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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2008 (02.05.2008)

PCT

(10) International Publication Number
WO 2008/052004 A1

(51) International Patent Classification:
H04Q 7/20 (2006.01)

(21) International Application Number:
PCT/US2007/082285

(22) International Filing Date: 23 October 2007 (23.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/862,595 23 October 2006 (23.10.2006) US

(71) Applicant *(for all designated States except US)*: **T-MOBILE USA, INC.** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CALDWELL, Christopher, E.** [US/US]; 18912 NE 168th Street, Woodinville, WA 98072 (US). **LINKOLA, Janne, P.** [FI/FI]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **HASSAN, Omar** [—/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **JENSEN, Chris** [—/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).

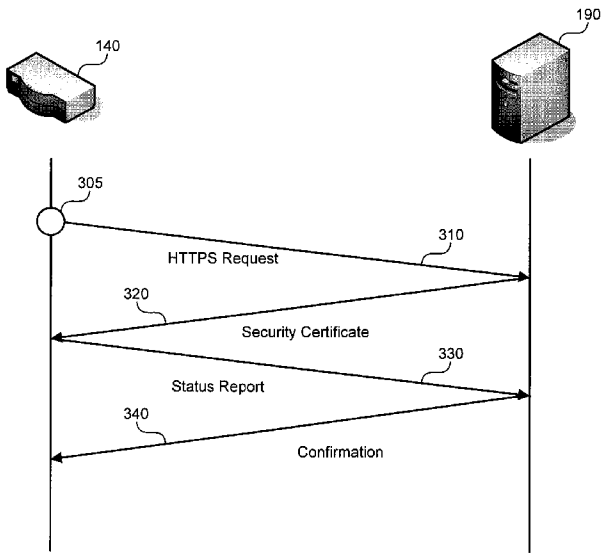
(74) Agents: **ARNETT, Stephen, E.** et al.; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(54) **Title:** SYSTEM AND METHOD FOR MANAGING ACCESS POINT FUNCTIONALITY AND CONFIGURATION



(57) **Abstract:** A system for managing access point functionally and configuration includes a server that is coupled to a computer network and configured to communicate with an access point via the computer network. The access point is configured to couple a mobile device to the computer network by providing a wireless link between the mobile device and the access point. The access point is further configured to produce a status point regarding the access point and the server is configured to receive the status report from the access point following a trigger event at the access point. In other examples, the server is further configured to transmit a response message and/or a configuration file to the access point in response to the status report that is received at the server. Other features and systems are also disclosed.

WO 2008/052004 A1

SYSTEM AND METHOD FOR MANAGING ACCESS POINT FUNCTIONALITY AND CONFIGURATION

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims priority to U.S. Provisional Patent Application No. 60/862,595, filed October 23, 2006, which is hereby incorporated by reference.

BACKGROUND

[0002] In this digital age, modern telecommunication service providers and device manufacturers are increasingly relying on public and/or private IP networks, including the Internet, as a core part of their technology. For example, many telecommunications service providers now offer a suite of Voice over IP ("VoIP") services, as well as various data services, that utilize IP networks and/or IP-based wireless access networks (e.g., access networks based on IEEE 802.16 ("WiMAX"), IEEE 802.20 Mobile Broadband Wireless Access (MBWA), Ultra Wideband (UWB), 802.11 wireless fidelity ("Wi-Fi"), Bluetooth, and similar standards) for at least part of their infrastructure. Likewise, device manufacturers are producing the next generation of mobile devices (e.g. wireless handhelds, wireless handsets, mobile phones, personal digital assistances, notebook computers, and similar devices) that are enabled to send and receive information utilizing IP-based telecommunications services. In fact, many of today's modern mobile devices are able to function as "dual-mode devices" that take advantage of both cellular network technologies and IP-based technologies.

[0003] Unlicensed Mobile Access (UMA) technology has developed as part of this trend to incorporate IP solutions into mobile device telecommunication systems. UMA technology has recently been accepted into Release 6 of the 3rd Generation Partnership Project (3GPP) and is also referred to as Generic Access Network (GAN) technology. In various implementation schemes, UMA allows wireless service providers to merge cellular networks, such as Global System for Mobile Communications (GSM) networks and IP-based wireless networks into one seamless service (with one mobile device, one user interface, and a common set of

network services for both voice and data). One goal of UMA is to allow subscribers to move transparently between cellular networks and IP-based wireless networks with seamless voice and data session continuity, much like they can transparently move between cells within the cellular network. Seamless in-call handover between the IP-based wireless network and the cellular network ensures that the user's location and mobility do not affect the services delivered to the user.

[0004] At an operational level, UMA technology effectively creates a parallel radio access network, the UMA network, which interfaces to the mobile core network using standard mobility-enabled interfaces. For example, UMA can replace a system's GSM radio technology on the lower protocol layers with a wireless LAN, or similar technology. A call or other communication may be tunneled to the Mobile Switching Center (MSC) of a mobile service provider via an access point (e.g., a WiFi access point connected to a modem via the Internet) and gateway (e.g., a UMA network controller). In many cases, the mobile core network remains unchanged, making it much easier to maintain full service and operational transparency and allowing other aspects of the service infrastructure to remain in place. For example, in many systems that utilize UMA, the existing service provider's business support systems (BSS), service delivery systems, content services, regulatory compliance systems, and operation support systems (OSS) can support the UMA network without change. Likewise, service enhancements and technology evolution of the mobile core network apply transparently to both cellular access and UMA.

[0005] As the incorporation of IP solutions, such as UMA, into mobile device telecommunication systems expands, wireless service providers and wireless users may face various obstacles. One challenge involves properly configuring or troubleshooting access points as they are deployed or when they are operating in the field. For example, as the number of access points deployed in the field grows, a larger number of access points may need periodic servicing, including changing or updating the configuration of individual access points. Because of the larger number of access points that may need support, service support may become increasingly difficult to provide.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Figure 1 illustrates aspects of a sample network system that allows VoIP-based communications in conjunction with a public switched telephone network (PSTN).

[0007] Figure 2 illustrates an example converged wireless network system that combines a cellular network with an IP-based wireless telecommunications network.

[0008] Figure 3 is a block diagram illustrating an example access point for use in the system of Figure 1 or the system of Figure 2.

[0009] Figure 4 is a communication diagram illustrating an example of an access point uploading configuration information to a server.

[0010] Figure 5 is a communication diagram illustrating an example of an access point receiving a new configuration from a server.

[0011] Figure 6 is a communication diagram illustrating an example of an access point receiving a firmware update.

DETAILED DESCRIPTION

[0012] The following description provides specific details for a thorough understanding of, and enabling description for, various embodiments of the technology. One skilled in the art will understand that the technology may be practiced without these details. In some instances, well-known structures and functions have not been shown or described in detail to avoid unnecessarily obscuring the description of the embodiments of the technology. It is intended that the terminology used in the description presented below be interpreted in its broadest reasonable manner, even though it is being used in conjunction with a detailed description of certain embodiments of the technology. Although certain terms may be emphasized below, any terminology intended to be interpreted in any restricted manner will be overtly and specifically defined as such in this Detailed Description section.

I. Sample Network Configurations

[0013] Figures 1 and 2 show sample network system configurations in which aspects of an access point can be implemented in accordance with various embodiments. In general, one aspect of the aspect point is that it can automatically produce a status report and upload a status report when it is triggered to do so. For example, such a status report can be uploaded to an upstream server, providing configuration information regarding the access point to customer support personnel. This information, in turn, can be used to manage the configuration and or functionality of the access point.

[0014] Figure 1 illustrates aspects of a sample network system 100 that allows VoIP-based communications in conjunction with a public switched telephone network (PSTN) 102. The system 100 includes at least one wireless access point 104. The access point 104 may be public or private, and may be located, for example, in a subscriber's residence (e.g., home, apartment or other residence), in a public location (e.g., coffee shops, retail stores, libraries, or schools) or in corporate or other private locations. In the sample system of Figure 1, the access point 104 can accept communications 106 from at least one suitably configured mobile device 108 (e.g., a VoIP device). Various types of network technology may be involved in communicating between the mobile device 108 and the access point 104. While "WiFi" is used herein as an example, mobile devices and access points may employ any type of non-cellular wireless protocol, including wireless local, wide, and metropolitan area network (WLAN, WWAN, WMAN, respectively) access protocols. For example, wireless protocols can include IEEE 802.16 (WiMAX), IEEE 802.20 Mobile Broadband Wireless Access (MBWA), Ultra Wideband (UWB), 802.11 wireless fidelity (Wi-Fi), Bluetooth standards, or other similar standards. The access point 104 can include a wireless router 110 and a broadband modem 112 that enable connection to an Internet Protocol (IP) network 114 (described in more detail with respect to Figure 3). The IP network 114 may comprise one or more public networks, private networks, or combination of public and private networks.

[0015] In a communication or set of communications 106, the access point 104 receives IP packets from the mobile device 108. These IP packets are then transported through the IP network 114 to a signaling gateway 116, which in the example of Figure 1, is operated by a telecommunications service provider. At the

signaling gateway 116, the IP packets are converted to a traditional phone service signal. The phone service signal is then conveyed to a recipient via the PSTN 102.

[0016] The network system 100 of Figure 1 also includes a call controller 118 that provides call logic and call control functions for communications sent through the system and servers 120 for providing one or more applications or services offered by the telecommunication provider. For example, individual servers 120 include application servers that provide logic and execution of one or more applications. In accordance with many embodiments described below, the servers 120 also include one or more support servers, which allow customer support service to receive communications from the access point 104.

[0017] Figure 2 illustrates a sample network system 200 in which aspects of the access point management can be implemented within a cellular telephone-type network. In general, with respect to the network system described in Figure 2, because the same cellular protocols are used in communications involving IP access points as with traditional radio towers, the cellular service provider maintains a large degree of system compatibility even though using an IP-based network. For example, the various systems of the cellular service provider that deliver content and handle mobility may not even need to be aware that a subscriber's mobile device is on an IP-based wireless telecommunications network. Instead, the various systems of the cellular service provider assume the mobile device is on its native cellular network. The IP network is, therefore, abstracted with respect to the cellular network, regardless of whether the mobile device connects to the cellular network via a base station (e.g., for licensed spectrum access) or a wireless access point (e.g., for licensed, semilicensed and/or unlicensed spectrum access—such as spectrums for IP-based telecommunications). Likewise, at a protocol level, because the same cellular protocols are used in communications involving the IP access points as with traditional radio towers, the cellular service provider maintains a large degree of system compatibility even though using an IP-based network.

[0018] Referring to Figure 2, a sample network system 200 combines a cellular telephone network 202 (such as a GSM network) and an IP network 204 in a UMA-type configuration that provides service to the user of a mobile device 206. Such service may include voice services, and also supplementary services like call forwarding and call waiting, text messaging services (e.g., SMS) and data-based

services like ring tone downloads, game downloads, picture messaging, email and web browsing. In addition to these services, and in particular, the network system also includes one or more support servers 207 for receiving configuration data from one or more access points (coupled to the IP network 204). Embodiments of the support server 207 and communication between support servers and access points are described in more detail with reference to Figures 4-6. Further, it will be appreciated that since the mobile device 206 is connected to an IP network, all manner of data services available over such networks may be provided to the mobile device 206.

[0019] In general, the described network system 200 accepts registration requests and communication connections from the mobile device 206. The accepted registration requests can be requests to either the cellular telephone network 202 or to the IP-based network 204. Accordingly, to handle requests to the cellular telephone network 202, the cellular telephone network 202 includes one or more cell towers 208 that are configured to accept cellular communications 210 from the mobile device 206. The cell towers 208 are connected to a base station controller 212 (such as a base station controller/radio network controller (BSC/RNC)) via a private network 214. The private network 214 can include a variety of connections (not shown) such as T1 lines, a wide area network (WAN), a local area network (LAN), various network switches, and other similar components.

[0020] The base station controller 212 controls communication traffic to a carrier core network 216, where all communications are managed (including both cellular and IP-based). Components of the carrier core network 216 in this example include a switch (e.g., a mobile switching center or MSC) 218, which is configured to control data/call flows and perform load balancing, as well as other functions. The carrier core network 216 may also include a variety of system databases such as an operation support subsystem (OSS) database 220, a business support system (BSS) database 222, and home location register (HLR) 224 or other central subscriber database that contains details of a carrier's subscribers for billing, call logging, etc.

[0021] The sample network system 200 of Figure 2 further includes one or more access points 226 that can accept IP-based communications 228 from the mobile device 206. For example, each access point 226 can be configured as part

of a wireless network in one or more locations such as a public network 230, a home network 232, or a private business network 234. Each access point 226 is coupled to the IP network 204 through, for example, a broadband connection (not shown) such as a DSL (Digital Subscriber Line) modem, a cable modem, a satellite modem, or any other broadband device.

[0022] When the mobile device 206 attempts to access the IP network 204 (i.e., to initiate an IP-based communication), information (e.g., data, voice, SMS, etc.) is initially formatted in the cellular system's 202 native protocol and then encapsulated into Internet Protocol (IP) packets, which are transmitted to the access point 226 and routed through the IP network 204 to a security gateway 236. In contrast to non-IP communication requests, such transmissions bypass the cellular telephone system's 202 existing network of radio towers. The security gateway 236 controls access to a network controller 238, which communicates with a data store 240 for logging and accessing communications data. Thus, one function of the network controller 238 is to manage access to the carrier network 216 when dealing with an IP-based communication (in a similar manner to that performed by the base station controller 212 for a non-IP-based communication).

[0023] In one example, authentication of a request for access by the mobile device 206 over the IP network 204 is handled by the security gateway 236, which communicates with an authentication, access and authorization (AAA) module 240 that is most likely associated with the carrier network 216. Challenges and responses to requests for access by the mobile device 206 are communicated between the HLR 224 and the AAA module 242. When authorization is granted, the security gateway 236 communicates the assignment of an IP address to the mobile device 206 that requested access. Once the security gateway 236 passes the IP address to the mobile device 206, the public IP address assigned to the mobile device 206 is passed to the network controller 238.

[0024] In another authorization example, upon receiving an identifier from the mobile device 206, the network controller 238 may query the data store 242 to determine if the mobile device 206 is authorized for accessing the IP network 204. Sample identifiers that may be utilized to determine access include a media access control (MAC) address associated with an access point, a mobile device or subscriber identifier (such as an International Mobile Subscriber Identifier (IMSI)), an

Internet Protocol (IP) address (or "Public IP address") associated with the access point, a fully qualified domain name (FQDN), or other similar types of information. The data store 242 may be a single database, table, or list, or a combination of databases, tables, or lists, such as one for IP addresses 244, one of MAC addresses 246, and one for FQDNs 248. The data store 242 may include "blocked" identifiers as well as "authorized" identifiers. Authorized accesses to the IP-based wireless telecommunications network may be maintained by the network controller 238 in an authorized session table or similar data construct.

[0025] In some cases, the signaling portion of a communication (e.g., the portion of the communication that governs various overhead aspects of the communication such as, for example, when the call starts, when the call stops, initiating a telephone ring, etc.) is routed through the network controller 238 to the switch 218, while the voice bearer portion of the communication (e.g., the portion of the communication that contains the actual content (either data or voice information) of the communication) is routed through the network controller 238 to a media gateway 250. In other words, the media gateway 250 controls the content flow between the service provider and the mobile device 206, while the switch 218 controls the signaling flow (or controls overhead-related flow) between the service provider and the mobile device 216.

II. Managing Access Point Functionality and Configuration

[0026] Customers of a wireless service provider often do not know much about the technology that they are using. In particular, customers who own or operate an access point do not know much about its operation and accordingly cannot give service support representatives accurate information regarding their access point. For example, a customer who is not computer literate may be unable to make necessary configuration changes to his or her access point even with the guidance of a technician. Alternatively, many computer-literate customers can make changes to their access points, but few, if any, keep records of changes they make, making it difficult for a customer to remember what has changed in order to narrow the search for the cause of an issue resulting from one of their changes. Further, an access point provider may, on occasion, wish to update the functionality of the access points it has provided. For example, a hacker may have discovered a security flaw or the provider may simply desire to release new features to access point owners.

Changing access point functionality often requires the application of an update. Customers may not apply these updates due to lack of time or interest, or may not be knowledgeable enough about access points that they feel comfortable deploying an update to their access point. Either of these situations could leave a customer's access point vulnerable to hostile attacks that can cause serious problems.

[0027] In contrast to conventional access points, aspects of individual access points 104 (Figure 1) and access point 226 (Figure 2) can be managed remotely, for example, by a customer service representative. In one example, the access point can automatically produce a status report and can upload the status report to one or more servers. The servers, in turn, may be coupled to a computer associated with a customer support service, which allows a customer support representative to retrieve this data and accordingly use it to troubleshoot or configure a customer's access point. As will be described in more detail below, such a status report can have other implementations.

A. Representative Access Point

[0028] Figure 3 is a block diagram that illustrates an access point 300 in which one or more examples of access point management may be implemented. The access point 300 includes one or more CPUs 302 (e.g., a processor), an input/output component 304, a wireless telecommunication component 306, and a memory 308. The CPU 302 can coordinate communications between the input/output component 304, the wireless telecommunication component 306, and the memory 308. The CPU 302 can also execute processing instructions (stored at the memory 308) for producing one or more status reports 310 regarding the access point and for triggering the uploading of such a status report to a server, such as the servers 120 (Figure 1) or servers 207 (Figure 2). For example, the memory 308 may store a resource locator or URL 312 corresponding to an IP address of the server. The input/output component 304 can include, for example, one or more data ports (e.g., 8P8C Ethernet jacks, RJ11 jacks, etc.) as well as keypads and LED and/or LCD displays.

[0029] In operation, the access point 300 serves as a communication link between mobile devices connected to the wireless telecommunication component 306 and a computer network coupled to the input/output component 304. In some

embodiments, such a communication link includes a non-cellular (or WiFi) wireless link. In other embodiments, the communication link includes a cellular wireless link that is established at an access point (and not a cell tower). For example, the access point 300 can include an IP-enabled femtocell or other type of consumer premises equipment (CPE). The status report 310, accordingly, pertains to information regarding the communication link between the mobile devices and the computer network. It will be appreciated that in other examples, other components may be added to or omitted from the access point 300, and a status report may reflect such an addition or omission. For example, an access point may also be integrated with a broadband modem (see, e.g., Figure 1) and the status report may also include information regarding network conditions downstream from the broadband modem.

B. Triggering Events

[0030] Figure 4 is a communication diagram that illustrates the exchange of messages when the access point 300 uploads status reports to a server 400, such as the servers 120 (Figure 1) or servers 207 (Figure 2). These status reports, for example, may be used by a service provider or customer care center to diagnose a problem with the access point, to determine whether the access point requires a configuration change, or for other reasons/uses by the service provider, manufacturer, or third party. The communication flow begins when a trigger event 405 occurs on an access point 300. The trigger event may be operator-initiated, such as when a user reboots the access point or the operator transmits/issues a command to the access point. For example, a status report may be sent to the server 400 upon rebooting the access point 300 and the access point may accordingly receive configuration data from the server 400 in response to the transmission of such a status report (e.g., in the form of a configuration file, described further with reference to Figure 5). Further, the user may have the option to toggle whether the status report is automatically generated and transmitted upon boot-up (e.g., via the I/O component 304). For example, in some instances it may be preferable to not perform a "bootupdump" of such a status report every time the access point is rebooted.

[0031] Alternatively, the access point may automatically or semi-automatically initiate the upload of a status report based on the occurrence of other types of

trigger events, such as when the access point detects a conflict on its communication channel, when congestion occurs at the access point, when the access point detects that a certain interval has passed since the last time it uploaded a configuration, when an alarm condition occurs, or when any other condition chosen by the access point manufacturer or service provider is satisfied. Further, under some circumstances, the service provider or someone operating on behalf of the service provider may remotely initiate the upload of a status report.

[0032] Once the trigger event 405 occurs, a secure connection is negotiated between the access point 300 and the server 400. For example, the access point 300 can retrieve the URL 312 (Figure 3) that is stored in the access point. The access point can accordingly use DNS to request an IP address for the server to which the URL 312 points. If the access point obtains an IP address, it makes a request 410 of server 400 using the obtained IP address via a network protocol, such as HTTPS. If the server 400 does not respond to the request 410, the access point 300 may log this event internally and cease further processing, or it may retry the request after an arbitrary interval. In the example pictured in Figure 4, the access point 300 is requesting a secure sockets layer (SSL) connection with the server 400, but one skilled in the art will appreciate other ways to connect to the server may be used. The server 400 receives the request and sends a response 420 that includes a server security certificate. The access point 300 confirms that the security certificate offered by the server 400 is valid and it is associated with a trusted root certificate. If confirmed, the access point 300 transmits a status report to the server in a response 430. As an additional level of security, in the response 420 the server 300 may include a request for the access point's client security certificate. If requested, the access point 300 would need to provide a security certificate that is valid in a subsequent response in order for the status report to be deemed reliable. The server 400 may validate the access point's client certificate by confirming that it is associated with a trusted root certificate, and/or by checking the certificate against a database of access point registrations to confirm that the access point 300 has authorization to communicate with the server 400.

C. Status Reports

[0033] The status report may contain information about the configuration, settings, status, and other information about the access point, including the communication link provided by the access point. For example, the status report may contain information such as the number of mobile devices that are connected to the wireless telecommunication side of an access point (including over a period of time), the number of populated/unpopulated 8P8C/RJ-11/RJ-45 jacks at the access point, the number of devices that have attempted to connect to the access point, and the number of such attempts which have been successful/unsuccessful. This information may also include connection and lease times associated with mobile devices, IP and MAC addresses of these devices, and the types of applications that have been historically run by such devices. Other information can include other access points or wireless telecommunication networks neighboring the access point, the signal strengths of these access points, the number of available channels at these access points, whether these access points (or networks) are locked, the type of stations that are connected to adjacent access points or networks, as well as the call history (i.e., to customer service) associated with these and other access points. Further, status reports can provide link or signal quality indicators associated with specific connections, intervals, etc.

[0034] Status reports may also be user-configured, for example, allowing a customer to select which type of information is contained in a status report and ultimately communicated to the server. Further, status reports may be communicated (from the server) to various other components, including the HLR.

[0035] In general, the server 400 stores the status report received from the access point in a database (not shown) so that it may be accessed in the future. The information stored in the database may include the identity of the access point providing the status report, the date and time that the status report was generated, and the contents of the status report. Below is a representative status report that may be transmitted to a server from an access point in an XML format. One skilled in the art will appreciate that the content, format, and organization of the status report could be varied significantly from that shown below without affecting the functionality described herein.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<STATUS_REPORT xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:noNamespaceSchemaLocation="vendorname_status_report_version.xsd">
<IDENTIFICATION>
        <RF_MAC_ADDRESS>12-34-56-AB-CD-EF</RF_MAC_ADDRESS>
        <WAN_MAC_ADDRESS>12-34-56-AB-CD-EF</WAN_MAC_ADDRESS>
        <HW_MODEL_NUMBER> T-MOBILE AP NAME</HW_MODEL_NUMBER>
        <HW_VERSION_NUMBER>A1/B1/C1/etc...</HW_VERSION_NUMBER>
<FIRMWARE_VERSION_NUMBER>4.0B6...etc</FIRMWARE_VERSION_NUMBER>
    <CERTIFICATE_ID_NUMBER>xxxxxxxxxxxx</CERTIFICATE_ID_NUMBER>
        <VENDOR_NAME>AP VENDOR PARTNER NAME</VENDOR_NAME>
</IDENTIFICATION>

<CONFIGURATION>
    <WAN_SETTINGS>
        <DHCP_STATUS>ENABLED</DHCP_STATUS>
        <IP_ADDRESS>64.36.112.252</IP_ADDRESS>
<IP_SUBNET_MASK>255.255.255.0</IP_SUBNET_MASK>
<DEFAULT_GATEWAY>64.36.112.1</DEFAULT_GATEWAY>
<DNS_SERVER_PRIMARY>127.0.0.1</DNS_SERVER_PRIMARY>
                        <DNS_SERVER_SECONDARY>127.0.0.1</DNS_SERVER_SECONDARY>
  </WAN_SETTINGS>

  <LAN_SETTINGS>
        <DHCP_SERVER>ENABLED</DHCP_SERVER>
        <FIREWALL_OPTIONS>ON/OFF</FIREWALL_OPTIONS>
        <NAT_SETTINGS>ON/OFF</NAT_SETTINGS>
        <BRIDGE_MODE>ON</BRIDGE_MODE>
        <PORT_FORWARDING>T237, U238, T817</PORT_FORWARDING>
  </LAN_SETTINGS>
  <WLAN_SETTINGS>
        <SSID> myhome</SSID>
        <OPERATING_MODE>AUTO</OPERATING_MODE>
<COUNTRY>ALL</COUNTRY>
<DEFAULT_CHANNEL>6</DEFAULT_CHANNEL>
<BEACON_INTERVAL>100</BEACON_INTERVAL>
<RTS_THRESHOLD>2346</RTS_THRESHOLD>
<FRAGMENTATION_LENGTH>2346</FRAGMENTATION_LENGTH>
<DTIM_INTERVAL>1(1:255)</DTIM_INTERVAL>
<PREAMBLE_TYPE>LONG</PREAMBLE_TYPE>
<HIDE_NETWORK_NAME>DISABLED</HIDE_NETWORK_NAME>
<TX_POWER>100%</TX_POWER>
<ANTENNA_TYPE>PRIMARY</ANTENNA_TYPE>
<WIRELESS_RADIO>ON</WIRELESS_RADIO>

        <WIRELESS_QOS_WMM>ON</WIRELESS_QOS_WMM>
        <CTS>ON</CTS>
</WLAN_SETTINGS>

<SECURITY_SETTINGS>
     <AUTHENTICATION_TYPE>OPEN/WEP/WPA/WPA-PSK/WPA2/WPA2-
PSK</AUTHENTICATION_TYPE>
  </SECURITY_SETTINGS>

</CONFIGURATION>


<STATUS>
    <WLAN_STATUS>
   <!-- FOR EACH STATION THE FOLLOWING INFO CAN BE REQUIRED -->
```

```
        <MAC_ADDRESS>01-23-45-67-89-ab</MAC_ADDRESS>
        <CURRENT_NOISE_LEVEL>-xxdBm</CURRENT_NOISE_LEVEL>
        <POWER_SAVE_MODE>NORMAL</POWER_SAVE_MODE>
        <ASSOCIATION_MODE>11G</ASSOCIATION_MODE>
        <TRAFFIC_COUNTER>tx=123 rx=321</TRAFFIC_COUNTER>
        <DHCP_LEASE>IP_ADDRESS_MAC_ADDRESS_LEASE_TIME??</DHCP_LEASE>
        <UPTIME>???</UPTIME>
</WLAN_STATUS>

<LAN_STATUS>
        <LAN_PORT1>
                <LINK_STATUS>100</LINK_STATUS>
                <TRAFFIC_COUNTER> tx=123 rx=321</TRAFFIC_COUNTER>
        </LAN_PORT1>

        <LAN_PORT2>
                <LINK_STATUS>100</LINK_STATUS>
                <TRAFFIC_COUNTER> tx=123 rx=321</TRAFFIC_COUNTER>
        </LAN_PORT2>

        <LAN_PORT3>
                <LINK_STATUS>100</LINK_STATUS>
                <TRAFFIC_COUNTER> tx=123 rx=321</TRAFFIC_COUNTER>
        </LAN_PORT3>


        <LAN_PORT4>
                <LINK_STATUS>100</LINK_STATUS>
                <TRAFFIC_COUNTER> tx=123 rx=321</TRAFFIC_COUNTER>
        </LAN_PORT4>

</LAN_STATUS>

  <WAN_STATUS>
        <LINK_STATUS>100</LINK_STATUS>
  </WAN_STATUS>
</STATUS>

<TEST>
        <PING_DNS_SERVER>IP_ADDRESS #PACKETS_SENT  #PACKETS_RECEIVED MINIMUM
MAXIMUM AVERAGE</PING_DNS_SERVER >

        <PING_DHCP_SERVER>IP_ADDRESS #PACKETS_SENT  #PACKETS_RECEIVED MINIMUM
MAXIMUM AVERAGE</PING_DHCP_SERVER>
        <PING_WAN_GATEWAY>IP_ADDRESS #PACKETS_SENT  #PACKETS_RECEIVED MINIMUM
MAXIMUM AVERAGE</PING_WAN_GATEWAY >
        <PING_TMO_SERVER>IP_ADDRESS #PACKETS_SENT  #PACKETS_RECEIVED MINIMUM
MAXIMUM AVERAGE</PING_TMO_SERVER >
</TEST>

 <DISABLE_STATUS_REPORT>DISABLED</DISABLE_STATUS_REPORT>

<VENDOR_EXTENDED_FEATURES>
<!--This section contains features/parameters that vendor supports and not included in the above
list -->
</VENDOR_EXTENDED_FEATURES>

</STATUS_REPORT>
```

D. Response Messages

[0036] Returning to Figure 4, after processing the request 430, the server 400 replies to the access point with a response 440 acknowledging the receipt of the status report. The response may echo much of the information received in the status report, and otherwise acknowledge the receipt of the status report. Below is a representative response message that may be transmitted from the server to the access point in an XML format. One skilled in the art will appreciate that the content, format, and organization of the response could be varied significantly from that shown below without affecting the functionality described herein. Once the status report has been transmitted to the server and receipt confirmed, no further communication between access point and server may be needed.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<RESPONSE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="vendorname_response_version.xsd">

<IDENTIFICATION>
        <RF_MAC_ADDRESS>12-34-56-AB-CD-EF</RF_MAC_ADDRESS>
        <WAN_MAC_ADDRESS>12-34-56-AB-CD-EF</WAN_MAC_ADDRESS>
        <HW_MODEL_NUMBER> T-MOBILE AP NAME</HW_MODEL_NUMBER>
        <HW_VERSION_NUMBER>A1/B1/C1/etc...</HW_VERSION_NUMBER>
<FIRMWARE_VERSION_NUMBER>4.0B6...etc</FIRMWARE_VERSION_NUMBER>
    <CERTIFICATE_ID_NUMBER>xxxxxxxxxxx</CERTIFICATE_ID_NUMBER>
        <VENDOR_NAME>AP VENDOR PARTNER NAME</VENDOR_NAME>
</IDENTIFICATION>

<CONFIGURATION>
    <WAN_SETTINGS>
        <DHCP_STATUS>ENABLED</DHCP_STATUS>
        <IP_ADDRESS>64.36.112.252</IP_ADDRESS>
<IP_SUBNET_MASK>255.255.255.0</IP_SUBNET_MASK>
<DEFAULT_GATEWAY>64.36.112.1</DEFAULT_GATEWAY>
        <DNS_SERVER_PRIMARY>127.0.0.1</DNS_SERVER_PRIMARY>
        <DNS_SERVER_SECONDARY>127.0.0.1</DNS_SERVER_SECONDARY>
  </WAN_SETTINGS>
  <LAN_SETTINGS>
        <DHCP_SERVER>ENABLED</DHCP_SERVER>
        <FIREWALL_OPTIONS>ON/OFF</FIREWALL_OPTIONS>
        <NAT_SETTINGS>ON/OFF</NAT_SETTINGS>
  </LAN_SETTINGS>
  <WLAN_SETTINGS>
        <SSID> myhome</SSID>
        <OPERATING_MODE>AUTO</OPERATING_MODE>
<COUNTRY>ALL</COUNTRY>
<DEFAULT_CHANNEL>6</DEFAULT_CHANNEL>
<BEACON_INTERVAL>100</BEACON_INTERVAL>
<RTS_THRESHOLD>2346</RTS_THRESHOLD>
<FRAGMENTATION_LENGTH>2346</FRAGMENTATION_LENGTH>
<DTIM_INTERVAL>1(1:255)</DTIM_INTERVAL>
<PREAMBLE_TYPE>LONG</PREAMBLE_TYPE><HIDE_NETWORK_NAME>DISABLED</HIDE_NET
WORK_NAME>
```

```
<TX_POWER>100%</TX_POWER>
<ANTENNA_TYPE>PRIMARY</ANTENNA_TYPE>
<WIRELESS_RADIO>ON</WIRELESS_RADIO>
        <WIRELESS_QOS_WMM>ON</WIRELESS_QOS_WMM>
        <CTS>ON</CTS>
</WLAN_SETTINGS>


<SECURITY_SETTINGS>
    <AUTHENTICATION_TYPE>OPEN/WEP/WPA/WPA-PSK/WPA2/WPA2-
PSK</AUTHENTICATION_TYPE>
 </SECURITY_SETTINGS>


</CONFIGURATION>

<DISABLE_STATUS_REPORT>DISABLED</DISABLE_STATUS_REPORT>


<FIRMWARE_POINTER>
        https://vendorx.firmware.t-mobile.com/firmware.xml
</FIRMWARE_POINTER >
</RESPONSE>
```

E. Service Support

[0037] A service support representative can use a computer coupled to a computer network (e.g., IP network 114 (Figure 1) and IP network 204 (Figure 2)) and the server 400 to retrieve and review status reports submitted by an access point. For example, the support representative may be affiliated with a customer support service provided to customers that operate the access point. Such customers could, for example, communicate with the support representative via a hotline or an online chat room. Using the status report, the customer support representative can provide up-to-date information regarding the access point. For example, the status report information may be used in individual cases to audit changes to the access point configuration over time in order to identify changes that have resulted in a customer problem. If a customer's access point requires a configuration change, the service support representative can connect to a data port of the access point to reconfigure the access point remotely. This can be accomplished either by the customer placing the access point in a remote help mode, or, in some cases, by the user rebooting the access point. For example, rebooting the access point may place the access point in remote help mode for a short period. The stored status report may also be analyzed in light of status reports from other access points, yielding aggregated data corresponding to the behavior of groups of access points. Such aggregated data could be used to identify systemic

improvements that may be made to the operation of the IP-based wireless telecommunications network. For example, an automated software routine may inspect the database to identify potential or actual problems that may result in a design change, a customer contact, or the pursuit of another solution.

F. Configuration Files

[0038] In addition to or in lieu of a response message, a configuration file may be downloaded from the server 400 to the access point 300 in order to add new settings to the access point or to change the existing settings of the access point. Figure 5 is a communication diagram that illustrates the exchange of messages when an access point receives a configuration file from a server. An event 505 triggers the access point 300 to open a secure network channel with the server 400 and send a communication 510 containing a status report from the access point to the server. The server analyzes the status report and determines whether an updated configuration file needs to be sent to the access point via a communication 520. Reasons for sending a configuration file include, but are not limited to, correcting an access point problem, optimizing the performance of the IP-based wireless telecommunications network, de-provisioning customers from the IP-based wireless telecommunications network, responding to a user request, or addressing other service provider, manufacturer, or third party issues. For example, the status report may indicate that a neighboring access point is causing interference or that mobile devices at the access point have conflicting IP addresses. The new configuration file contains one or more new or changed settings that are to be implemented by the access device. The configuration file may be communicated in XML-formatted text that must be accepted by the access point as legitimate. For example, access point 300 may confirm that the XML is well formed, valid, and meets other correctness criteria such as business rules or internal conventions. The access point 300 can determine whether the XML is well formed and valid using a schema that is stored at the access point and other methods known to those skilled in the art.

[0039] Once the configuration file is received by the access point 300, the access point processes the received file and applies the new or changed settings to

its configuration. Adding or changing a setting may trigger the access point to reboot in order to make the settings operational. After applying the settings, the access point sends a communication 530 containing a status report with the access point's settings to the server 400. Sending a status report to the server enables the server to confirm that the settings have been correctly applied. After receiving the status report and verifying that the access point is correctly configured, the server 400 sends a confirmation message 540 to the access point. In several embodiments, the server cannot initiate the transmission of a configuration file, but can only send such a configuration file upon receiving a status report. Alternatively, in other embodiments, the server can only send a configuration file or response when directed to do so by a carrier network (e.g., via an HLR).

G. Disabling/Enabling Status Reporting

[0040] One of the settings that may be sent in a configuration file is a setting that disables the access point from sending a status report to a server when events occur that would normally have triggered the sending a status report. This change to access point behavior occurs when the setting DISABLE_STATUS_REPORT is changed to "OFF" at the access point. When the DISABLE_STATUS_REPORT setting is "OFF" an access point will send status reports to a server only when specifically requested to do so by a user or operator. The user or operator may request the access point to send a status report using a computer that is coupled to the access point 300. The disable status report setting may be particularly useful to a service provider to control the number of status reports that they receive from access points that are within the service provider's network. The service provider is able to thereby selectively determine which groups of access points need to be monitored and control the frequency of access point monitoring.

H. Firmware Upgrading

[0041] On a periodic basis, the firmware of the access point may need to be updated. Updating the firmware may be necessary, for example, to correct a security vulnerability, to correct or improve performance problems at an access point, to add new functionality or to change existing functionality, or to address other service provider, manufacturer, or third party issues. Figure 6 is a communication diagram that illustrates the exchange of messages when an access point receives a

firmware update from the server. The firmware update process reflected in Figure 6 may be similar to the configuration process reflected in Figure 5. An event 605 triggers the access point 300 to open a secure network channel with the server 400 and send a communication 610 containing a status report from the access point to the server. The status report may include the date and version of the firmware on the access point. The server 400 processes the status report and determines whether the access point requires a firmware update. If a firmware update is required, the server includes a "FIRMWARE POINTER" setting in a response 620. The access point identifies the "FIRMWARE POINTER" setting and uses the value of this setting as a URI (uniform resource identifier) to make a request 630 to obtain the firmware update from the server 400 or from another server (not shown). The server processes request 630 and responds by sending a communication 640 containing the firmware update. Upon obtaining the firmware update, the access point processes, validates, and applies the firmware update. The firmware update may optionally require the access point to reboot at an event 650 and, subsequently, reestablish a secure network channel with server 400. A status report is sent by the access point 300 to the server 400 in a communication 660. Sending a status report to the server enables the server to confirm that the new firmware has been correctly installed. After receiving the status report and verifying that the firmware is correctly installed, the server 400 sends a confirmation message 670 to the access point.

[0042] It will be appreciated that although the process described in Figure 6 contemplates that the access point uses a web request to obtain the firmware update, one skilled in the art would appreciate that the access point could use any of a variety of network protocols to download the firmware update. Alternatively, other non-network methods may be used. As an example, request 610 might cause the service provider that manages server 400 to send the firmware update on computer readable medium to the owner of the access point. Upon receiving the computer readable medium, the owner or operator of the access point could apply the firmware update to the access point using a local personal computer.

III. Conclusion

[0043] Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” and the like are to be construed

in an inclusive sense, as opposed to an exclusive or exhaustive sense; that is to say, in the sense of “including, but not limited to.” As used herein, the terms "connected," "coupled," or any variant thereof, means any connection or coupling, either direct or indirect, between two or more elements; the coupling of connection between the elements can be physical, logical, or a combination thereof. Additionally, the words “herein,” “above,” "below," and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. Where the context permits, words in the above Detailed Description using the singular or plural number may also include the plural or singular number respectively. The word "or," in reference to a list of two or more items, covers all of the following interpretations of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

[0044] The above detailed description of embodiments of the system is not intended to be exhaustive or to limit the system to the precise form disclosed above. While specific embodiments of, and examples for, the system are described above for illustrative purposes, various equivalent modifications are possible within the scope of the system, as those skilled in the relevant art will recognize. For example, some network elements are described herein as performing certain functions. Those functions could be performed by other elements in the same or differing networks, which could reduce the number of network elements. Alternatively or additionally, network elements performing those functions could be replaced by two or more elements to perform portions of those functions. In addition, while processes, message/data flows, or blocks are presented in a given order, alternative embodiments may perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes, message/data flows, or blocks may be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed in parallel, or may be performed at different times. Further any specific numbers noted herein are only examples: alternative implementations may employ differing values or ranges. Those skilled in the art will also appreciate that the actual implementation of a database may take a variety of forms, and the term "database" is used herein in

the generic sense to refer to any data structure that allows data to be stored and accessed, such as tables, linked lists, arrays, etc.

[0045] The teachings of the methods and system provided herein can be applied to other systems, not necessarily the system described above. The elements and acts of the various embodiments described above can be combined to provide further embodiments.

[0046] Any patents and applications and other references noted above, including any that may be listed in accompanying filing papers, are incorporated herein by reference. Aspects of the technology can be modified, if necessary, to employ the systems, functions, and concepts of the various references described above to provide yet further embodiments of the technology.

[0047] These and other changes can be made to the invention in light of the above Detailed Description. While the above description describes certain embodiments of the technology, and describes the best mode contemplated, no matter how detailed the above appears in text, the invention can be practiced in many ways. Details of the system may vary considerably in its implementation details, while still being encompassed by the technology disclosed herein. As noted above, particular terminology used when describing certain features or aspects of the technology should not be taken to imply that the terminology is being redefined herein to be restricted to any specific characteristics, features, or aspects of the technology with which that terminology is associated. In general, the terms used in the following claims should not be construed to limit the invention to the specific embodiments disclosed in the specification, unless the above Detailed Description section explicitly defines such terms. Accordingly, the actual scope of the invention encompasses not only the disclosed embodiments, but also all equivalent ways of practicing or implementing the invention under the claims.

[0048] While certain aspects of the technology are presented below in certain claim forms, the inventors contemplate the various aspects of the technology in any number of claim forms. For example, while only one aspect of the invention is recited as embodied in a computer-readable medium, other aspects may likewise be embodied in a computer-readable medium. Accordingly, the inventors reserve the

right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the technology.

CLAIMS

We claim:

1. A system for managing functionality and/or configuration of an access point in communication with a carrier network that manages, at least in part, communication associated with one or more mobile devices, the communication being exchanged over a communication path that includes at least a portion of a computer network, the system comprising:

a server computer coupled to the computer network; and

wherein the server is configured to communicate with the access point via the computer network, wherein the access point is further configured to produce a status report regarding the access point following a trigger event at the access point, and wherein the server is configured to receive the status report from the access point.

2. The system of claim 1 wherein the server is configured to transmit a response message and/or a configuration file to the access point, the response message and/or configuration file being responsive to the status report that is received at the server.

3. The system of claim 1, further comprising one or more customer-care computers coupled to the server via the computer network either directly or through other servers (middleware), the server being configured to transmit the status report to the customer-care computers.

4. The system of claim 1, further comprising a database coupled to the server, the database including the status report communicated to the server and multiple status reports corresponding to other access points coupled to the computer network, wherein the server is configured to automatically review the status reports

and improve a service provided to one or more of the access points based on the review.

5. The system of claim 1 wherein the trigger event is an operator-initiated event including at least one of rebooting the access point, providing an input at the access point, or providing an input at a computer coupled to the access point.

6. The system of claim 1 wherein the trigger event is initiated by a detection event including at least one of a conflict on a radio communication channel of the access point, a level of communication congestion at the access point, an elapsed time period associated with a previously uploaded status report, an alarm condition at the access point, and a predetermined condition chosen by a provider of the access point.

7. The system of claim 1 wherein the access point is configured for coupling the mobile devices to the computer network by providing a non-cellular wireless link between the mobile devices and the access point.

8. The system of claim 1 wherein the access point is configured for coupling the mobile devices to the computer network by providing a cellular wireless link between the mobile devices and the access point, wherein the access point is not a cell tower.

9. A computer-implemented method for operating consumer premises equipment (CPE), the method comprising:

producing a status report regarding the CPE, the status report being initially stored at the CPE;

responsive to a trigger event, automatically transmitting the status report to a server, the server being coupled to the CPE via a computer network;

receiving a configuration file from the server; and

automatically changing the functionality and/or configuration of the CPE based, at least in part, on the configuration file.

10. A method of claim 9 wherein the method provides a communication link between a wireless mobile device and a carrier network associated with the mobile device.

11. The method of claim 9 wherein the status report includes information regarding the status of firmware installed at the CPE, and wherein changing the functionality and/or configuration of the CPE includes receiving and installing updated firmware at the CPE.

12. The method of claim 9 wherein the trigger event includes at least one of a boot-up, a power-up, or an operated-initiated signal.

13. The method of claim 9 wherein changing the functionality and/or configuration of the CPE includes at least temporarily suspending future automatic transmission of status reports from the CPE.

14. The method of claim 9 wherein changing the functionality and/or configuration of the CPE includes changing user-configurable settings remotely via the computer network.

15. The method of claim 9 wherein transmitting the status report to the server includes requesting and setting up a secure socket layer connection with the server.

16. The method of claim 9 wherein transmitting the status report to the server includes certificate based authentication to authenticate both the server and CPE before communicating the status report.

17. The method of claim 9 wherein transmitting the status report to the server includes:

retrieving a URL stored at the CPE; and

transmitting the status report to an IP address associated with the URL and corresponding to the server.

18. The method of claim 9 wherein the CPE includes an access point for establishing a cellular or non-cellular wireless link between the access point and the computer network, wherein the access point is not a cell tower.

19. An access point, comprising:

a wireless communication component;

a data port;

at least one processor; and

a memory, including:

first operating instructions executable by the processor to set up a communication link between at least one wireless mobile device in communication with the WiFi component and a wireless service provider in communication with the data port, the carrier network being associated with the mobile devices;

second operating instructions executable by the processor to automatically generate a status report regarding the access point; and

third operating instructions executable by the processor to automatically communicate the status report to a server that is coupled to the access point through a computer network, wherein the status report is communicated to the server in response to at least one of an automatic initiation at the access point, a user initiation at the access point, or a remote initiation via the computer network.

20. The access point of claim 19 wherein the memory further includes information corresponding to a uniform resource locator (URL) or uniform resource identifier (URI) for the server.

21. The access point of claim 19 wherein the status report includes information corresponding to firmware installed at the access point, and wherein the memory further includes fourth operating instructions executable by the processor to

download and/or install updated firmware based on one or more configuration files that are returned to the access point and based on the status report.

22. The access point of claim 19 wherein the status report includes information regarding the multiple mobile devices, including a number of successful/unsuccessful connection attempts, connection and/or lease times of the mobile devices, and IP and/or MAC addresses of the mobile devices.

23. The access point of claim 19 wherein the status report includes information regarding neighboring access points.

24. A system for changing and/or monitoring the configuration of an access point, the system comprising:

means for receiving a status report regarding the access point at a server, the access point being coupled to the server through a computer network, and

means for using the status report to:

(a) transmit a response message and/or a configuration file to the access point, the response message and/or configuration file being based on the status report, the response message acknowledging receipt of the of the status report, and the configuration file corresponding to an updated configuration of the access point;

(b) transmit the status report to one or more computers coupled to the computer network, the computers being associated with a customer support service; or

(c) both (a) and (b).

25. The system of claim 24, further comprising means for remotely and automatically configuring the access point based on the status report.

26. The system of claim 24, further comprising:

means for determining whether the access point requires a firmware change based on the status report; and

means for automatically providing the firmware change at the access point.

27. The system of claim 24, further comprising means for initiating a triggering event at the access point, the triggering event causing the access point to transmit the status report to the server and including at least one of a request from the server to send the status report, a reboot of the access point, and placing the access point in a remote help mode.

28. A computer-readable storage medium whose contents cause an access point to perform a method for uploading a status report to a server, the access point being in communication with a carrier network that manages, at least in part, communication associated with one or more mobile devices wirelessly coupled to the access point, the method comprising:

automatically generating the status report regarding the access point; and

automatically uploading the status report to a server responsive to a triggering event at the access point.

29. The computer-readable storage medium of claim 28 wherein the method further includes providing an IP-based telecommunication service to the one or more mobile devices.

30. The computer-readable storage medium of claim 28 wherein the method further includes providing an unlicensed mobile access (UMA) service to the one or more mobile devices.

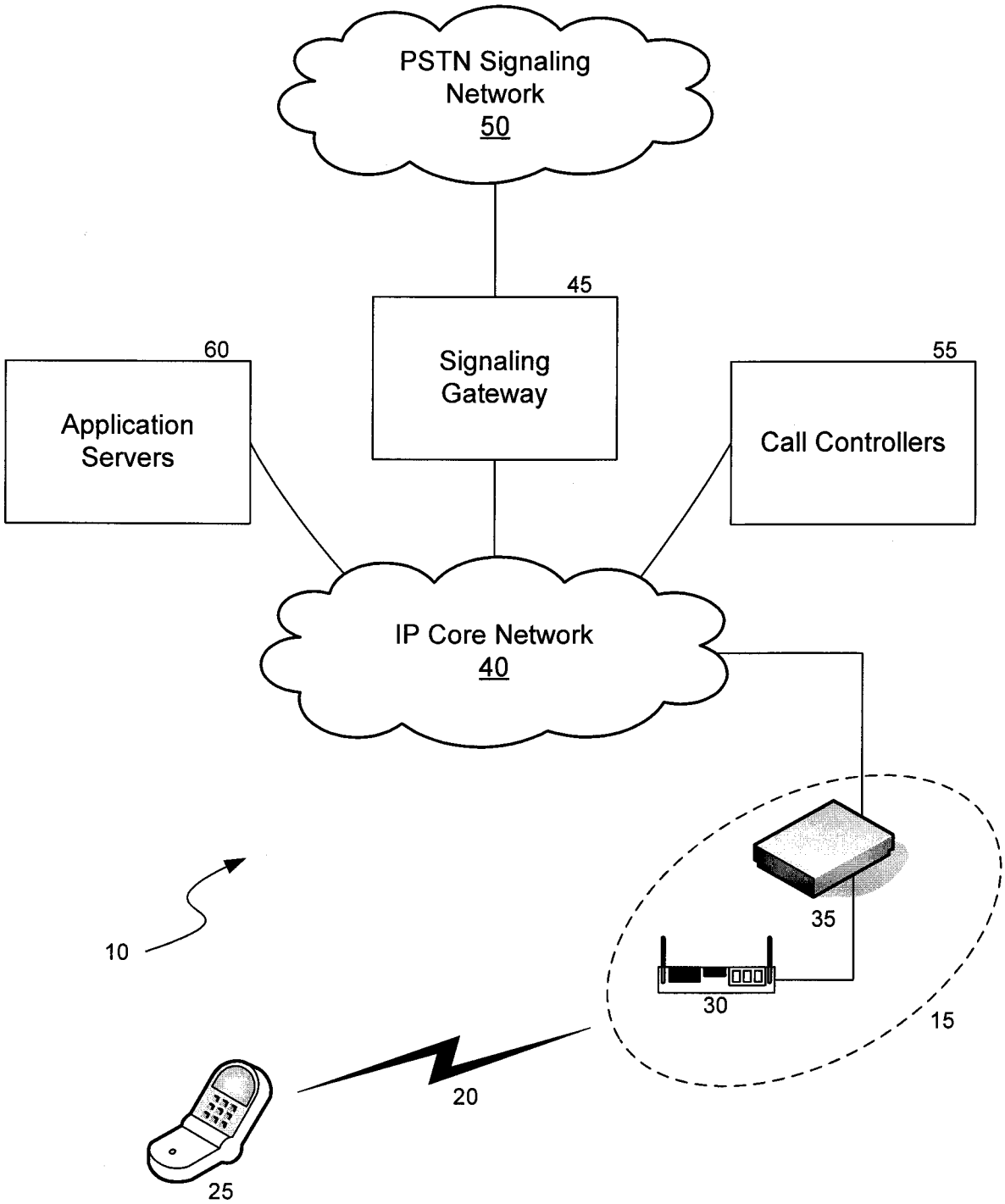

PSTN Signaling Network
50
45
Signaling Gateway
60
Application Servers
55
Call Controllers
IP Core Network
40
35
30
15
10
20
25

FIG. 1

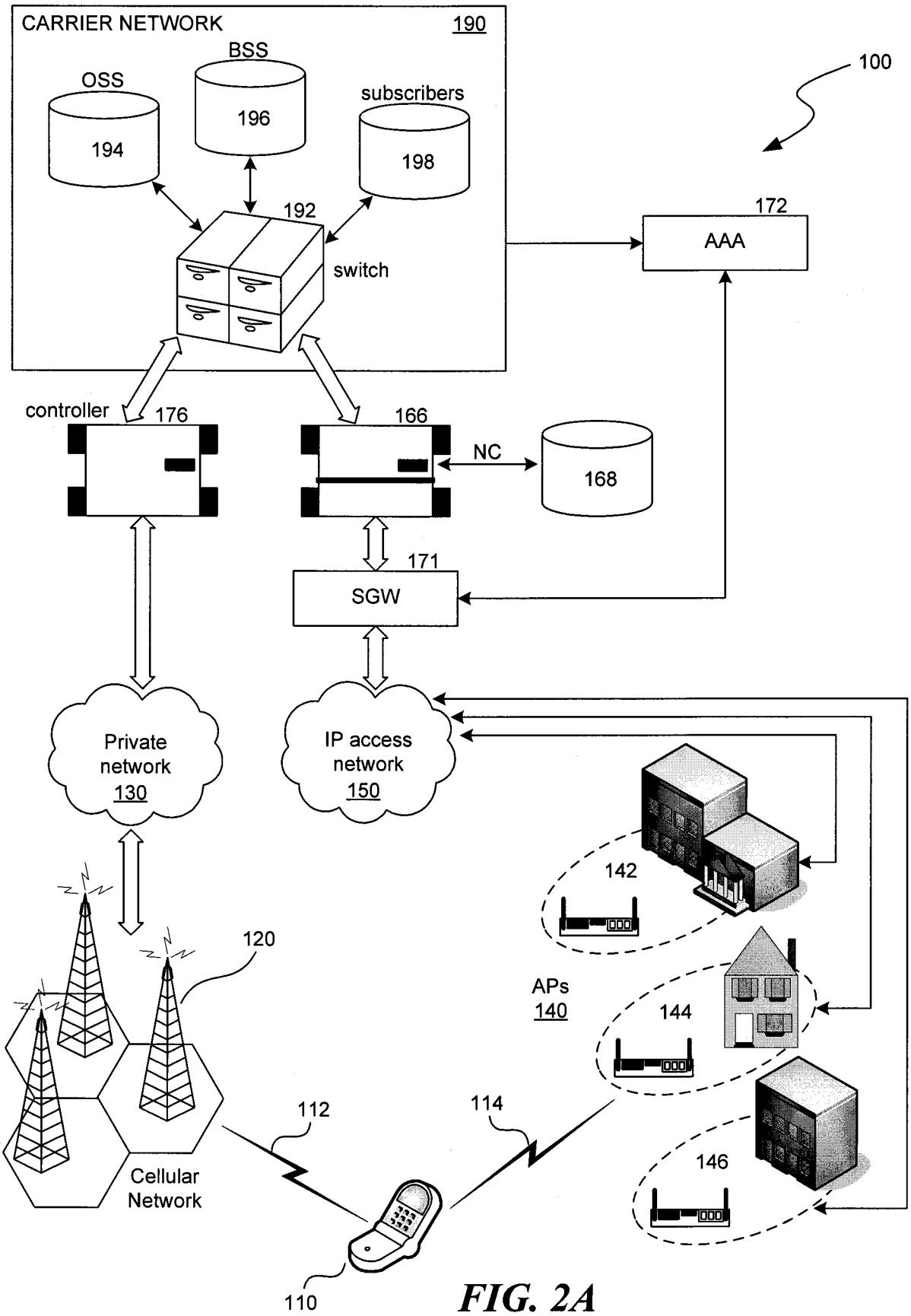

CARRIER NETWORK
190
BSS
196
OSS
194
subscribers
198
192
switch
100
172
AAA
controller
176
166
NC
168
171
SGW
Private network 130
IP access network 150
142
120
APs 140
144
112
114
146
Cellular Network
110

FIG. 2A

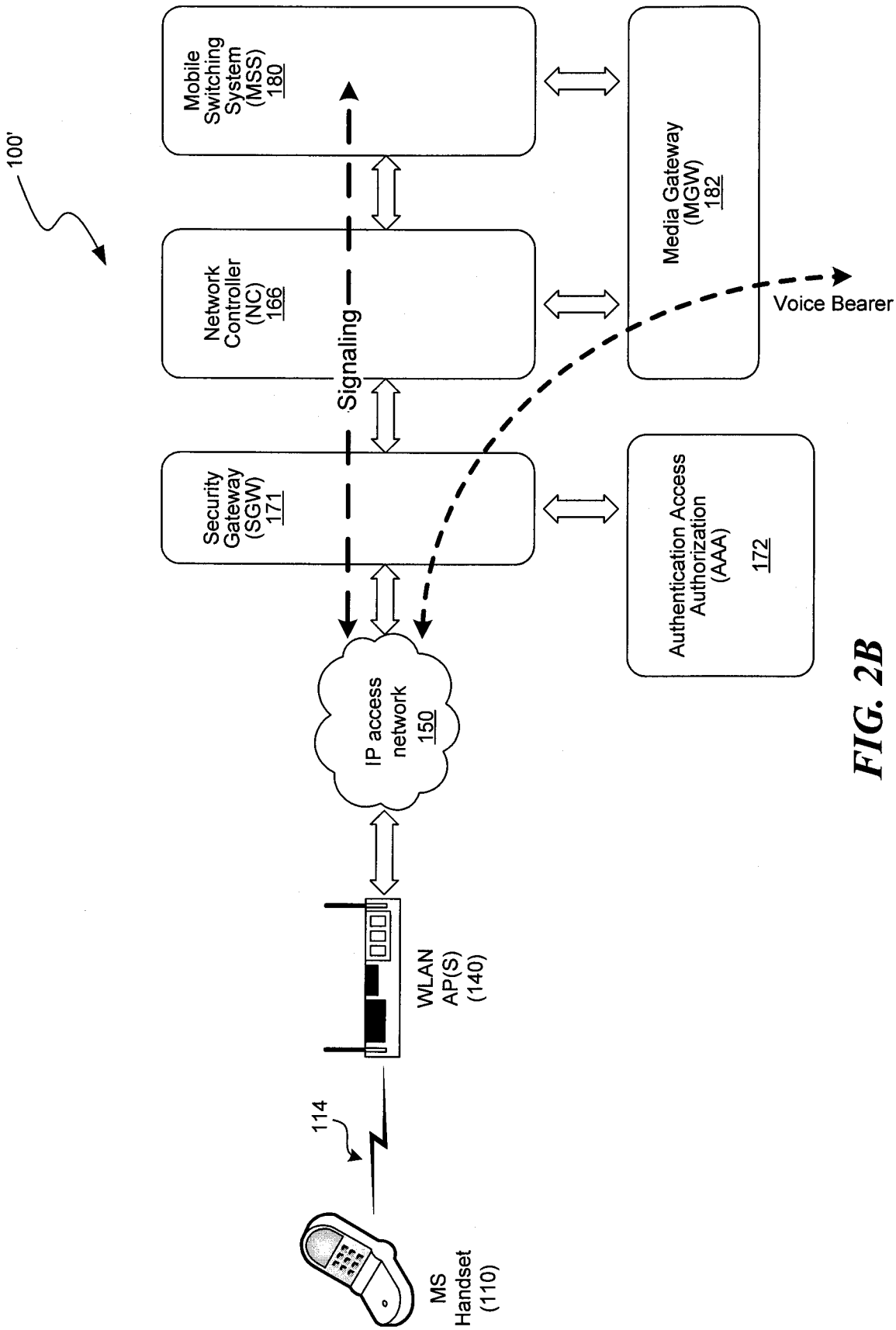

100'
Mobile Switching System (MSS) 180
Network Controller (NC) 166
Security Gateway (SGW) 171
Media Gateway (MGW) 182
Authentication Access Authorization (AAA) 172
Signaling
Voice Bearer
IP access network 150
WLAN AP(S) (140)
114
MS Handset (110)

FIG. 2B

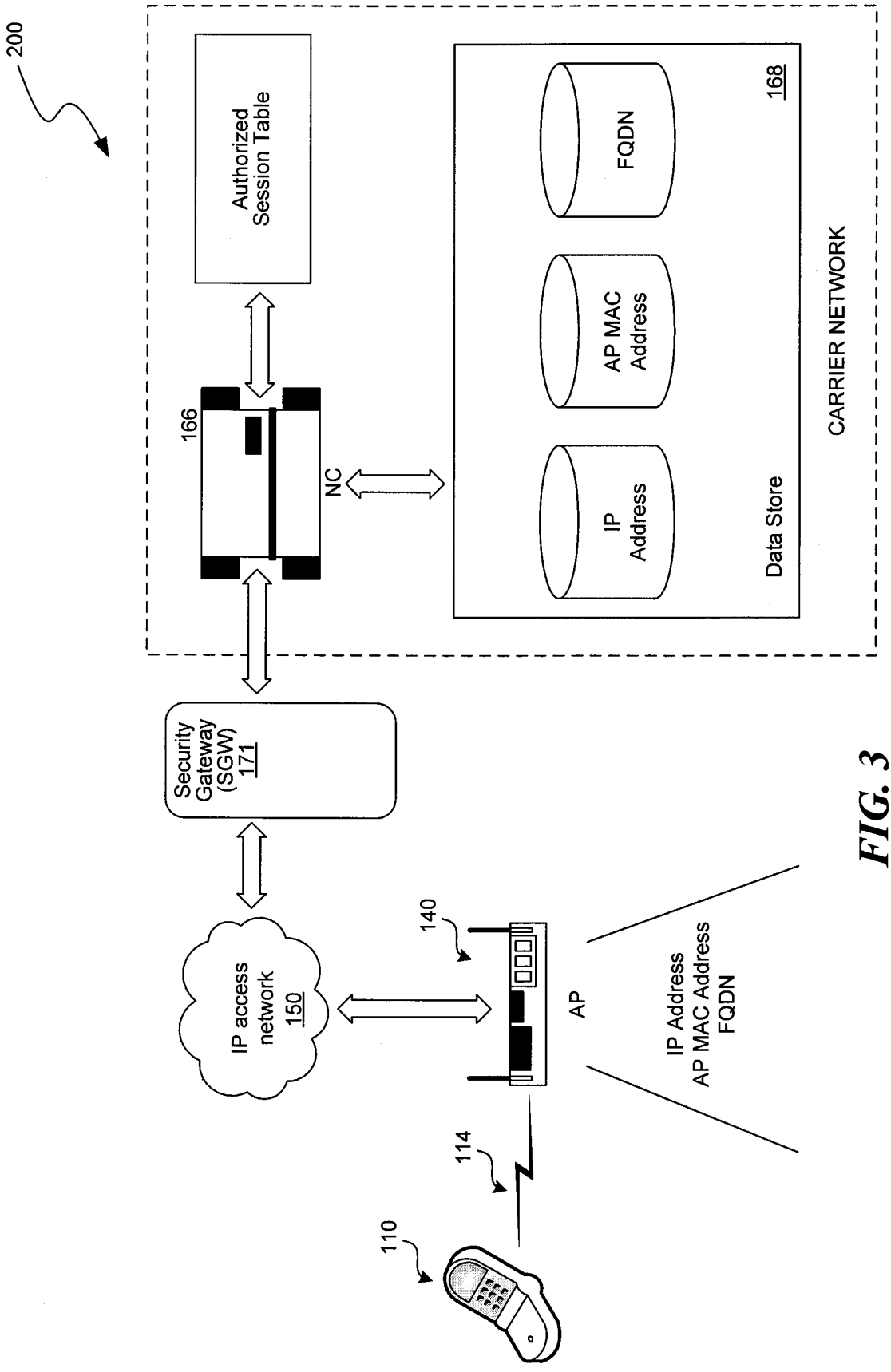

200
Authorized Session Table
166
NC
IP Address
AP MAC Address
FQDN
Data Store
168
CARRIER NETWORK
Security Gateway (SGW) 171
IP access network 150
140
AP
IP Address
AP MAC Address
FQDN
114
110

FIG. 3

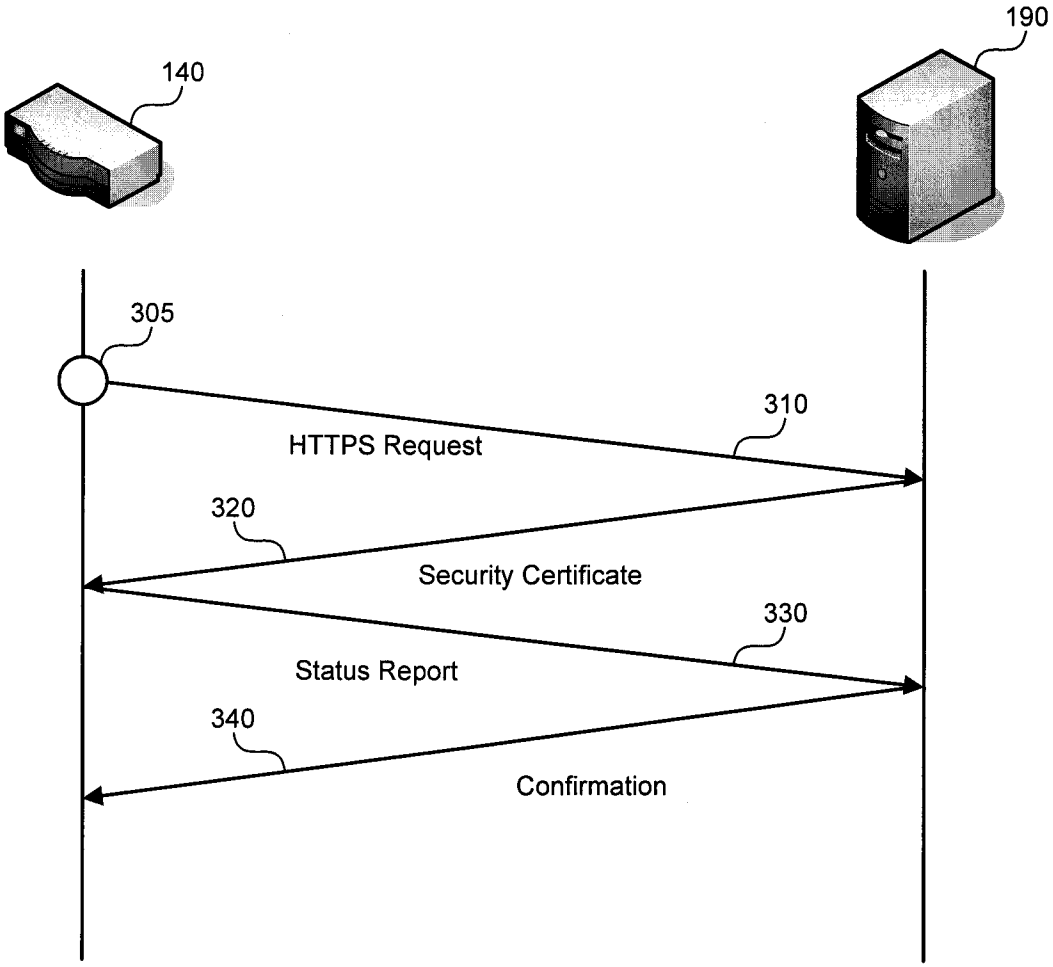

140
190
305
310
HTTPS Request
320
Security Certificate
330
Status Report
340
Confirmation

FIG. 4

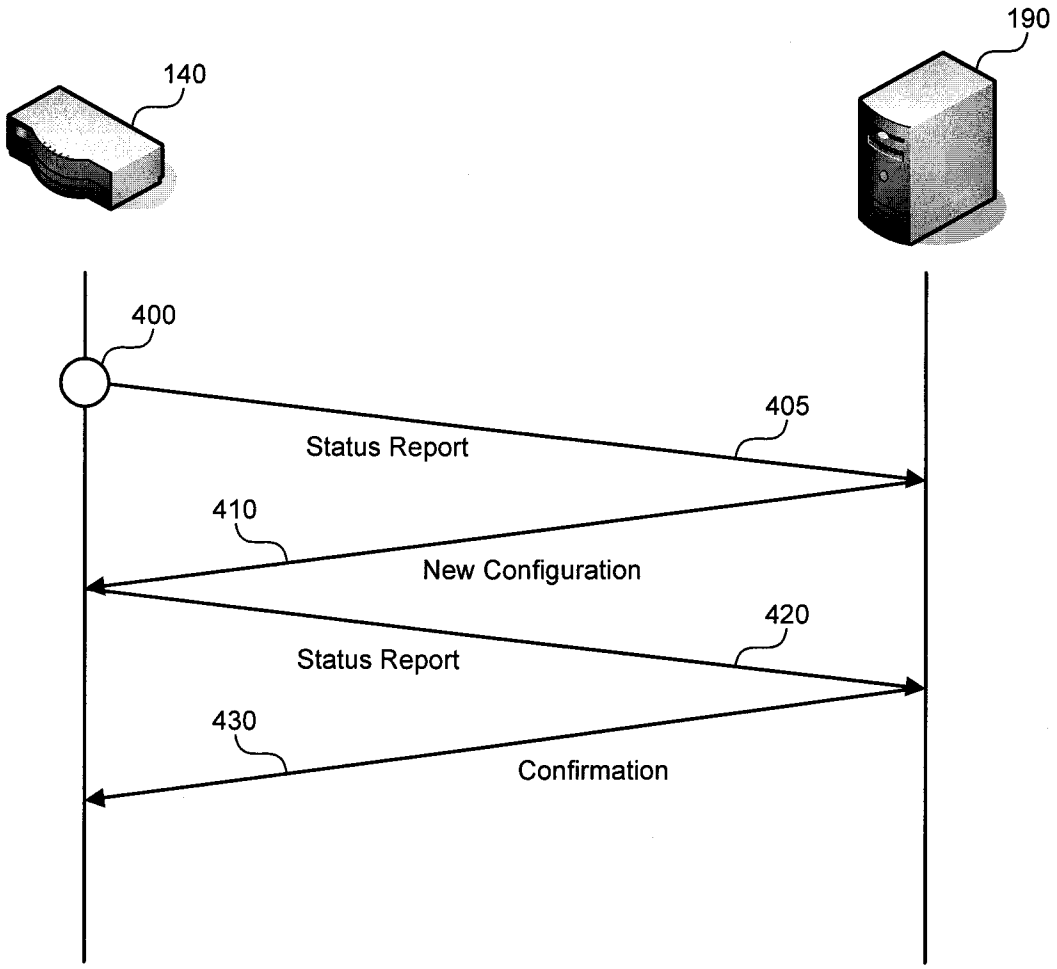

140
190
400
405
Status Report
410
New Configuration
420
Status Report
430
Confirmation

FIG. 5

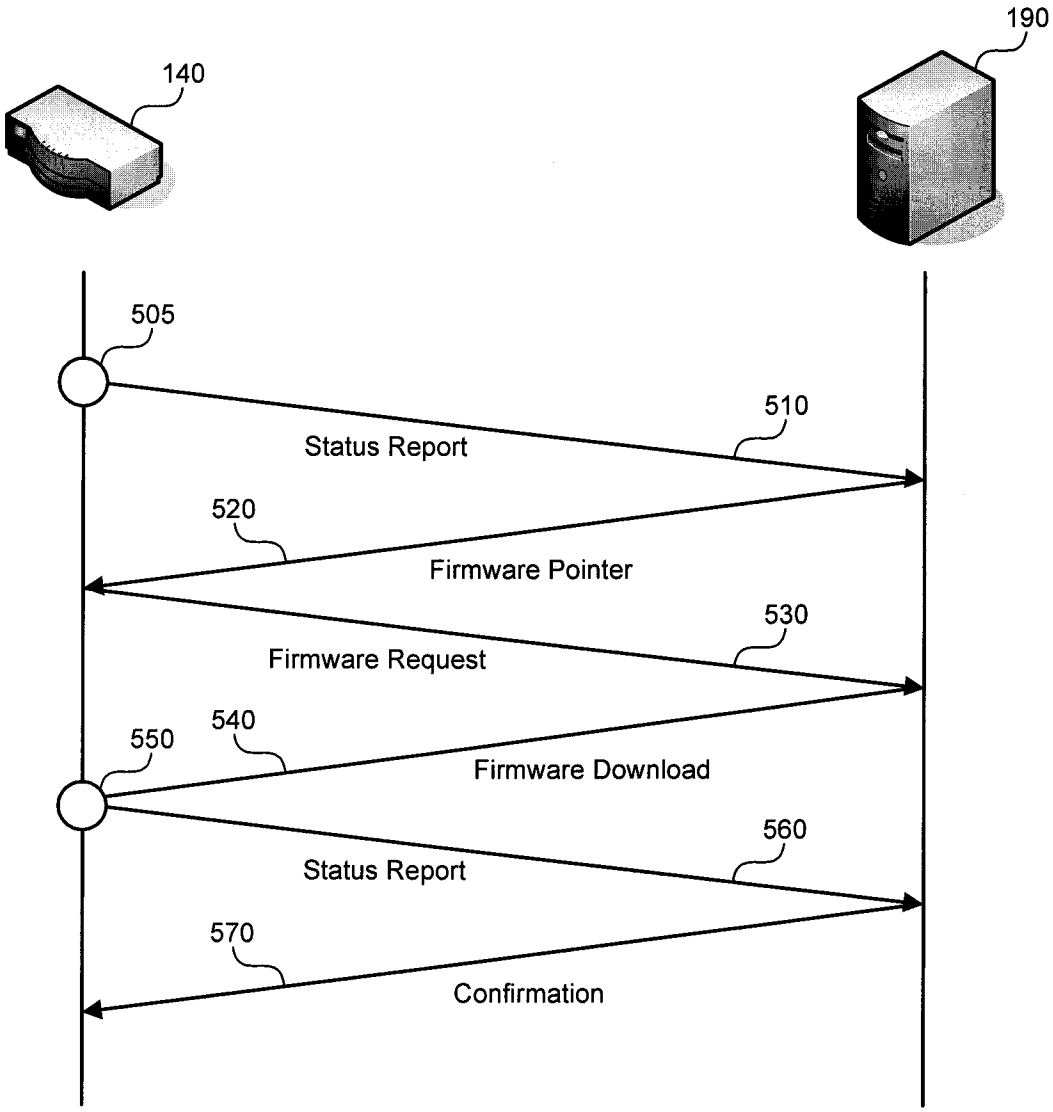

140
190
505
510
Status Report
520
Firmware Pointer
530
Firmware Request
540
550
Firmware Download
560
Status Report
570
Confirmation

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/82285

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04Q 7/20 (2008.01)
USPC - 709/223
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)
USPC: 709/223

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 455/517; 709/207, 221, 222, 223, 224

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
USPTO WEST (PGPB, USPT, EPAB, JPAB); Google Scholar
Search terms: configuring or troubleshooting or servicing or updating or managing or monitoring, access point or Wireless access point or AP, configuration file or update, status report or check or update, server, mobile or cell or phone, UMA or unlicensed mobile access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2005/0114504 A1 (MAROLIA et al.) 26 May 2005 (26.05.2005), Fig. 1, para [0009]-[0011], [0021]-[0027], [0031]-[0037]	1-14, 18-19, 21-29 15-17, 20, 30
Y	US 2001/0052006 A1 (BARKER et al.) 13 December 2001 (13.12.2001), abstract, para [114]-[0115]	15-17, 20
Y	US 2006/0223498 A1 (GALLAGHER et al.) 05 October 2006 (05.10.2006), abstract	30

☐ 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	Date of mailing of the international search report
12 February 2008 (12.02.2008)	10 MAR 2008
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

Form PCT/ISA/210 (second sheet) (April 2007)