Fig. 12 is a flow diagram of an example process 1200 for generating a nonce. The process 1200 generates a nonce from a single source value, and can be implemented in the sensor 102.

The process 1200 generates a source value (1202). For example, the sensor 102 can select a value of a nonce counter and increment the counter. In other implementations, the sensor can select the current system clock value.

The process 1200 hashes the source value to generate a nonce (1204). For example, the sensor 102 can hash the source value using a hash algorithm.

The process 1200 provides a nonce with query (1206). For example, the sensor 102 provides the nonce with an agent query, or can provide the nonce as part of the HTTP 401 authentication realm.

The process 1200 receives a reply to the query and an authentication code (1208). For example, the sensor 102 receives a reply an authentication code that is a hash of the reply and the nonce.

5           The process 1200 hashes the reply and the nonce to generate a digest (1210). For example, the sensor 102 hashes the reply and the nonce using the same hash algorithm that was used to create the authentication code.

10           The process 1200 determines if the digest matches the authentication code (1212). If the digest matches the authentication code, then the process 1200 determines the reply is authentic (1214). Conversely, if the digest does not match the authentication code, then the process determines the reply is not authentic (1216). For example, the sensor 102 can determine that reply to the agent query, or user credentials provided through the guest access portal 401, are authentic and continue processing communications from the host device 110 (1214). Alternatively, the sensor 102 can block further communications from the host device 110 if the reply or credentials are determined not to be authentic (1216).

Fig. 13 is a flow diagram of another example process 1300 for generating a nonce. The process 1300 generates a nonce from two or more source values, and can be  
20           implemented in the sensor 102. Generating a nonce from two or more source values makes it more difficult to predict what the next nonce will be in a replay attack, and thus provides an additional level of security.

25           The process 1300 generates source values (1302). For example, the sensor 102 can select two successive values of a nonce counter, or can select the system clock value and increment the system clock value to generate a second source value.

          The process 1300 hashes the source values to generate hash values (1304). For example, the sensor 102 can hash each of the values to generate respective hash values.

30           The process 1300 generates a nonce from the hash values (1306). In some implementations, the sensor 102 can concatenate the hash values. For example, the nonce

counter can be a 4-byte nonce counter, and the hashing function returns a 4-byte hash. The 4-byte hashes are concatenated to form an 8-byte nonce.

5           The process 1300 provides a nonce with query (1308). For example, the sensor 102 provides the nonce with an agent query, or can provide the nonce as part of the HTTP 401 authentication realm.

10           The process 1300 receives a reply to the query and an authentication code (1310). For example, the sensor 102 receives a reply with an authentication code that is a hash of the reply and the nonce.

15           The process 1200 hashes the reply and the nonce to generate a digest (1312). For example, the sensor 102 hashes the reply and the nonce using the same hash algorithm that was used to create the authentication code.

20           The process 1300 determines if the digest matches the authentication code (1314). If the digest matches the authentication code, then the process 1200 determines the reply is authentic (1316). Conversely, if the digest does not match the authentication code, then the process determines the reply is not authentic (1318). For example, the sensor 102 can determine that reply to the agent query, or user credentials provided through the guest access portal 401, are authentic and continue processing communications from the host device 110 (1316). Alternatively, the sensor 102 can block further communications from the host device 110 if the reply or credentials are determined not to be authentic (1318).

25           Embodiments of the subject matter and the operations described in this specification can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. Embodiments of the subject matter described in this specification can be implemented as one or more computer programs, i.e., one or more modules of computer program instructions, encoded on  
30           computer storage medium for execution by, or to control the operation of, data processing apparatus. Alternatively or in addition, the program instructions can be encoded on an

artificially-generated propagated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal, that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. A computer storage medium can be, or be included in, a computer-readable storage device, a computer-readable storage substrate, a random or serial access memory array or device, or a combination of one or more of them. Moreover, while a computer storage medium is not a propagated signal, a computer storage medium can be a source or destination of computer program instructions encoded in an artificially-generated propagated signal. The computer storage medium can also be, or be included in, one or more separate physical components or media (e.g., multiple CDs, disks, or other storage devices).

The operations described in this specification can be implemented as operations performed by a data processing apparatus on data stored on one or more computer-readable storage devices or received from other sources.

The term "data processing apparatus" encompasses all kinds of apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing. The apparatus can include special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit). The apparatus can also include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, a cross-platform runtime environment, a virtual machine, or a combination of one or more of them. The apparatus and execution environment can realize various different computing model infrastructures, such as web services, distributed computing and grid computing infrastructures.

A computer program (also known as a program, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A computer program

may, but need not, correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub-programs, or portions of code). A computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

The processes and logic flows described in this specification can be performed by one or more programmable processors executing one or more computer programs to perform actions by operating on input data and generating output. The processes and logic flows can also be performed by, and apparatus can also be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit).

Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. The essential elements of a computer are a processor for performing actions in accordance with instructions and one or more memory devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from or transfer data to, or both, one or more mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks. However, a computer need not have such devices. Moreover, a computer can be embedded in another device, e.g., a mobile telephone, a personal digital assistant (PDA), a mobile audio or video player, a game console, a Global Positioning System (GPS) receiver, or a portable storage device (e.g., a universal serial bus (USB) flash drive), to name just a few. Devices suitable for storing computer program instructions and data include all forms of non-volatile memory, media and memory devices, including by way of example semiconductor memory devices, e.g., EPROM, EEPROM, and flash memory devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The

processor and the memory can be supplemented by, or incorporated in, special purpose logic circuitry.

To provide for interaction with a user, embodiments of the subject matter described in this specification can be implemented on a computer having a display device, e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor, for displaying information to the user and a keyboard and a pointing device, e.g., a mouse or a trackball, by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback, e.g., visual feedback, auditory feedback, or tactile feedback; and input from the user can be received in any form, including acoustic, speech, or tactile input. In addition, a computer can interact with a user by sending documents to and receiving documents from a device that is used by the user; for example, by sending web pages to a web browser on a user's client device in response to requests received from the web browser.

While this specification contains many specific implementation details, these should not be construed as limitations on the scope of any inventions or of what may be claimed, but rather as descriptions of features specific to particular embodiments of particular inventions. Certain features that are described in this specification in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment can also be implemented in multiple embodiments separately or in any suitable subcombination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a subcombination or variation of a subcombination.

Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing

may be advantageous. Moreover, the separation of various system components in the embodiments described above should not be understood as requiring such separation in all embodiments, and it should be understood that the described program components and systems can generally be integrated together in a single software product or packaged into multiple software products.

Thus, particular embodiments of the subject matter have been described. Other embodiments are within the scope of the following claims. In some cases, the actions recited in the claims can be performed in a different order and still achieve desirable results. In addition, the processes depicted in the accompanying figures do not necessarily require the particular order shown, or sequential order, to achieve desirable results. In certain implementations, multitasking and parallel processing may be advantageous.

What is claimed is:

1. A method performed by data processing apparatus, the method for collecting host attributes of a host and comprising:

receiving data at the data processing apparatus indicating a host device is connecting to a network;

in response to the host device connecting to the network, initiating a host detection phase for the host device during which host attributes of the host are collected by the data processing apparatus and network access for the host device is restricted, and during the host collection phase for the host device:

transmitting a plurality of information probes to the host device, the information probes including an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes requesting one or more other host attributes;

monitoring for replies to the information probes from the host device during the host detection phase;

ending the host detection phase in response to receiving a reply to the agent probe that includes the unique agent identifier;

resending the plurality of information probes and incrementing a repeat counter in response to not receiving a reply to the agent probe after the expiration of a time period; and

ending the host detection phase in response to a value of the repeat counter exceeding a maximum repeat value.

2. The method of claim 1, further comprising, during the collection phase:

not repeating an information probe after the expiration of the time period in response to receiving a reply to the information probe, the information probe being an information probe other than the agent probe.

3. The method of claim 1, further comprising, during the collection phase:  
monitoring for an agent beacon sent from the host device during the host detection phase, the agent beacon being a data that is sent independent of the information probes;  
and  
ending the host detection phase in response to receiving the unique agent identifier from the agent beacon.
4. The method of claim 3, further comprising, during the collection phase:  
not repeating an information probe after the expiration of the time period in response to receiving a reply to the information probe, the information probe being an information probe other than the agent probe.
5. The method of claim 3, wherein the plurality of information probes further include an NBTSTAT query.
6. The method of claim 3, wherein the plurality of information probes further include and ICMP ping.
7. The method of claim 3, wherein the agent query queries the agent identifier of the agent, the MAC address of the host device, and user login information associated with the host device.
8. The method of claim 3, wherein the agent beacon provides the agent identifier of the agent, the MAC address of the host device, and user login information associated with the host device.

9. A computer storage medium encoded with a computer program, the program comprising instructions that when executed by data processing apparatus cause the data processing apparatus to perform operations comprising:

receiving data indicating a host device is connecting to a network;

in response to the host device connecting to the network, initiating a host detection phase for the host device during which host attributes of the host are collected by the data processing apparatus and network access for the host device is restricted, and during the host collection phase for the host device:

transmitting a plurality of information probes to the host device, the information probes including an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes requesting one or more other host attributes;

monitoring for replies to the information probes from the host device during the host detection phase;

ending the host detection phase in response to receiving a reply to the agent probe and that includes the unique agent identifier;

resending the plurality of information probes and incrementing a repeat counter in response to not receiving a reply to the agent probe after the expiration of a time period; and

ending the host detection phase in response to a value of the repeat counter exceeding a maximum repeat value.

10. The computer storage medium of claim 9, comprising further instructions that cause the data process apparatus to perform further operations comprising:

not repeating an information probe after the expiration of the time period in response to receiving a reply to the information probe, the information probe being an information probe other than the agent probe.

11. The computer storage medium of claim 9, comprising further instructions that cause the data process apparatus to perform further operations comprising:

monitoring for an agent beacon sent from the host device during the host detection phase, the agent beacon being a data that is sent independent of the information probes;  
and

ending the host detection phase in response to receiving the unique agent identifier from the agent beacon.

12. The computer storage medium of claim 11, comprising further instructions that cause the data process apparatus to perform further operations comprising:

not repeating an information probe after the expiration of the time period in response to receiving a reply to the information probe, the information probe being an information probe other than the agent probe.

13. The method of claim 3, wherein the plurality of information probes further include an NBTSTAT query.

14. The method of claim 3, wherein the plurality of information probes further include and ICMP ping.

15. The method of claim 3, wherein the agent query queries the agent identifier of the agent, the MAC address of the host device, and user login information associated with the host device.

16. The method of claim 3, wherein the agent beacon provides the agent identifier of the agent, the MAC address of the host device, and user login information associated with the host device.

17. A data processing apparatus, comprising:

a memory subsystem, an input/output subsystem that transmits and receives data over a network, and a processor in data communication with the memory subsystem and the input/output subsystem, the processor programmed to perform operations comprising:

receiving data indicating a host device is connecting to a network;

in response to the host device connecting to the network, initiating a host detection phase for the host device during which host attributes of the host are collected by the data processing apparatus and network access for the host device is restricted, and during the host collection phase for the host device:

transmitting a plurality of information probes to the host device, the information probes including an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes requesting one or more other host attributes;

monitoring for replies to the information probes from the host device during the host detection phase;

ending the host detection phase in response to receiving a reply to the agent probe and that includes the unique agent identifier;

resending the plurality of information probes and incrementing a repeat counter in response to not receiving a reply to the agent probe after the expiration of a time period; and

ending the host detection phase in response to a value of the repeat counter exceeding a maximum repeat value.

18. The data processing apparatus of claim 17, wherein the processor is further programmed to perform operations comprising:

not repeating an information probe after the expiration of the time period in response to receiving a reply to the information probe, the information probe being an information probe other than the agent probe.

19. The data processing apparatus of claim 18, wherein the processor is further programmed to perform operations comprising:

monitoring for an agent beacon sent from the host device during the host detection phase, the agent beacon being a data that is sent independent of the information probes; and

ending the host detection phase in response to receiving the unique agent identifier from the agent beacon.

20. A method for an authentication protocol, the method performed by data processing apparatus and comprising:

generating, by the data processing apparatus, a source value;

hashing, by the data processing apparatus, the source value to generate a nonce;

providing, by the data processing apparatus, the nonce with a query over a network;

receiving, in response to the query, reply data and an authentication code;

hashing a combination of the reply data and the nonce to generate a digest; and

determining the reply is authentic if the digest matches the authentication code.

21. The method of claim 20, wherein generating a source value comprises:

selecting a counter value of a counter as the source value; and

incrementing the counter in response to the selection;

wherein counter values of the counter are used for source values for generating nonces.

22. The method of claim 20, wherein generating a source value comprises:

selecting a clock value of a system clock of the data processing apparatus as the source value.

23. The method of claim 20, wherein hashing the source value to generate the nonce comprises hashing the source value to generate an 8-byte hash value, the 8-byte hash value being the nonce value.

24. A method for an authentication protocol, the method performed by data processing apparatus and comprising:

- generating, by the data processing apparatus, a plurality of source values;
- hashing, by the data processing apparatus, the source values to generate hash values;
- generating, by the data processing apparatus, a nonce from the hash values;
- providing, by the data processing apparatus, the nonce with a query over a network;
- receiving, in response to the query, reply data and an authentication code;
- hashing, by the data processing apparatus, a combination of the reply data and the nonce to generate a digest; and
- determining, by the data processing apparatus, the reply is authentic if the digest matches the authentication code.

25. The method of claim 24, wherein generating a plurality of source values comprises:

- selecting a counter value of a counter as a first source value;
- incrementing the counter in response to the selection; and
- selecting the incremented counter value of the counter as a second source value.

26. The method of claim 25, wherein generating the nonce from the hash values comprises concatenating hash values to form the nonce value.

27. The method of claim 24, wherein generating a plurality of source values comprises:

- selecting a first clock value of a system clock of the data processing apparatus as the first source value;
- incrementing the first clock value to generate the second source value.

28. The method of claim 24, wherein:

hashing the source values to generate the nonce comprises hashing each source value to generate a 4-byte hash value; and

generating the nonce from the hash values comprises concatenating the 4-byte hash values to generate the nonce.

29. A computer storage medium encoded with a computer program, the program comprising instructions that when executed by data processing apparatus cause the data processing apparatus to perform operations comprising:

generating a plurality of source values;

hashing the source values to generate hash values;

generating a nonce from the hash values;

providing the nonce with a query over a network;

receiving reply data and an authentication code;

hashing a combination of the reply data and the nonce to generate a digest; and

determining the reply is authentic if the digest matches the authentication code.

30. The computer storage medium of claim 29, wherein generating a plurality of source values comprises:

selecting a counter value of a counter as a first source value;

incrementing the counter in response to the selection; and

selecting the incremented counter value of the counter as a second source value.

31. The computer storage medium of claim 29, wherein generating the nonce from the hash values comprises concatenating hash values to form the nonce value.

32. The computer storage medium of claim 29, wherein generating a plurality of source values comprises:

selecting a first clock value of a system clock of the data processing apparatus as the first source value;

incrementing the first clock value to generate the second source value.

33. The computer storage medium of claim 29, wherein:

hashing the source values to generate the nonce comprises hashing each source value to generate a 4-byte hash value; and

generating the nonce from the hash values comprises concatenating the 4-byte hash values to generate the nonce.

34. A method performed by data processing apparatus, the method comprising:

storing in the memory of the data processing apparatus a host table, the host table including, for each of a plurality of host devices monitored on a network, a record including:

an IP address field for storing an IP address assigned to the host device;

an agent identifier field for storing an agent identifier of agent installed on the host device; and

a time stamp field for storing a time stamp indicating the time that host attributes were stored in the record;

receiving from a peer data processing apparatus, in response to a synchronization event, a peer record for a host device, the peer record comprising data for a record stored in a host table in the memory of the peer data processing apparatus;

determining whether an IP address of the peer record is stored in a record in the host table;

in response to determining that the IP address of the peer record is not stored in a record of the host table:

determining whether the peer record includes an agent identifier;

in response to determining that the peer record includes the agent identifier, determining whether the agent identifier of the peer record is stored in a record of the host table;

in response to determining that the agent identifier of the peer record is stored in a record of the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with data of the peer

record.

35. The method of claim 34, further comprising, in response to determining that the agent identifier of the peer record is not stored in a record of the host table:

determining whether the peer record includes a MAC address;

in response to determining that the peer record includes a MAC address,  
determining whether the MAC of the peer record is stored in a record of the host table;

in response to determining that the MAC address of the peer record is  
stored in a record of the host table, determining whether the peer record is more recent  
than the record of the host table based on the time stamp of the peer record and the time  
stamp of the records in the host table; and

in response to determining that the peer record is more recent than  
the record of the host table, updating the record in the host table with data of the peer  
record.

36. The method of claim 35, further comprising, in response to determining that the MAC address of the peer record is not stored in a record of the host table, generating a new host device detection event.

37. The method of claim 34, further comprising, in response to determining that the IP address of the peer record is stored in a record of the host table:

determining whether an agent identifier of the record stored in the host table  
matches an agent identifier of the peer record;

in response to determining that the agent identifier of the record stored in the host  
table does not match the agent identifier of the peer record, determining whether the peer  
record is more recent than the record of the host table based on the time stamp of the peer  
record and the time stamp of the records in the host table;

in response to determining that the peer record is more recent than the record of the  
host table, deleting the record of the host table and generating a new host device detected  
event.

38. The method of claim 37, further comprising, in response to determining that the peer record is not more recent than the record of the host table:

determining whether a MAC address of the record stored in the host table matches a MAC address of the peer record;

in response to determining that the MAC address of the record stored in the host table does not match MAC address of the peer record, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, deleting the record stored in the host table and generating a new host detected event.

39. The method of claim 38, wherein each record includes a user identifier field, the user identifier field storing a user identifier of a user, and further comprising, in response to determining that the MAC address of the record stored in the host table matches MAC address of the peer record:

determining whether the user identifier of the peer records matches the user identifier of the record in the host table;

in response to determining that the user identifier of the peer record does not match the user identifier of the record stored in the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with the data of the peer record and generating a new user detection event.

40. The method of claim 39, further comprising, in response to determining that the user identifier of the peer record matches the user identifier of the record stored in the host table:

determining whether an information probe type of an information probe used to collect the data of the peer record is different from an information probe type of an information probe used to the data of the record stored in the host table;

in response to determining that the information probe type of the information probe used to collect the data of the peer record is different from the information probe type of the information probe used to the data of the record stored in the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with the data of the peer record and using, at the data processing apparatus, an information probe of the probe type used to collect the data of the peer record for subsequent probes to the host device.

41. The method of claim 34, wherein the time stamps are unsynchronized system clock values.

42. The method of claim 34, wherein the time stamp of the peer record is a difference of the system clock value of the peer data processing apparatus at the time the peer data processing apparatus transmitted the peer record a time stamp of the peer record stored as stored in the host table in the memory of the peer data processing apparatus.

43. The method of claim 34, wherein the time stamps are system clock values synchronized to a reference time.

44. A data processing apparatus, comprising:

a memory subsystem, an input/output subsystem that transmits and receives data over a network, and a processor in data communication with the memory subsystem and the input/output subsystem, the processor programmed to perform operations comprising:

storing in the memory of the data processing apparatus a host table, the host table including, for each of a plurality of host devices monitored on a network, a record

including:

- an IP address field for storing an IP address assigned to the host device;
- an agent identifier field for storing an agent identifier of agent installed on the host device; and

- a time stamp field for storing a time stamp indicating the time that host attributes were stored in the record;

- receiving from a peer data processing apparatus, in response to a synchronization event, a peer record for a host device, the peer record comprising data for a record stored in a host table in the memory of the peer data processing apparatus;

- determining whether an IP address of the peer record is stored in a record in the host table;

- in response to determining that the IP address of the peer record is not stored in a record of the host table:

- determining whether the peer record includes an agent identifier;

- in response to determining that the peer record includes the agent identifier, determining whether the agent identifier of the peer record is stored in a record of the host table;

- in response to determining that the agent identifier of the peer record is stored in a record of the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

- in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with data of the peer record.

45. The data processing apparatus of claim 44, wherein the processor is further programmed to perform operations comprising, in response to determining that the agent identifier of the peer record is not stored in a record of the host table:

determining whether the peer record includes a MAC address;

in response to determining that the peer record includes a MAC address, determining whether the MAC of the peer record is stored in a record of the host table;

in response to determining that the MAC address of the peer record is stored in a record of the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with data of the peer record.

46. The data processing apparatus of claim 45, wherein the processor is further programmed to perform operations comprising, in response to determining that the MAC address of the peer record is not stored in a record of the host table, generating a new host device detection event.

47. The data processing apparatus of claim 44, wherein the processor is further programmed to perform operations comprising, in response to determining that the IP address of the peer record is stored in a record of the host table:

determining whether an agent identifier of the record stored in the host table matches an agent identifier of the peer record;

in response to determining that the agent identifier of the record stored in the host table does not match the agent identifier of the peer record, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table;

in response to determining that the peer record is more recent than the record of the host table, deleting the record of the host table and generating a new host device detected event.

48. The data processing apparatus of claim 47, wherein the processor is further programmed to perform operations comprising, in response to determining that the peer record is not more recent than the record of the host table:

determining whether a MAC address of the record stored in the host table matches a MAC address of the peer record;

in response to determining that the MAC address of the record stored in the host table does not match MAC address of the peer record, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, deleting the record stored in the host table and generating a new host detected event.

49. The data processing apparatus of claim 48, wherein each record includes a user identifier field, the user identifier field storing a user identifier of a user, and wherein the processor is further programmed to perform operations comprising, in response to determining that the MAC address of the record stored in the host table matches MAC address of the peer record:

determining whether the user identifier of the peer records matches the user identifier of the record in the host table;

in response to determining that the user identifier of the peer record does not match the user identifier of the record stored in the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with the data of the peer record and generating a new user detection event.

50. The data processing apparatus of claim 49, wherein the processor is further programmed to perform operations comprising, in response to determining that the user identifier of the peer record matches the user identifier of the record stored in the host table:

determining whether an information probe type of an information probe used to collect the data of the peer record is different from an information probe type of an information probe used to the data of the record stored in the host table;

in response to determining that the information probe type of the information probe used to collect the data of the peer record is different from the information probe type of the information probe used to the data of the record stored in the host table, determining whether the peer record is more recent than the record of the host table based on the time stamp of the peer record and the time stamp of the records in the host table; and

in response to determining that the peer record is more recent than the record of the host table, updating the record in the host table with the data of the peer record and using, at the data processing apparatus, an information probe of the probe type used to collect the data of the peer record for subsequent probes to the host device.

51. A system, comprising:

a pair of peer sensors configured to control access to a network for a plurality of host devices, each of the peer sensors including a memory subsystem, an input/output subsystem that transmits and receives data over the network, and a processor in data communication with the memory subsystem and the input/output subsystem, wherein each processor is processor programmed to cause each peer sensor to perform operations comprising:

storing in the memory of the peer sensor a host table, the host table including, for each of the plurality of host devices monitored on the network by the peer sensors, a record including:

an IP address field for storing an IP address assigned to the host device;

an agent identifier field for storing an agent identifier of agent installed on the host device; and

a time stamp field for storing a time stamp indicating the time that host attributes were stored in the record;

receiving from the other peer sensor, in response to a synchronization event, peer record for a host device, the peer record being a record stored in the host table in the memory the other peer sensor;

determining whether an IP address of the peer record is stored in a record in host table of the peer sensor;

in response to determining that the IP address of the peer record is not stored in a record of the host table of the peer sensor:

determining whether the peer record includes an agent identifier;

in response to determining that the peer record includes the agent identifier, determining whether the agent identifier of the peer record is stored in a record of the host table of the peer sensor;

in response to determining that the agent identifier of the peer record is stored in a record of the host table of the peer sensor, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table; and

in response to determining that the peer record is more recent than the record of the host table of the peer sensor, updating the record in the host table of the

peer sensor with data of the peer record.

52. The system of claim 51, wherein each processor is further programmed to cause each peer sensor to perform operations comprising, in response to determining that the agent identifier of the peer record is not stored in a record of the host table of the peer sensor:

determining whether the peer record includes a MAC address;

in response to determining that the peer record includes a MAC address, determining whether the MAC of the peer record is stored in a record of the host table peer sensor;

in response to determining that the MAC address of the peer record is stored in a record of the host table of the peer sensor, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table of the peer sensor;

in response to determining that the peer record is more recent than the record of the host table of the peer sensor, updating the record in the host table of the peer sensor with data of the peer record; and

in response to determining that the MAC address of the peer record is not stored in a record of the host table of the peer sensor, generating a new host device detection event.

53. The system of claim 52, wherein each processor is further programmed to cause each peer sensor to perform operations comprising, in response to determining that the IP address of the peer record is stored in a record of the host table:

determining whether an agent identifier of the record stored in the host table of the peer sensor matches an agent identifier of the peer record;

in response to determining that the agent identifier of the record stored in the host table of the peer sensor does not match the agent identifier of the peer record, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table;

in response to determining that the peer record is more recent than the record of the host table, deleting the record of the host table and generating a new host device detected event.

54. The system of claim 53, wherein each processor is further programmed to cause each peer sensor to perform operations comprising, in response to determining that the peer record is not more recent than the record of the host table:

determining whether a MAC address of the record stored in the host table of the peer sensor matches a MAC address of the peer record;

in response to determining that the MAC address of the record stored in the host table of the peer sensor does not match MAC address of the peer record, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table; and

in response to determining that the peer record is more recent than the record of the host table of the peer sensor, deleting the record stored in the host table and generating a new host detected event.

55. The system of claim 54, wherein each record includes a user identifier field, the user identifier field storing a user identifier of a user, and wherein each processor is further programmed to cause each peer sensor to perform operations comprising, in response to determining that the MAC address of the record stored in the host table of the peer sensor matches MAC address of the peer record:

determining whether the user identifier of the peer record matches the user identifier of the record in the host table of the peer sensor;

in response to determining that the user identifier of the peer record does not match the user identifier of the record stored in the host table of the peer sensor, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table of the peer sensor; and

in response to determining that the peer record is more recent than the record of the host table of the peer sensor, updating the record in the host table of the peer sensor with the data of the peer record and generating a new user detection event.

56. The system of claim 55, wherein each processor is further programmed to cause each peer sensor to perform operations comprising, in response to determining that the user identifier of the peer record matches the user identifier of the record stored in the host table of the peer sensor:

determining whether an information probe type of an information probe used to collect the data of the peer record is different from an information probe type of an information probe used to the data of the record stored in the host table of the peer sensor;

in response to determining that the information probe type of the information probe used to collect the data of the peer record is different from the information probe type of the information probe used to the data of the record stored in the host table of the peer sensor, determining whether the peer record is more recent than the record of the host table of the peer sensor based on the time stamp of the peer record and the time stamp of the record in the host table; and

in response to determining that the peer record is more recent than the record of the host table of the peer sensor, updating the record in the host table of the peer sensor with the data of the peer record and using an information probe of the probe type used to collect the data of the peer record for subsequent probes to the host device.

57. A method for controlling access to a network, the method performed by a data processing apparatus, the method comprising:

- defining a state machine in a memory of the data processing apparatus, the state machine comprising a plurality of states, and wherein network access for a host device is controlled in each state according to one or more network access zones associated with the state, each network access zone defining network access capabilities for the host device;

- monitoring, by the data processing apparatus, host devices attempting to access the network and host devices that have access to the network;

- transitioning, for each host device, a state of the host based on the monitoring and a current state of the host;

- storing in the memory of the data processing apparatus, for each monitored host device attempting to access the network or that has access to the network:

- host attributes of the host device that identify the host; and

- the state of the host; and

- controlling network access of the host device according to the one or more network access zones associated with the state of the host device.

58. The method of claim 56, wherein the states comprise:

an initial preadmission state during which the data processing apparatus sends host information collection queries to the host device to receive host attributes from the host device in response;

a host detection preadmission state during which the data processing apparatus determines a host status based on the host attributes of the host;

a user detection preadmission state during which a user identifier associated with the host device is mapped to a user role associated with a corresponding network access zone; and

a post admission state during which the host device is granted access to the network according to a one of a plurality of network access zones; and

transitioning the state of the host device based on the monitoring and the state of the host comprises:

transitioning the state of the host device to the initial preadmission state when the host attributes stored in the memory are a new entry in the memory for the host device;

transitioning the state of the host device to the user detection preadmission state from the initial preadmission state or the host detection preadmission state when an identity-based access control process is enabled for the host device and a user identifier for the host device has been determined;

transitioning the state of the host device to the host detection preadmission state from the initial preadmission state when the identity-based access control process is enabled for the host device and host attributes of the host are not received in response to host information collection queries or a media access control address is received in a data link layer detection mode;

transitioning the state of the host device from the host detection preadmission state to the post admission state when the host is determined to be a managed host or the host is determined to be an unmanaged host with a pre-determined health level that is acceptable for transition to the post admission state; and

transitioning the state of the host device from the user detection preadmission state to the post admission state when the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is disabled.

59. The method of claim 58, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning the state of the host device from the user detection preadmission state to the host detection preadmission state when the user identifier is mapped to a user role and further network accesses control for the user role is enabled.

60. The method of claim 58, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning the state of the host device from the post admission state to the user detection preadmission state when a user logout of the host device is detected.

61. The method of claim 58, wherein:

the states further comprise a secure guest preadmission state during which HTTP traffic from the host device is directed to a guest access portal managed by the data processing apparatus and which causes the host device to generate a user login and password prompt and receive a user identifier and password in response; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the initial preadmission state to the secure guest preadmission state when the identity based access-control process for the host device is enabled and the host attributes received for the host device indicate that the host device is not a member of a predefined directory or a user identifier for the host is not determined from the received host attributes; and

transitioning from the secure guest preadmission state to the user detection preadmission state when the user identifier is determined.

62. The method of claim 58, wherein:

the states further comprise a remediate preadmission state during which HTTP traffic from the host device is directed to a remediate portal managed by the data processing apparatus and which caused an agent to be downloaded to the host device, the agent being configured to provide health data indicating a health level of the host device; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the initial preadmission state to the remediate preadmission state when the host is determined to be an unmanaged host with an unknown health level; and

transitioning from the remediate preadmission state to the post admission state when the host device is determined, from the health data provided by the agent, to have health level that is acceptable for transition to the post admission state.

63. The method of claim 62, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning from the user detection preadmission state to the remediate preadmission state the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is enabled.

64. The method of claim 58, wherein:

the states further comprise a post boot admission state during which the host attributes of all hosts stored in a persistent memory prior to a reboot of the data processing apparatus and after reboot of the data processing apparatus determines a host status based on the host attributes of the host; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the post boot admission state to the post admission state when the host attributes of the host device received after the reboot match the host attributes of the host device stored in the persistent memory.

65. The method of claim 58, wherein:

the states further comprise a quarantine post admission state during which network access for the host is limited to a quarantine zone; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the quarantine post admission state in response to determining that the health level of the host device is acceptable for transition to the post admission state.

66. The method of claim 56, wherein the network access capabilities of each network zone are configurable by an administrator.

67. A data processing apparatus, comprising:

a memory subsystem, an input/output subsystem that transmits and receives data over a network, and a processor in data communication with the memory subsystem and the input/output subsystem, the processor programmed to perform operations comprising:

defining a state machine in the memory, the state machine comprising a plurality of states, and wherein network access for a host device is controlled in each state according to one or more network access zones associated with the state, each network access zone defining network access capabilities for the host device;

monitoring host devices attempting to access the network and host devices that have access to the network;

transitioning a state of the host based on the monitoring and a current state of the host;

storing in the memory, for each monitored host device attempting to access the network or that has access to the network:

host attributes of the host device that identify the host; and

the state of the host; and

controlling network access of the host device according to the one or more network access zones associated with the state of the host device.

68. The data processing apparatus of claim 67, wherein the states comprise:

an initial preadmission state during which the processor sends host information collection queries to the host device and receives host attributes from the host device in response;

a host detection preadmission state during which the processor determines a host status based on the host attributes of the host;

a user detection preadmission state during which a user identifier associated with the host device is mapped to a user role associated with a corresponding network access zone; and

a post admission state during which the processor grants the host device access to the network according to a one of a plurality of network access zones; and

transitioning the state of the host device based on the monitoring and the state of the host comprises:

transitioning the state of the host device to the initial preadmission state when the host attributes stored in the memory are a new entry in the memory for the host device;

transitioning the state of the host device to the user detection preadmission state from the initial preadmission state or the host detection preadmission state when an identity-based access control process is enabled for the host device and a user identifier for the host device has been determined;

transitioning the state of the host device to the host detection preadmission state from the initial preadmission state when the identity-based access control process is enabled for the host device and host attributes of the host are not received in response to host information collection queries or a media access control address is received in a data link layer detection mode;

transitioning the state of the host device from the host detection preadmission state to the post admission state when the host is determined to be a managed host or the host is determined to be an unmanaged host with a pre-determined health level that is acceptable for transition to the post admission state; and

transitioning the state of the host device from the user detection preadmission state to the post admission state when the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses

control for this role is disabled.

69. The data processing apparatus of claim 67, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning the state of the host device from the user detection preadmission state to the host detection preadmission state when the user identifier is mapped to a user role and further network accesses control for the user role is enabled.

70. The data processing apparatus of claim 67, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning the state of the host device from the post admission state to the user detection preadmission state when a user logout of the host device is detected.

71. The data processing apparatus of claim 67, wherein:

the states further comprise a secure guest preadmission state during which HTTP traffic from the host device is directed to a guest access portal managed by the data processing apparatus and which causes the host device to generate a user login and password prompt and receive a user identifier and password in response; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the initial preadmission state to the secure guest preadmission state when the identity based access-control process for the host device is enabled and the host attributes received for the host device indicate that the host device is not a member of a predefined directory or a user identifier for the host is not determined from the received host attributes; and

transitioning from the secure guest preadmission state to the user detection preadmission state when the user identifier is determined.

72. The data processing apparatus of claim 67, wherein:

the states further comprise a remediate preadmission state during which HTTP traffic from the host device is directed to a remediate portal managed by the data processing apparatus and which caused an agent to be downloaded to the host device, the agent being configured to provide health data indicating a health level of the host device; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the initial preadmission state to the remediate preadmission state when the host is determined to be an unmanaged host with an unknown health level; and

transitioning from the remediate preadmission state to the post admission state when the host device is determined, from the health data provided by the agent, to have health level that is acceptable for transition to the post admission state.

73. The data processing apparatus of claim 72, wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises transitioning from the user detection preadmission state to the remediate preadmission state the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is enabled.

74. The data processing apparatus of claim 67, wherein:

the states further comprise a post boot admission state during which the host attributes of all hosts stored in a persistent memory prior to a reboot of the data processing apparatus and after reboot of the data processing apparatus determines a host status based on the host attributes of the host; and

wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:

transitioning from the post boot admission state to the post admission state when the host attributes of the host device received after the reboot match the host attributes of the host device stored in the persistent memory.

75. The data processing apparatus of claim 67, wherein:
- the states further comprise a quarantine post admission state during which network access for the host is limited to a quarantine zone; and
  - wherein transitioning the state of the host device based on the monitoring and the state of the host device further comprises:
    - transitioning from the quarantine post admission state in response to determining that the health level of the host device is acceptable for transition to the post admission state.

76. A data processing apparatus, comprising:

a memory subsystem, an input/output subsystem that transmits and receives data over a network, and a processor in data communication with the memory subsystem and the input/output subsystem, the processor programmed to perform operations comprising:

defining a state machine in the memory, the state machine comprising a plurality of states, and wherein network access for a host device is controlled in each state according to one or more network access zones associated with the state, each network access zone defining network access capabilities for the host device, wherein the states comprise:

an initial preadmission state during which the processor sends host information collection queries to the host device and receives host attributes from the host device in response;

a host detection preadmission state during which the processor determines a host status based on the host attributes of the host;

a user detection preadmission state during which a user identifier associated with the host device is mapped to a user role associated with a corresponding network access zone; and

a post admission state during which the processor grants the host device access to the network according to a one of a plurality of network access zones;

monitoring host devices attempting to access the network and host devices that have access to the network;

transitioning a state of the host device to the initial preadmission state when the host attributes indicate a new host device attempting to access the network;

transitioning the state of the host device to the user detection preadmission state from the initial preadmission state or the host detection preadmission state when an identity-based access control process is enabled for the host device and a user identifier for the host device has been determined;

transitioning the state of the host device to the host detection preadmission state from the initial preadmission state when the identity-based access control process is enabled for the host device and host attributes of the host are not received in response to host information collection queries;

transitioning the state of the host device from the host detection preadmission state

to the post admission state when the host is determined to be a managed host or the host is determined to be an unmanaged host with a pre-determined health level that is acceptable for transition to the post admission state; and

transitioning the state of the host device from the user detection preadmission state to the post admission state when the user identifier is mapped to a user role associated with a corresponding network access zone and further network accesses control for this role is disabled.

77. A system, comprising:

a pair of peer sensors to control access to a network for a plurality of host devices, one of the peer sensors being designated a primary sensor and the other peer sensor being designated a secondary sensor, each peer sensor comprising a memory subsystem, an input/output subsystem that transmits and receives data over the network, and a processor in data communication with the memory subsystem and the input/output subsystem, wherein the processors of the primary sensor and secondary sensor are respectively programmed to cause the primary sensor and the secondary sensor to perform operations comprising:

in response to a detection of a host device attempting to access the network, transmitting, from each of the primary sensor and the secondary sensor, a plurality of information probes to the host device, each of the information probes being prioritized according to their probe types by the primary sensor in a descending priority order;

determining, at the primary sensor, a first probe type, the first probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the primary sensor;

determining, at the secondary sensor, a second probe type, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor;

transmitting, from the secondary sensor, data indicating the second probe type to the primary sensor;

determining, at the primary sensor, whether the second probe type is prioritized higher than the first probe type;

in response to determining the second probe type is prioritized higher than the first probe type, transmitting, from the primary sensor, data indicating a probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor; and

transmitting subsequent information probes to the host device from the secondary sensor.

78. The system of claim 77, wherein:

the processors of the primary sensor and the secondary sensor are programmed to cause each sensor to store in its respective memory a host table, the host table including, for each of a plurality of host devices monitored on the network by the primary and the secondary sensor, a record including identification information describing the identity of the host device; and

wherein the processor of the primary sensor is further programmed to cause the primary sensor to store, for each host device, the first and second probe types of the information probes used by the primary sensor and the secondary sensor for the host device;

and wherein the processor of the secondary sensor is further programmed to cause the secondary sensor to perform operations comprising:

transmitting information probes to the host device in response to receiving data indicating the probe handover from the primary sensor;

determining that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the secondary sensor, and in response to the determination that the host device is offline:

deleting a record for the host device from the host table in the memory of the secondary sensor; and

transmitting data indicating the host device is offline to the primary sensor.

79. The system of claim 78, where the processor of the primary sensor is further programmed to cause the primary sensor to perform operations comprising, in response to receiving from the secondary sensor the data indicating the host device is offline, deleting a record for the host device from the host table in the memory of the primary sensor.

80. The system of claim 78, wherein the processor of the primary sensor is further programmed to cause the primary sensor to perform, in response to determining the second probe type is not prioritized higher than the first probe type, operations comprising:

determining that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the primary sensor, and in response to the determination that the host device is offline:

determining whether the second probe type prioritized equally to the first probe type; and

in response to determining that the second probe type prioritized equally to the first probe type, transmitting, from the primary sensor, data indicating the probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor.

81. The system of claim 80 wherein:

the processor of the primary sensor is further programmed to cause the primary sensor to perform, in response to determining that the second probe type is not prioritized equally to the first probe type, operations comprising:

deleting a record for the host device from the host table in the memory of the primary sensor; and

transmitting data indicating the host device is offline to the secondary sensor.

82. The system of claim 81, wherein the processor of the primary sensor is further programmed to cause the primary sensor to perform operations comprising, in response to receiving from the secondary sensor the data indicating the host device is offline, deleting a record for the host device from the host table in the memory of the primary sensor.

83. The system of claim 77, wherein the information probes include:

an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes request one or more other host attributes; and

the probe type of the agent probe is the highest priority probe type.

84. The system of claim 83, wherein the information probes include an NBTSTAT query, and the probe type of the NBTSTAT is lower in priority than the probe type of the agent probe.

85. The system of claim 84, wherein the information probes include an IMCP ping, and the probe type of the IMCP ping is lower in priority than the probe type of the agent probe.

86. The system of claim 85, wherein the probe type of the IMCP ping is lower in priority than the probe type of the NBTSTAT query.

87. A method performed by a pair of network traffic sensors, one of the sensors being designated a primary sensor and the other of the sensors being designated a secondary sensor, the method comprising:

in response to a detection of a host device attempting to access the network, transmitting, from each of the primary sensor and the secondary sensor, a plurality of information probes to the host device, each of the information probes being prioritized according to their probe types by the primary sensor in a descending priority order;

determining, at the primary sensor, a first probe type, the first probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the primary sensor;

- determining, at the secondary sensor, a second probe type, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor;

transmitting, from the secondary sensor, data indicating the second probe type to the primary sensor;

determining, at the primary sensor, whether the second probe type is prioritized higher than the first probe type;

in response to determining the second probe type is prioritized higher than the first probe type, transmitting, from the primary sensor, data indicating a probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor; and

transmitting subsequent information probes to the host device from the secondary sensor.

88. The method of claim 87, wherein:

storing a host table in respective memories of the primary sensor and the secondary sensor, the host table including, for each of a plurality of host devices monitored on the network by the primary sensor and the secondary sensor, a record including identification information describing the identity of the host device;

storing in the memory of the primary sensor, for each host device, the first and second probe types of the information probes used by the primary sensor and the secondary sensor for the host device;

transmitting, from the secondary sensor, information probes to the host device in response to receiving data indicating the probe handover from the primary sensor;

determining, by the secondary sensor, that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the secondary sensor, and in response to the determination that the host device is offline:

deleting a record for the host device from the host table in the memory of the secondary sensor; and

transmitting, from the secondary sensor to the primary sensor, data indicating the host device is offline.

89. The method of claim 88, further comprising deleting, at the primary sensor, a record for the host device from the host table in the memory of the primary sensor in response to receiving from the secondary sensor the data indicating the host device is offline.

90. The method of claim 88, further comprising:

in response to determining, by the primary sensor, the second probe type is not prioritized higher than the first probe type:

determining, by the primary sensor, that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the primary sensor, and in response to the determination that the host device is offline:

determining, by the primary sensor, whether the second probe type prioritized equally to the first probe type; and

in response to determining that the second probe type prioritized equally to the first probe type, transmitting, from the primary sensor, data indicating the probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor.

91. The method of claim 90, further comprising:

in response to determining, by the primary sensor, that the second probe type is not prioritized equally to the first probe type:

deleting a record for the host device from the host table in the memory of the primary sensor; and

transmitting, from the primary sensor, data indicating the host device is offline to the secondary sensor.

92. The method of claim 91, further comprising:

in response to the primary sensor receiving from the secondary sensor the data indicating the host device is offline, deleting a record for the host device from the host table in the memory of the primary sensor.

93. The method of claim 87, wherein the information probes include:

an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes request one or more other host attributes; and

the probe type of the agent probe is the highest priority probe type.

94. The method of claim 93, wherein the information probes include an NBTSTAT query, and the probe type of the NBTSTAT is lower in priority than the probe type of the agent probe.

95. The method of claim 94, wherein the information probes include an ICMP ping, and the probe type of the ICMP ping is lower in priority than the probe type of the agent probe.

96. The method of claim 95, wherein the probe type of the ICMP ping is lower in priority than the probe type of the NBTSTAT query.

97. A method performed by a network traffic sensor, the sensor being designated a primary sensor and paired with another sensor designated a secondary sensor, the method comprising:

in response to a detection of a host device attempting to access the network, transmitting a plurality of information probes to the host device, each of the information probes being prioritized according to their probe types by the primary sensor in a descending priority order;

determining a first probe type, the first probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the primary sensor;

receiving, from the secondary sensor, data indicating the second probe type to the primary sensor, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor;

determining whether the second probe type is prioritized higher than the first probe type;

in response to determining the second probe type is prioritized higher than the first probe type, transmitting, from the primary sensor, data indicating a probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor.

98. The method of claim 97, further comprising:

storing a host table in a memory of the primary sensor, the host table including, for each of a plurality of host devices monitored on the network by the primary sensor and the secondary sensor, a record including identification information describing the identity of the host device, and the first and second probe types of the information probes used by the primary sensor and the secondary sensor for the host device;

receiving, from the secondary sensor, data indicating the host device is offline and in response, deleting a record for the host device from the host table in the memory of the primary sensor.

99. The method of claim 98, further comprising:

in response to determining, by the primary sensor, the second probe type is not prioritized higher than the first probe type:

determining, by the primary sensor, that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the primary sensor, and in response to the determination that the host device is offline:

determining, by the primary sensor, whether the second probe type prioritized equally to the first probe type; and

in response to determining that the second probe type prioritized equally to the first probe type, transmitting, from the primary sensor, data indicating the probe handover to the secondary sensor and precluding further probing of the host device from the primary sensor.

100. The method of claim 99, further comprising:

in response to determining, by the primary sensor, that the second probe type is not prioritized equally to the first probe type:

deleting a record for the host device from the host table in the memory of the primary sensor; and

transmitting, from the primary sensor, data indicating the host device is offline to the secondary sensor.

101. The method of claim 100, wherein the information probes include:

an agent probe that queries an agent installed on the host device for a unique agent identifier, and each of the information probes request one or more other host attributes; and

an NBTSTAT query;

wherein:

the probe type of the agent probe is the highest priority probe type, and the probe type of the NBTSTAT is lower in priority than the probe type of the agent probe.

102. A method performed by a network traffic sensor, the sensor being designated a secondary sensor and paired with another sensor designated a primary sensor, the method comprising:

in response to a detection of a host device attempting to access the network, transmitting a plurality of information probes to the host device, each of the information probes being prioritized according to their probe types by the primary sensor in a descending priority order;

determining a second probe type, the second probe type being the probe type of the highest priority information probe for which a reply from the host device was received at the secondary sensor;

transmitting, from the secondary sensor, data indicating the second probe type to the primary sensor; and

precluding further probing of the host device from the secondary sensor until data indicating a probe handover is received from the primary sensor.

103. The method of claim 102, further comprising:

storing a host table in a memory of the secondary sensor, the host table including, for each of a plurality of host devices monitored on the network by the primary sensor and the secondary sensor, a record including identification information describing the identity of the host device;

transmitting, from the secondary sensor, information probes to the host device in response to receiving data indicating the probe handover from the primary sensor;

determining, by the secondary sensor, that the host device is offline in response to a failure to receive a reply from the host device to an information probe transmitted from the secondary sensor, and in response to the determination that the host device is offline:

deleting a record for the host device from the host table in the memory of the secondary sensor; and

transmitting, from the secondary sensor to the primary sensor, data indicating the host device is offline.

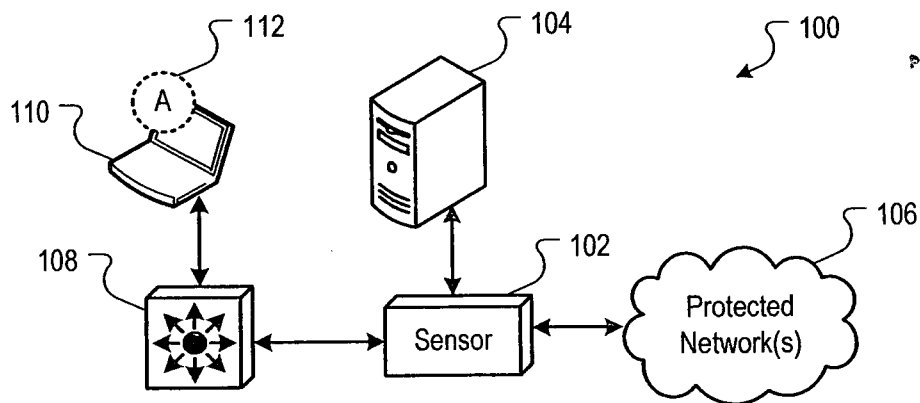


FIG. 1

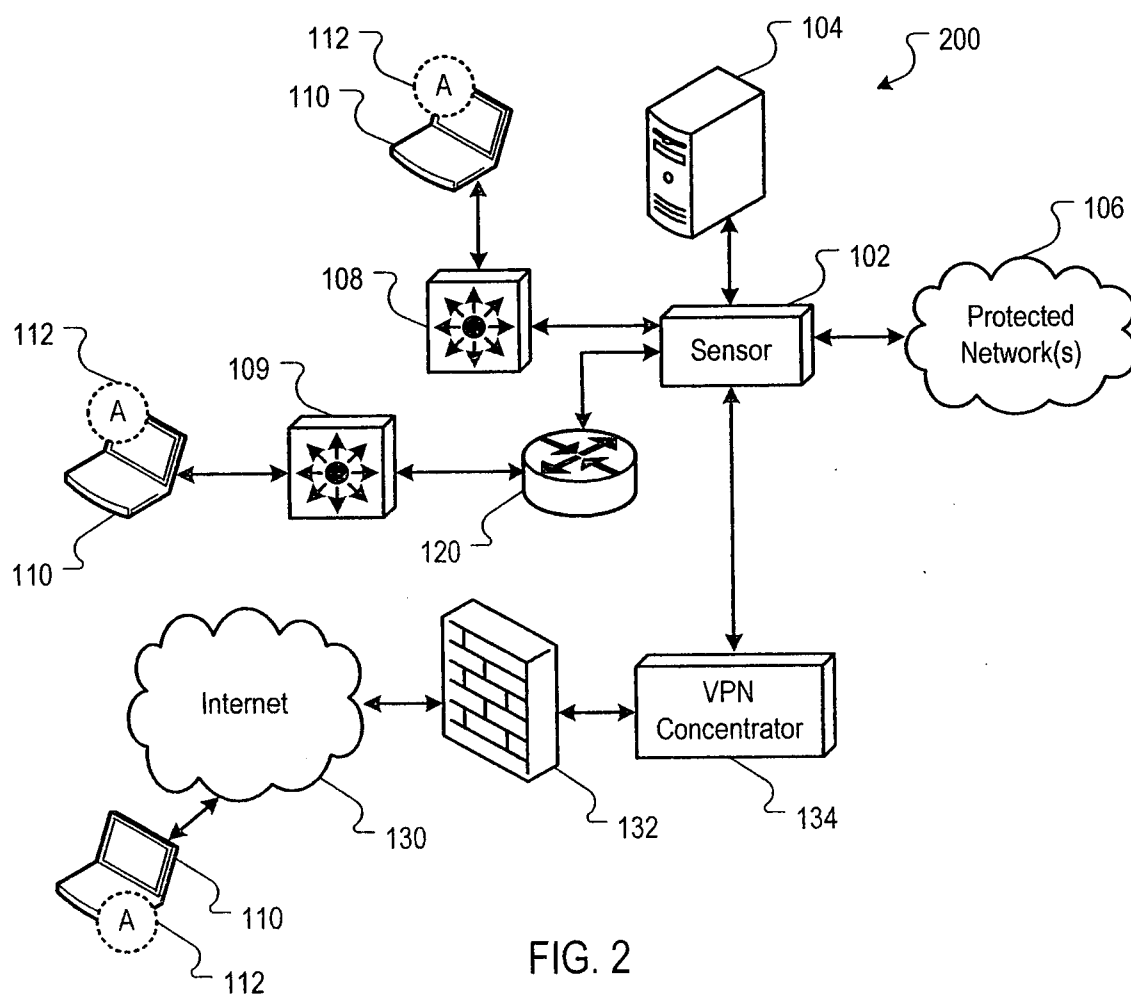


FIG. 2

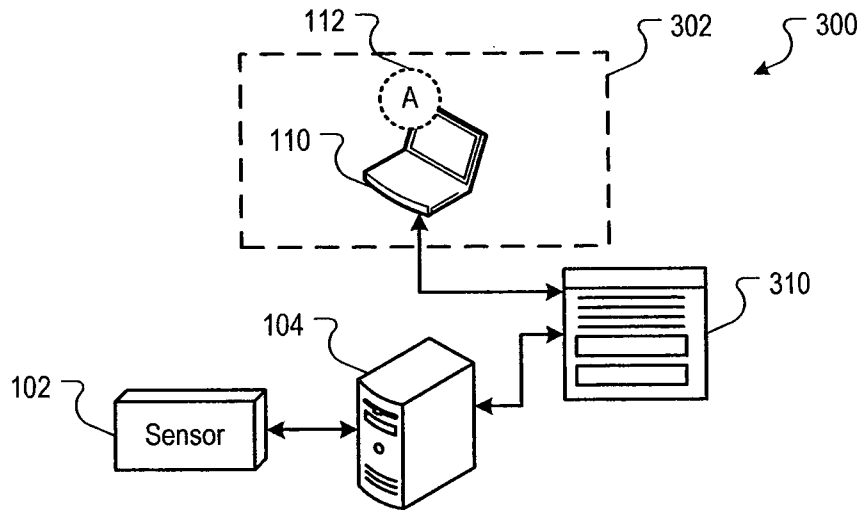


FIG. 3

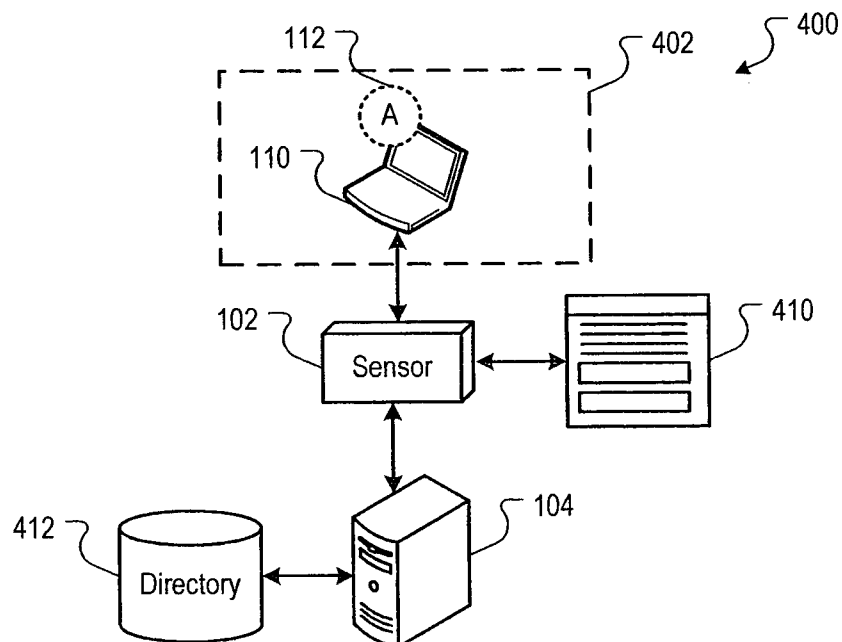


FIG. 4

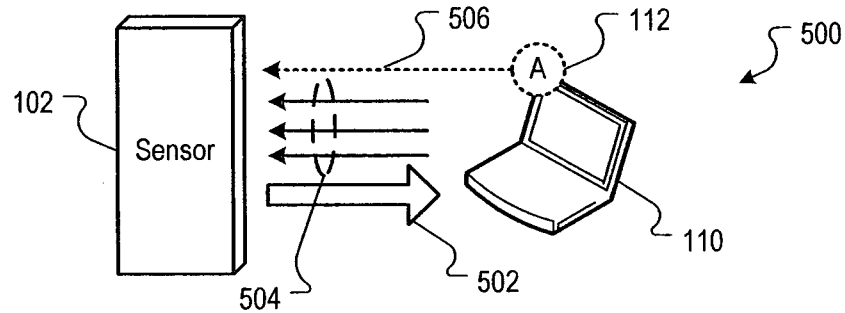


FIG. 5

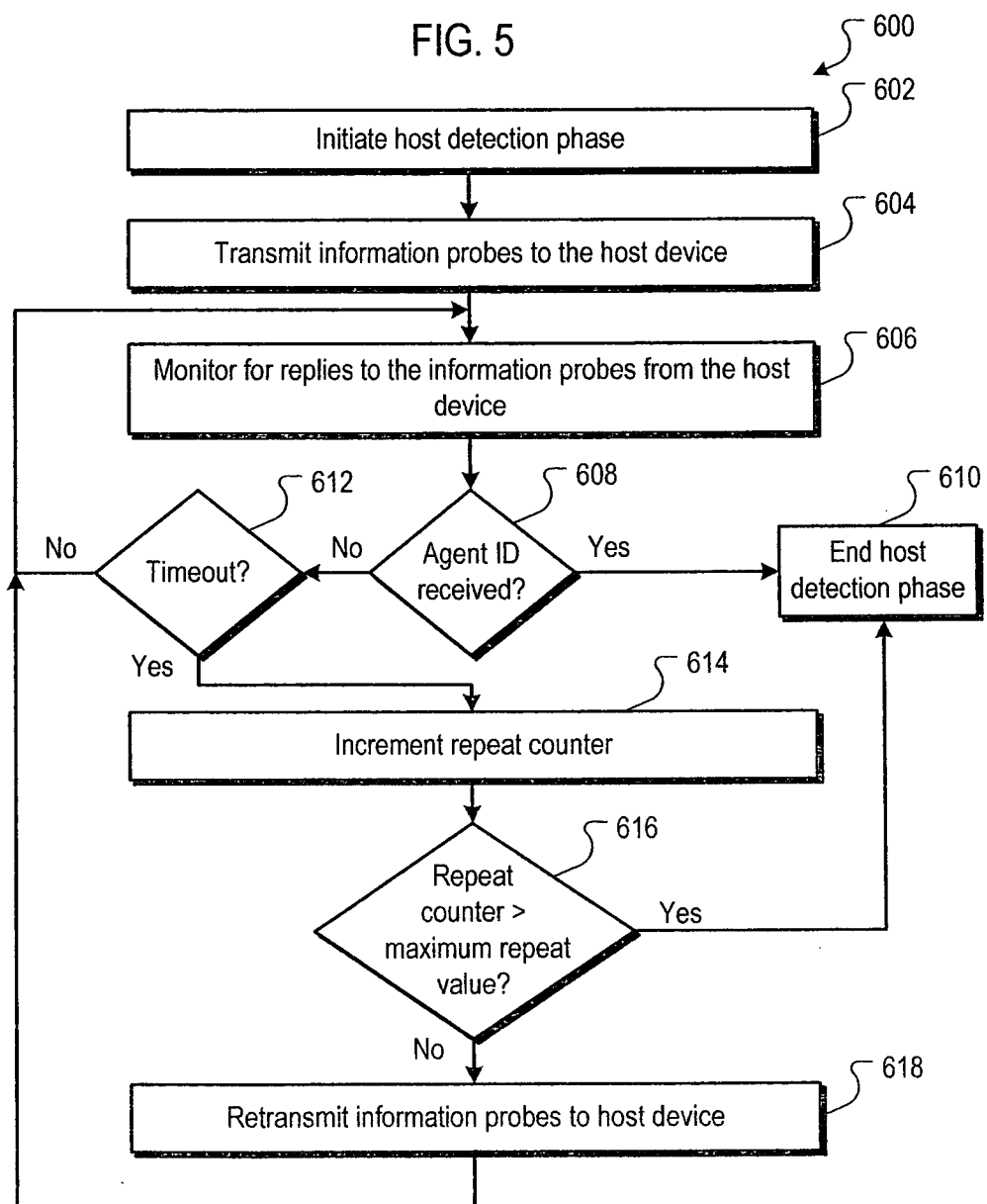


FIG. 6

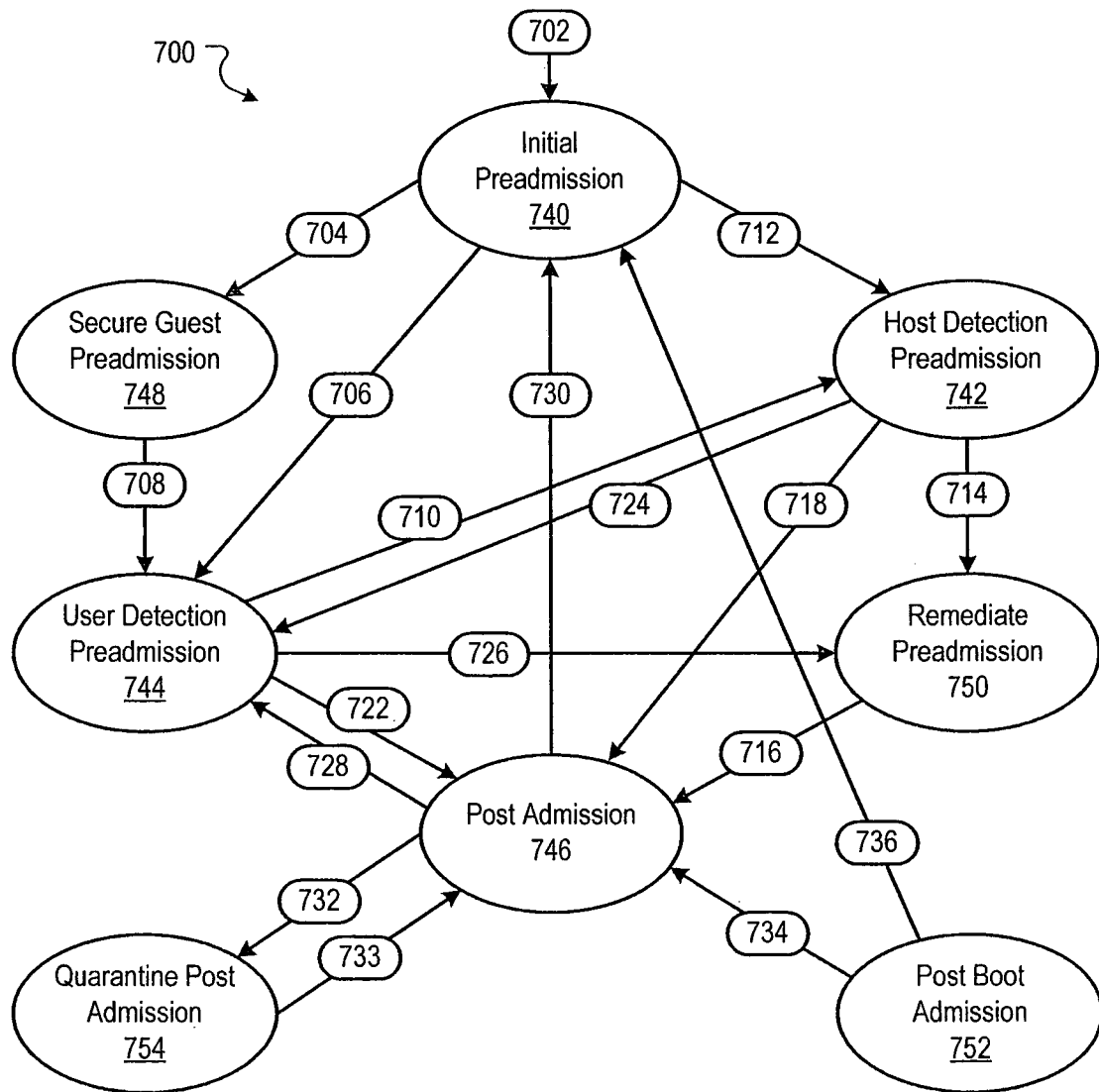


FIG. 7

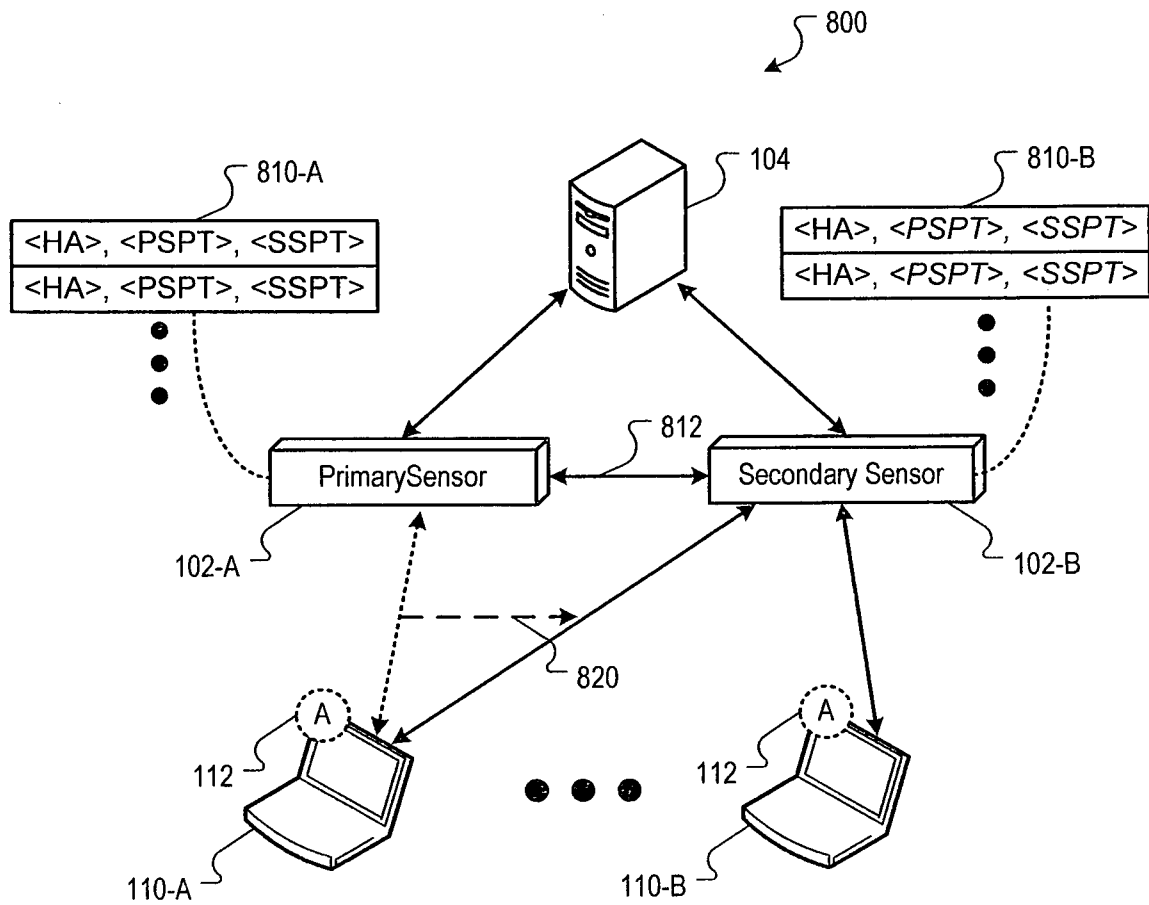


FIG. 8

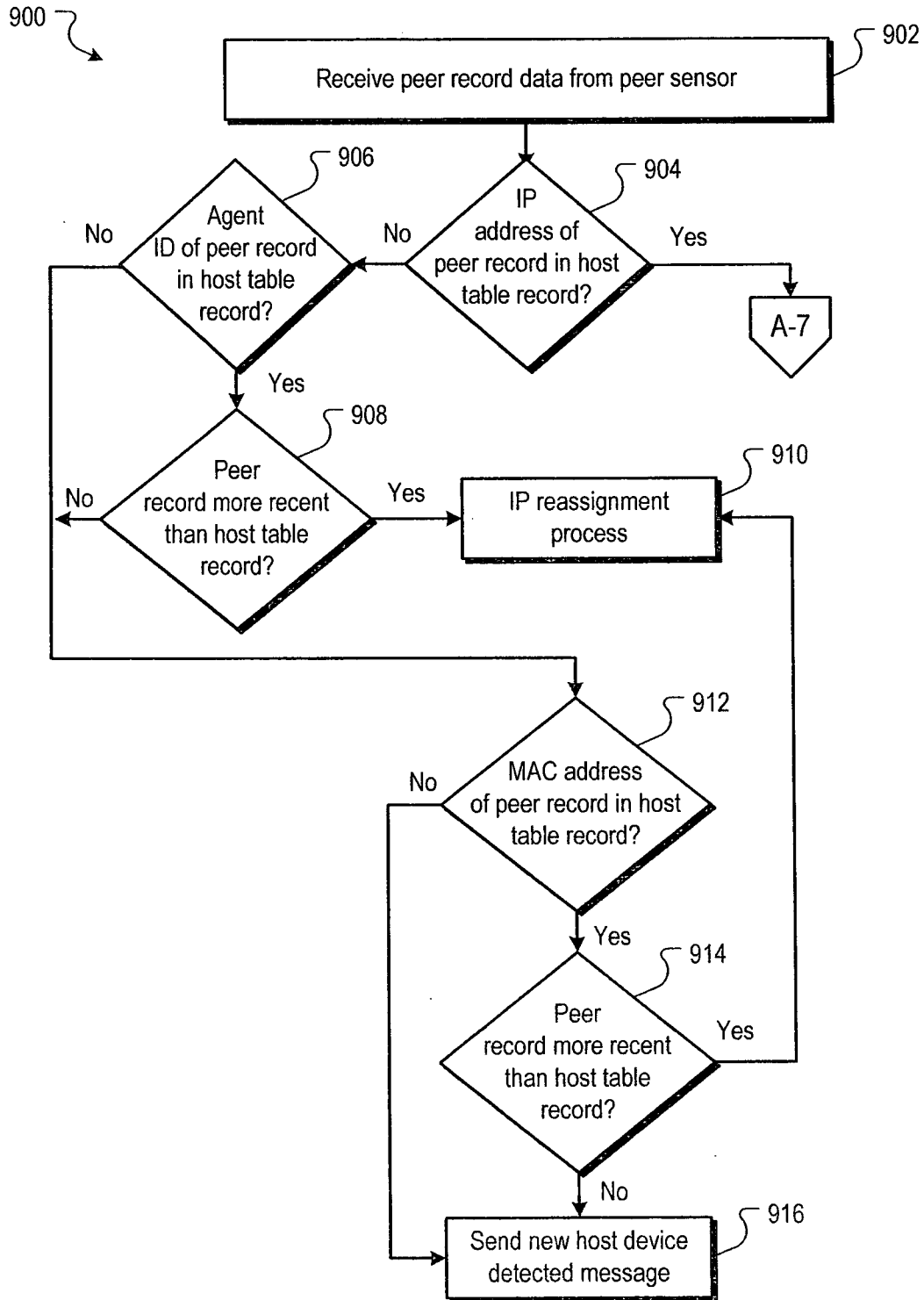


FIG. 9A

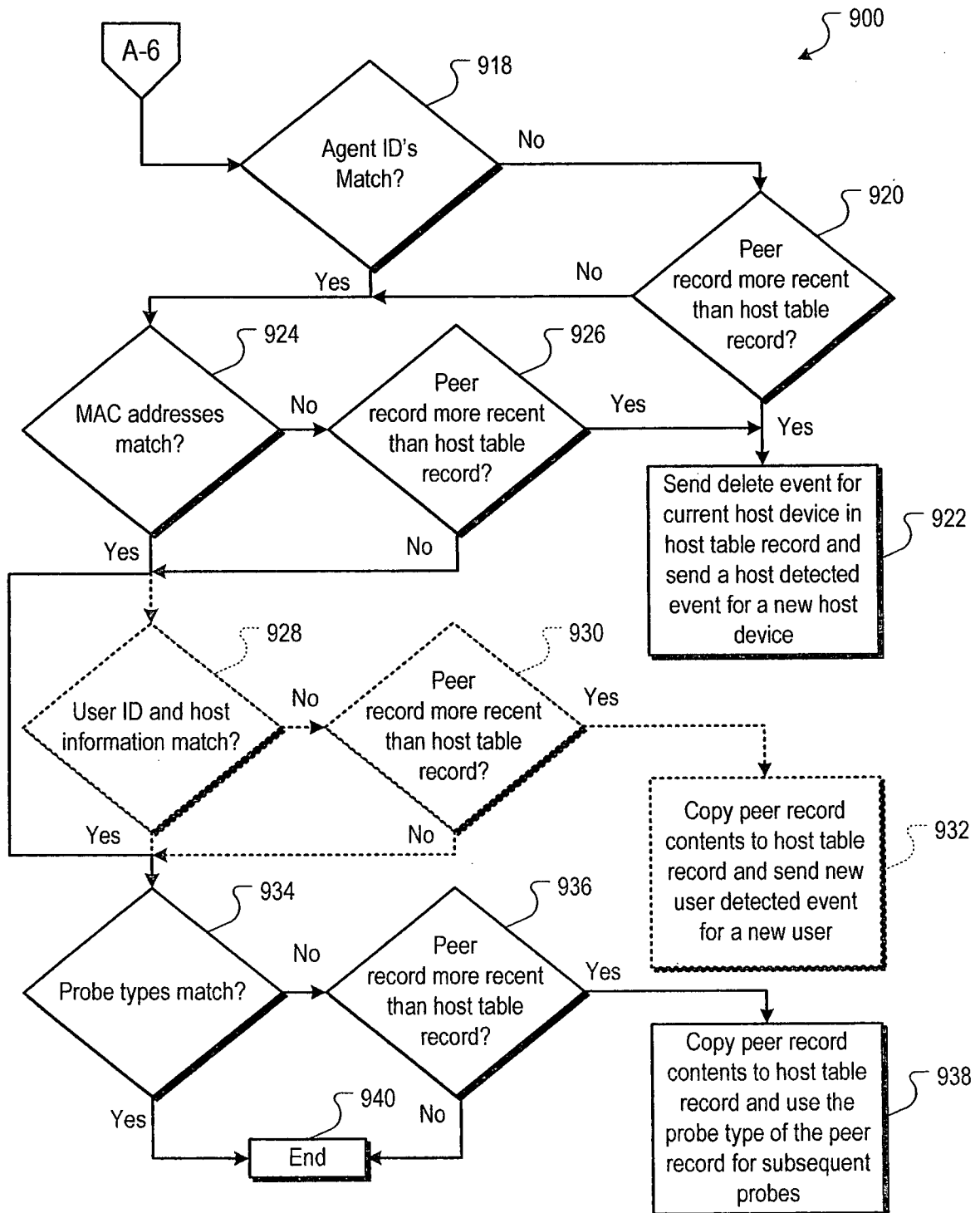


FIG. 9B

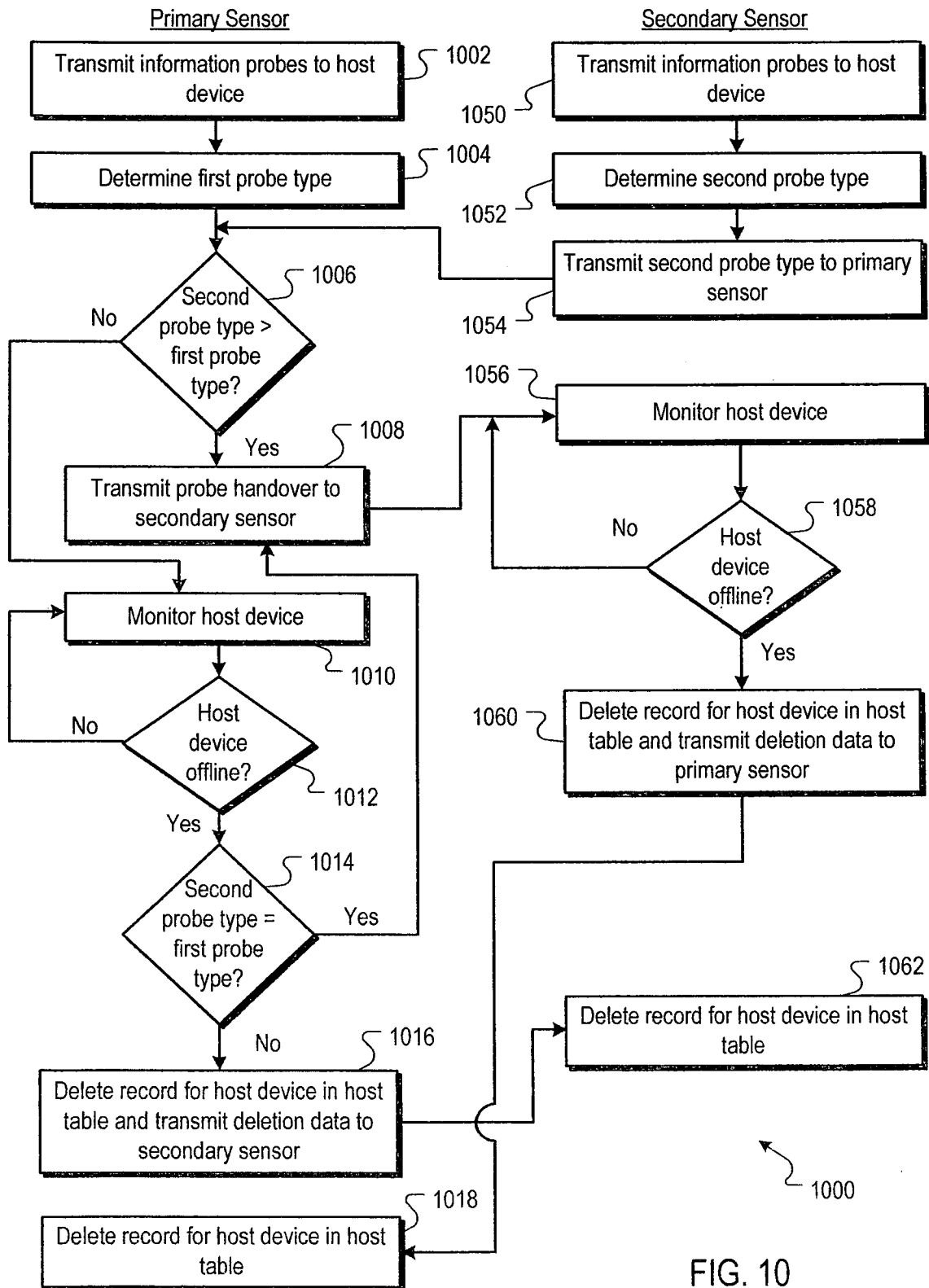


FIG. 10

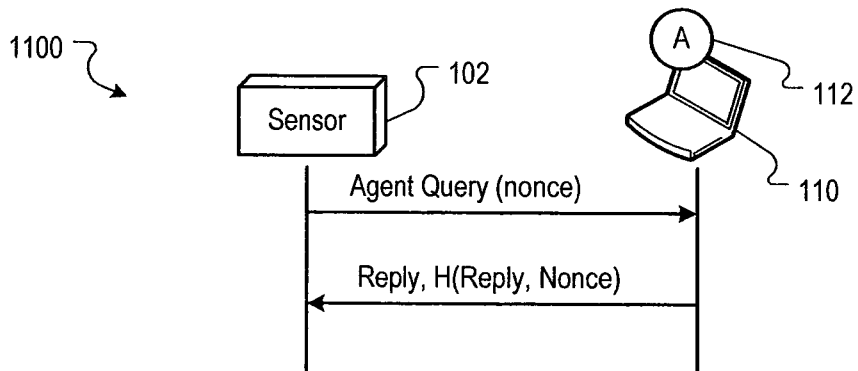


FIG. 11

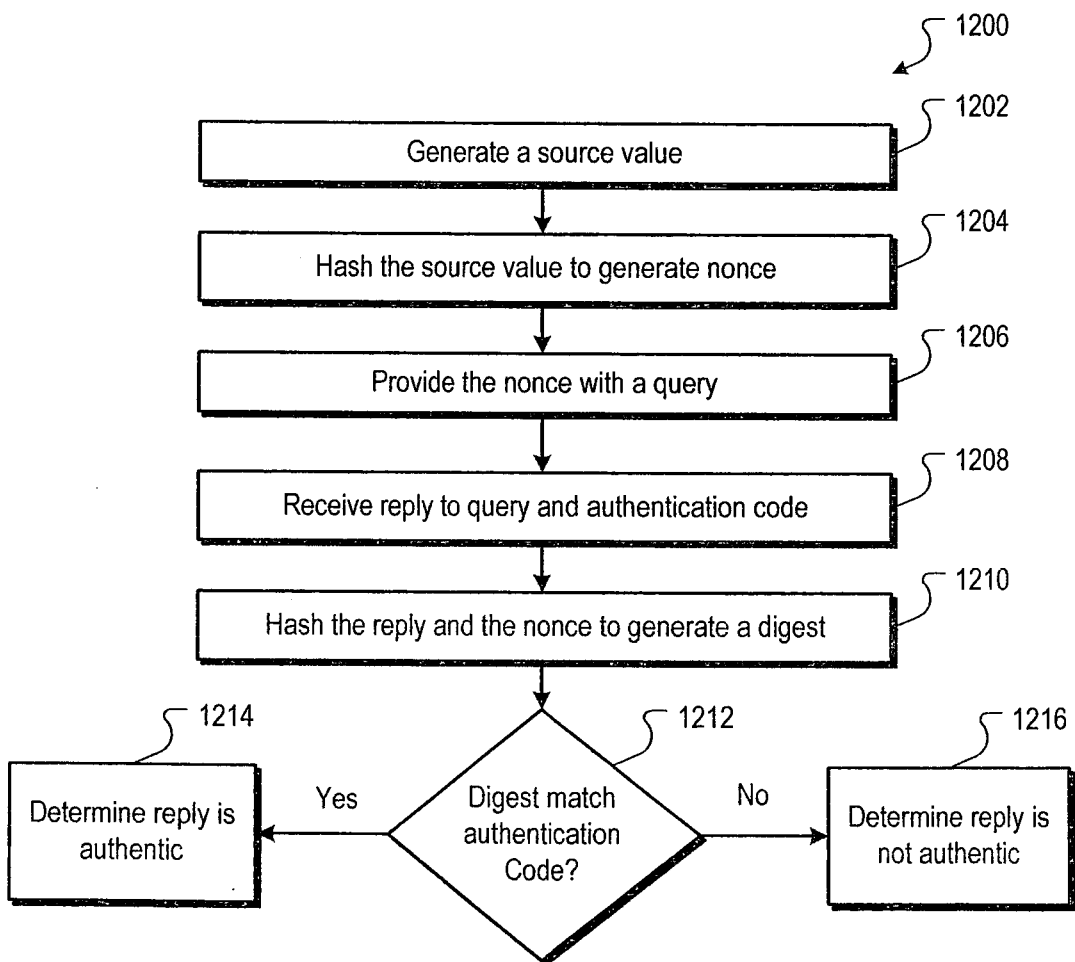


FIG. 12

10 / 10

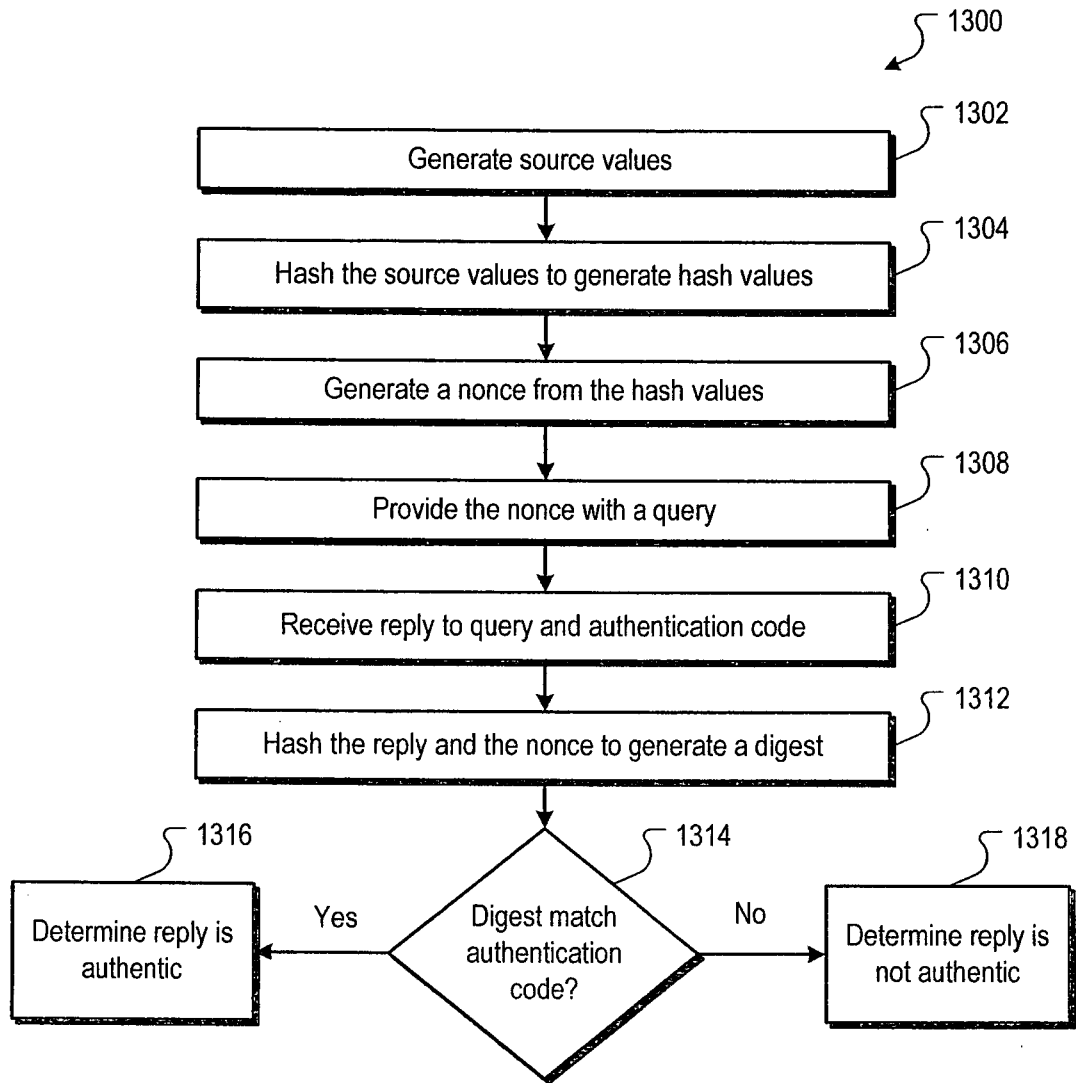


FIG. 13

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IN 09/00486

A. CLASSIFICATION OF SUBJECT MATTER  
IPC(8) - G06F 15/1 6 (201 0.01 )  
USPC - 726/3

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)

IPC(8): G06F 15/16 (2010.01)  
USPC: 726/3

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

IPC(8): G06F 15/16 (2010.01) (Keyword limited - see search terms below)  
USPC: 726/2, 3, 4, 6; 709/223, 224, 225, 227, 229, 250 (Keyword limited - see search terms below)

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

PubWEST (PGPB, USPT, EPAB, JPAB); Google Scholar

Search Terms Used: network management host connect information status address mac ping scan hash access zone quarantine probe detect priority state machine storage etc.

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0210654 A1 (HRASTAR), 21 October 2004 (21.10.2004), entire document, especially para [00201], [0026]-[0027], [0064H0065], [0077], [0079], [0091], [0119]-[0120], [0139], [0186]-[0187], [0190], [0194], [0200]-[0203], [0232]	1-19, 34-56
X	US 2003/0233541 A1 (FOWLER et al.), 18 December 2003 (18.12.2003), entire document, especially para [0013], [0052]-[0053], [0063], [0070]-[0071], [0112], [0114]-[0115], [0118]-[0119], [0121]	20-33
X Y	US 2006/0090023 A1 (OLSEN et al.), 27 April 2006 (27.04.2006), entire document, especially para [0006]-[0007], [0045], [0065]-[0066], [0075]-[0077], [0088]-[0089]	57-60, 64-70, and 74-76 61-63 and 71-73
X	US 2002/0077786 A1 (VOGEL et al.), 20 June 2002 (20.06.2002), entire document, especially para [0029], [0036]-[0037], [0039], [0041], [0049], [0055], [0074], [0083]-[0084], [0087], [0095]	77-103
Y	US 2006/0239254 A1 (SHORT et al.), 26 October 2006 (26.10.2006), entire document, especially para [0062]-[0063], [0066]	61-63 and 71-73

☐ Further documents are listed in the continuation of Box C. ☐

\* 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 January 2010 (29.01.2010)

Date of mailing of the international search report

**16 FEB 2010**

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents  
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774