

METHODS AND APPARATUS FOR USE IN FACILITATING THE COMMUNICATION OF
NEIGHBORING NETWORK INFORMATION TO A MOBILE TERMINAL WITH USE OF A
RADIUS COMPATIBLE PROTOCOL

5 RELATED APPLICATIONS

[0001] This Patent claims the benefit of U.S. Provisional Patent Application No. 61/184,116,
filed on June 4, 2009 and U.S. Patent Application No. 12/793,977 filed on June 4, 2010 which is
hereby incorporated herein by reference in its entirety.

10 Field of the Technology

[0002] The present disclosure relates generally to communication techniques for assisting
wireless mobile terminals for wireless communications, and more particularly to techniques for
facilitating the communication of neighboring network information to mobile terminals for
handover purposes.

15 BACKGROUND

Description of the Related Art

[0003] Mobile terminals may be adapted to operate in one or more of a variety of different types
of wireless networks, such as wireless local area networks (WLANs), WiMAX networks,
cellular telecommunication networks, etc. When operating in a WLAN or WiMAX network, the
20 mobile terminal may lose radio coverage with the network or otherwise need to switch to an
alternative neighboring wireless network to continue communications.

[0004] To do this, the mobile terminal could scan using its one or more wireless transceivers to
identify available wireless networks in its coverage region. Excessive scanning by the mobile
terminal, however, may consume too much time and power of the mobile terminal. It may be

helpful, on the other hand, if the identifications of the available wireless networks could be obtained by the mobile terminal via the current wireless network before the switching occurs. Given the new network components and modules which could be required to achieve this goal, however, deployment could become burdensome and difficult, especially given the many diverse
5 wireless networks already in existence today.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Embodiments of present disclosure will now be described by way of example with reference to attached figures, wherein:

10 [0006] FIG. 1 is an illustrative representation of a communication system which includes a radio access network (RAN), which may be a wireless local area network (WLAN) such as an IEEE 802.11-based wireless network, and a wireless wide area network (WWAN) such as a public land mobile network (PLMN), within which a mobile terminal may operate;

15 [0007] FIG. 2 is a schematic diagram of the mobile terminal which may operate in both the WLAN and the PLMN of FIG. 1;

[0008] FIG. 3 is a top down view showing the mobile terminal moving in accordance with a travel path through coverage regions of the WLAN and the PLMN of FIG. 1;

[0009] FIG. 4 is a general illustrative representation of the communication system of FIG. 1 which may be utilized for facilitating the communication of neighboring network information to
20 the mobile terminal;

[0010] FIG. 5 is a process flow diagram for describing a technique for use in facilitating communication of neighboring network information to the mobile terminal in the environments described in relation to FIGs. 1-4;

[0011] FIG. 6 is another process flow diagram for describing another technique for use in facilitating communication of neighboring network information to the mobile terminal in the environments described in relation to FIGs. 1-4;

[0012] FIG. 7 is an illustrative representation of the communication system of FIG. 1, where the mobile terminal is shown to perform communication operations in the WLAN; and

[0013] FIG. 8 is an illustrative representation of the communication system of FIG. 1, where the mobile terminal switches from communication operations in the WLAN to the PLMN.

DETAILED DESCRIPTION

[0014] What are described herein are methods and apparatus for use in facilitating the communication of neighboring network information to a mobile terminal. The communication of neighboring network information to mobile terminals for handover purposes as described herein does not require excessive scanning by the mobile terminal, and does not require burdensome and difficult deployment of network components or modules.

[0015] One illustrative technique is employed in a radio access network, such as a wireless local area network (WLAN). This technique involves the steps of receiving, from the mobile terminal, a request for neighboring network information; producing, in response to receiving the request, a corresponding request for the neighboring network information in accordance with a remote access dial-in user server (RADIUS) compatible protocol; sending the corresponding request to an information server (e.g. an authentication, authorization, and accounting (AAA) server) of a core network of a public land mobile network (PLMN) associated with the mobile terminal; receiving, from the information server, in response to the corresponding request, the neighboring network information in accordance with the RADIUS compatible protocol; and sending, in

response to the request, the neighboring network information to the mobile terminal. The request/response for the neighboring network information may be an IEEE 802.21 information request/response. If the radio access network is a WLAN adapted in accordance with IEEE 802.11, the request/response may be communicated in accordance with IEEE 802.11u (e.g.,
5 generic access service or GAS) or an extensible authentication protocol (EAP). If the radio access network is a WiMAX network adapted in accordance with IEEE 802.16, the request/response may be communicated in accordance with IEEE 802.16g.

[0016] Another illustrative technique is employed in the information server of the core network of the PLMN and involves receiving, from the radio access network, a request for neighboring
10 network information in accordance with the RADIUS compatible protocol; retrieving, in response to receiving the request, neighboring network information corresponding to an indication provided in the request; and sending, to the network access server, in response to receiving the request, the retrieved neighboring network information in accordance with the RADIUS compatible protocol.

[0017] To help further illustrate these techniques, FIG. 1 is an illustrative representation of a communication system 100 which includes a wireless local area network (WLAN) 102 and a public land mobile network (PLMN) 104. WLAN 102 may be or be referred to as one type of radio access network (RAN) utilized by a mobile terminal 106. Having one or more base stations and base station controllers, PLMN 104 may be or be referred to as a wireless wide area
20 network (WWAN) or a mobile telecommunications network which may be further utilized by mobile terminal 106.

[0018] In the embodiment described, WLAN 102 is an IEEE 802.11-based wireless network. WLAN 102 may be part of a communication network such as a local area network (LAN) 110.

In this embodiment, LAN 110 is part of a private communication network, which may be an enterprise network of an enterprise having a gateway including a firewall 116. Alternatively, LAN 110 may be a public communication network which may not require any gateway. Terminals may connect to LAN 110 through any suitable means, such as through a plurality of
5 wireless access points (APs) (e.g. APs 112 and 114) of WLAN 102. Such mobile terminals and wireless APs can operate in accordance with IEEE 802.11 standards.

[0019] LAN 110, which includes WLAN 102, provides various local data and communication services to its terminals. For example, LAN 110 may provide for voice telephony communication services for its terminals with use of Voice over IP (VoIP) communications. For
10 such services, LAN 110 may utilize servers such as a VoIP type server 118 or at least one session server which is a session initiation protocol (SIP) server. Communication applications, such as VoIP applications, may require the use of SIP. SIP is well-documented in standard documents such as Request For Comments (RFC) 3261. In some embodiments, LAN 110 also includes an AAA proxy server (or "proxy server") 190, the purpose and use of which will be
15 described in more detail below.

[0020] Note that each wireless AP may include or cooperate with a network access server (NAS) function of WLAN 102. In general, a NAS serves as a gateway for a network to guard access to a protected resource; typically, when a mobile terminal connects to a NAS, the NAS communicates with another network resource to identify whether credentials of the mobile
20 terminal are valid for granting/denying access.

[0021] PLMN 104 includes a core network 136, a plurality of base station controllers such as a base station controller (BSC) 138 coupled to core network 136, and a plurality of base stations such as a base station (BS) 140 coupled to associated BSCs 138. Core network 136, BSC 138,

and base station 140 operate in a conventional fashion as well-documented. Other PLMNs in the environment have a similar or the same architecture as PLMN 104, such as a PLMN 105 having a core network 146, a plurality of base station controllers such as a base station controller (BSC) 148, a plurality of base stations such as a base station (BS) 150 coupled to associated BSCs 148, and a gateway/controller 144 provided between the Internet 101 and core network 146.

[0022] In this example, mobile terminal 106 of LAN 110 is shown as a mobile communication device/wireless handset (WH) of the dual-mode type, having both WLAN and WWAN radio interfaces. In particular, mobile terminal 106 is shown to have one or more processors 120, a WLAN radio interface 122, a WWAN radio interface 124, and antenna components 125 and 126 coupled to radio interfaces 122 and 124. Thus, mobile terminal 106 may access services of core network 136 of PLMN 104 with use of WWAN radio interface 124, as well as access services of LAN 110 with use of WLAN radio interface 122.

[0023] Communications between LAN 110 and core network 136 of PLMN 104 may be facilitated through a suitable connecting network such as a broadband, wide-area IP communication network (e.g. the Internet 101) or any suitable public or private wide area network. Gateway/controller 142 is provided between the Internet 101 and core network 136 of PLMN 104 in order to facilitate access to core network 136 by terminals through alternative links (e.g. radio links wireless APs 112 and 114) different than those conventional radio links offered in the PLMN 104 (e.g. radio links of base station 140). Thus, mobile terminal 106 may also access services of core network 136 of PLMN 104 via WLANs, such as WLAN 102, through use of WLAN radio interface 122. For such communications, gateway/controller 142 and mobile terminal 106 are adapted to establish and maintain a (secure) tunnel connection between each other through the intervening networks. Note that WLAN 102 may be operator-

controlled or provided (e.g. controlled or provided by the operator associated with PLMN 104), user-controlled or provided (e.g. controlled or provided by the end user of mobile terminal 106), or third-party-controlled or provided.

[0024] Core network 136 also has an authentication, authorization, and accounting (AAA) server 180. Similarly, core network 146 has an AAA server 182. Such AAA servers 180 and 182 may operate in accordance with a Remote Authentication Dial-In User Service (RADIUS) protocol (e.g. RFC 2865) or RADIUS compatible protocol. Hence, AAA servers 180 and 182 may be or be referred to as RADIUS servers. The idea behind a central AAA server is that, instead of requiring every NAS to maintain a list of authorized usernames and passwords, RADIUS Access-Requests are forwarded to the AAA server. Thus, use of a central user database is provided, consolidating decision-making at a single point, while allowing calls to be supported by a large, physically-distributed set of NASs. Such AAA servers and protocols are already widely deployed and in use in a variety of different networks.

[0025] When mobile terminal 106 connects, the NAS typically sends a RADIUS Access-Request message to AAA server 180, relaying information such as the user's name and password, type of connection (port), NAS identity, and a message Authenticator. Upon receipt, AAA server 180 uses the packet source, NAS identity, and Authenticator to determine whether the NAS is permitted to send requests. If so, AAA server 180 attempts to identify the user's name in its database. It then applies the password and perhaps other attributes carried in the Access-Request to decide whether access should be granted to this user. Depending upon the authentication method being used, AAA server 180 may return a RADIUS Access-Challenge message that carries a random number. The NAS relays the challenge to mobile terminal 106, which must respond with the correct value to prove its asserted identity (e.g. encrypting the challenge with its

password), which the NAS relays to AAA server 180 inside another RADIUS Access-Request message. If AAA server 180 is satisfied that mobile terminal 106 is authentic and authorized to use the requested service, it returns a RADIUS Access-Accept message. If not, AAA server 180 returns a RADIUS Access-Reject message and the NAS disconnects mobile terminal 106. When
5 an Access-Accept message is received and RADIUS Accounting is enabled, the NAS sends a RADIUS Accounting-Request (Start) message to AAA server 180. AAA server 180 adds an accounting record to its log and acknowledges the request, whereupon the NAS activates the user's session. At the end of the session, a similar RADIUS Accounting-Request (Stop) message is exchanged so that accounting records will reflect the actual session duration and disconnect
10 reason.

[0026] Alternatively, AAA servers 180 and 182 may operate in accordance with a different (but nonetheless RADIUS compatible) protocol, such as a Diameter protocol. A Diameter NASREQ (network access server requirements) application provides for AAA services. The Diameter NASREQ application uses existing RADIUS attributes where possible to carry data objects, to
15 ease migration of existing RADIUS servers to Diameter, and to reduce the protocol conversion work required for a server that acts as a RADIUS/Diameter gateway.

[0027] Diameter is defined in terms of a base protocol and a set of applications, which allows the protocol to be extended to new access technologies. The base protocol provides basic mechanisms for reliable transport, message delivery, and error handling. The base protocol is
20 used in conjunction with a Diameter application. Each application relies on the services of the base protocol to support a specific type of network access. The two major applications are Mobile IPv4 and NASREQ. The base protocol defines the basic Diameter message format. Data is carried within a Diameter message as a collection of Attribute-Value Pairs (AVPs), which are

similar to RADIUS attributes. An AVP consists of multiple fields including an AVP Code, a Length, Flags, and Data. RFC 3169, Criteria for Evaluating Network Access Server Protocols, defines a number of requirements for AAA protocols used by NASs, addressing transport requirements, scalability, server failover, AVP requirements, security, authentication, authorization, policy, resource management, accounting, and more. RFC 2477, Criteria for Evaluating Roaming Protocols, similarly addresses the needs of AAA protocols supporting a roaming environment. The Diameter NASREQ application (combined with the base protocol) satisfies the requirements of both of these specifications. Even further, the NASREQ application, with native Extensible Authentication Protocol (EAP), offers secure authentication.

The NASREQ application defines the Diameter-EAP-Request and Diameter-EAP-Answer messages that allow the EAP payload to be encapsulated within the Diameter protocol. The NASREQ application's AA-Request message corresponds to the RADIUS Access-Request. The AA-Answer message corresponds to the RADIUS Access-Accept and Access-Reject messages. The NASREQ application has guidelines to be used by a server that acts as a RADIUS-Diameter protocol gateway, i.e. a server that receives a RADIUS message that is to be translated and transmitted as a Diameter message, and vice versa.

[0028] Note that the description of the architecture for FIG. 1 relates to a specific example for illustration, where the WLAN is an IEEE 802.11-based network and the WWAN is a cellular telecommunications network. However, the WLAN and WWAN may be networks different from those networks. The WLAN may be a WiMAX-based network (i.e. IEEE 802.16), a Ultra-WideBand (UWB)-based network (i.e. IEEE 802.15), a Bluetooth-based network, as a few examples. The WWAN may be a Long-Term Evolution (LTE)-based network, an EVolution-Data Only (EV-DO)-based network, or a UMTS-based network, as a few examples.

[0029] Referring now to FIG. 2, electrical components of a typical mobile terminal 106 (e.g. a wireless handset, a mobile station) which operates in a wireless network environment which includes both WLANs (represented in FIG. 2 by AP 112) and WWANs/PLMNs (represented in FIG. 2 by cellular base stations 200 which include base stations 140 and 150 for its associated PLMNs) are now described. Mobile terminal 106 may be representative of one or more terminals which operate in communication system 100 of FIG. 1. Mobile terminal 106 can be a two-way communication device having at least voice and advanced data communication capabilities, including the capability to communicate with other computer systems. Depending on the functionality provided by mobile terminal 106, it may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities).

[0030] As shown in FIG. 2, mobile terminal 106 is adapted to wirelessly communicate with base stations 200. For communication with base stations 200, mobile terminal 106 utilizes a communication subsystem 211 which includes RF transceiver circuitry. Communication subsystem 211 includes a receiver 212, a transmitter 214, and associated components, such as one or more (embedded or internal) antenna elements 216 and 218, local oscillators (LOs) 213, and a digital signal processor (DSP) 220. The specific design of communication subsystem 211 depends on the communication network in which mobile terminal 106 is intended to operate. In the present application, communication subsystem 211 (including its associated processor/processing components) are operative in accordance with a cellular or other suitable WWAN standards (i.e. a standard other than IEEE 802.11), such as GSM/GPRS standards.

[0031] Mobile terminal 106 may send and receive communication signals through the network after required network procedures have been completed. Signals received by antenna 216

through the network are input to receiver 212, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection, and like, and in example shown in FIG. 2, analog-to-digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in DSP 220. In a similar manner, signals to be transmitted are processed, including modulation and encoding, for example, by DSP 220. These processed signals are input to transmitter 214 for digital-to-analog (D/A) conversion, frequency up conversion, filtering, amplification and transmission through the network via antenna 218. DSP 220 not only processes communication signals, but may also provide for receiver and transmitter control. Note that receiver 212 and transmitter 214 may share one or more antennas through an antenna switch (not shown in FIG. 2), instead of having two separate dedicated antennas 216 and 218 as shown.

[0032] Mobile terminal 106 also has a communication subsystem 291 which includes RF transceiver circuitry operative in accordance with a suitable WLAN standard, such as the IEEE 802.11 standard, for communications with WLANs (e.g. represented by AP 112 in FIG. 2). Communication subsystem 291 is similar in structure and functionality to communication subsystem 211, where DSP 220 may be replaced with a processing module referred to as a baseband (BB) and media access control (MAC) module. Although mobile terminal 106 may have separate and independent subsystems for these purposes, at least some portions or components of these otherwise different subsystems may be shared where possible. As mobile terminal 106 operates in accordance with both a cellular network interface standard (e.g. GSM/GPRS standard) and the IEEE 802.11 standard, it may be referred to as a “dual mode” mobile terminal.

[0033] Since mobile terminal 106 may be a handheld, portable, battery-powered device, it also includes a battery interface 254 for receiving one or more rechargeable batteries 256. Such a battery 256 provides electrical power to most if not all electrical circuitry in mobile terminal 106, and battery interface 254 provides for a mechanical and electrical connection for it. Battery interface 254 is coupled to a regulator (not shown in FIG. 2) that provides a regulated voltage V to all of the circuitry.

[0034] Mobile terminal 106 includes a microprocessor 238 (one type of processor or controller) that controls overall operation of mobile terminal 106. This control includes the communication techniques of the present disclosure. Communication functions, including at least data and voice communications, are performed through communication subsystem 211. Microprocessor 238 also interacts with additional device subsystems such as a display 222, a flash memory 224, a random access memory (RAM) 226, auxiliary input/output (I/O) subsystems 228, a serial port 230, a keyboard (or keypad) 232, a speaker 234, a microphone 236, a short-range communications subsystem 240, and any other device subsystems generally designated at 242. Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 232 and display 222, for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list. Operating system software used by microprocessor 238 can be stored in a persistent store such as flash memory 224, which may alternatively be a read-only memory (ROM) or similar storage element (not shown). Specific device applications, or parts thereof, may be temporarily loaded into a volatile store such as RAM 226.

[0035] Microprocessor 238, in addition to its operating system functions, enables execution of software applications on mobile terminal 106. A predetermined set of applications that control basic device operations, including at least data and voice communication applications, will normally be programmed and/or installed on mobile terminal 106 during its manufacture (including the network selection control techniques of the present disclosure). An application that may be loaded onto mobile terminal 106 may be a personal information manager (PIM) application having the ability to organize and manage data items relating to user such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items. Naturally, one or more memory stores are available on mobile terminal 106, and memory 262 (designed as "mem" in FIG. 2) such as a subscriber identity module (SIM) or the like coupled via an interface 264 is used to facilitate storage of PIM data items and other user information.

[0036] The PIM application has the ability to send and receive data items via the wireless network. In one embodiment, PIM data items are seamlessly integrated, synchronized, and updated via the wireless network, with the wireless device user's corresponding data items stored and/or associated with a host computer system thereby creating a mirrored host computer on mobile terminal 106 with respect to such items. This can be especially useful where the host computer system is the wireless device user's office computer system. Additional applications may also be loaded onto mobile terminal 106 through network, an auxiliary I/O subsystem 228, serial port 230, short-range communications subsystem 240, or any other suitable subsystem 242, and installed by a user in RAM 226 or a non-volatile store (not shown) for execution by microprocessor 238. Such flexibility in application installation increases the functionality of mobile terminal 106 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic

commerce functions and other such financial transactions to be performed using mobile terminal 106.

[0037] In a data communication mode, a received signal such as a text message, an e-mail message, or web page download will be processed by communication subsystem 211 and input to microprocessor 238. Microprocessor 238 will further process the signal for output to display 222 or alternatively to auxiliary I/O device 228. A user of mobile terminal 106 may also compose data items, such as e-mail messages, for example, using keyboard 232 in conjunction with display 222 and possibly auxiliary I/O device 228. Keyboard 232 is a complete alphanumeric keyboard and/or telephone-type keypad. These composed items may be transmitted over a communication network through communication subsystem 211. For voice communications, the overall operation of mobile terminal 106 is substantially similar, except that the received signals would be output to speaker 234 and signals for transmission would be generated by microphone 236. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on mobile terminal 106. Although voice or audio signal output is accomplished primarily through speaker 234, display 222 may also be used to provide an indication of the identity of a calling party, duration of a voice call, or other voice call related information, as some examples.

[0038] Serial port 230 in FIG. 2 is normally implemented in a personal digital assistant (PDA)-type communication device for which synchronization with a user's desktop computer is a desirable, albeit optional, component. Serial port 230 enables a user to set preferences through an external device or software application and extends the capabilities of mobile terminal 106 by providing for information or software downloads to mobile terminal 106 other than through a wireless communication network. The alternate download path may, for example, be used to

load an encryption key onto mobile terminal 106 through a direct and thus reliable and trusted connection to thereby provide secure device communication. Short-range communications subsystem 240 of FIG. 2 is an additional optional component that provides for communication between mobile terminal 106 and different systems or devices, which need not necessarily be similar devices. For example, subsystem 240 may include an infrared device and associated circuits and components, or a BLUETOOTH® communication module to provide for communication with similarly enabled systems and devices. BLUETOOTH® is a registered trademark of Bluetooth SIG, Inc.

[0039] Although a specific mobile terminal 106 has just been described, any suitable mobile communication device or terminal may be part of the disclosed methods and apparatus which will be described in fuller detail below.

[0040] FIG. 3 is a top down view of a geographic region 300, which shows mobile terminal 106 moving in accordance with a travel path 310 through a coverage region 350 of PLMN 105 (e.g. a GSM/GPRS based network) and a coverage region 304 of WLAN 102. Coverage region 350 of PLMN 105 may be defined by one or more base stations of the network, whereas coverage region 304 of WLAN 102 may be defined by one or more wireless APs 112 and 114 of the network. Another coverage region 306 may be that of another wireless network, such as another WLAN or, alternatively, a WiMAX network. As shown, coverage regions 304 and 306 may overlap in whole or in part with coverage region 350 of PLMN 105. As described earlier, mobile terminal 106 may have different transceiver portions (e.g. WLAN radio interface 122 and WWAN radio interface 124 of FIG. 1, or communication subsystems 211 and 291 of FIG. 2) associated with the two different types of networks (WLAN and WWAN). Mobile terminal 106 may generally have wireless access to only one of the networks for services at any given time.

As it moves along travel path 310, in order to maintain continuity in service when losing coverage with its current wireless network, mobile terminal 106 is required to switch its communication operations to a different wireless network. For example, mobile terminal 106 may switch communication operations from WLAN 102 to PLMN 105.

5 [0041] This is shown in more detail with reference ahead to FIGs. 7 and 8. In FIG. 7, an illustrative representation of the communication system of FIG. 1 is shown, where mobile terminal 106 performs communication operations in WLAN 102 over a wireless link 702. On the other hand, in FIG. 8, mobile terminal 106 is shown to switch from communication operations in WLAN 102 to PLMN 105 over a wireless link 802. The general methodology for
10 switching may be based on processing of a received signal strength indicator (RSSI) of a radio frequency (RF) signal from the wireless AP of the WLAN (e.g. AP 112 of WLAN 102), or a signal-to-noise ratio (SNR) of the RF signal from the wireless AP, or other signal conditions or events. The switching operation may be initiated by mobile terminal 106 itself, or with the assistance or instruction from the network.

15 [0042] Referring now to FIG. 4, a general illustrative representation of the communication system of FIG. 1 which may be utilized for facilitating the communication of neighboring network information to the mobile terminal is shown. In general, while operating in WLAN 102, mobile terminal 106 sends a request for neighboring network information to WLAN 102. The NAS associated with wireless AP 112 of WLAN 102 receives and identifies such request and, in
20 response, produces and sends a corresponding request for the neighboring network information in accordance with a RADIUS compatible protocol. The corresponding request may be sent to AAA server 180 of core network 136 of (e.g. the home) PLMN 104 associated with mobile terminal 106. AAA server 180 has access to and retrieves the neighboring network information

in response to the corresponding request. The neighboring network information may be correlated based on NAS location or the like, and may be stored either locally or at a mobility server. For example, the neighboring network information may be stored in a database based on an identification of the NAS. The neighboring network information includes one or more
5 network identifications of one or more wireless networks (e.g. other surrounding PLMNs, WLANs in the figure) located within the vicinity of WLAN 102. The wireless networks identified may be any suitable type of wireless networks, including GSM, GPRS/EDGE, UMTS, WLANs, WiMAX, etc. AAA server 180 replies, in accordance with the RADIUS compatible protocol, to the NAS of wireless AP 112 with a response which includes the retrieved
10 neighboring network information. The NAS of wireless AP 112 then sends the neighboring network information to mobile terminal 106. Thereafter, mobile terminal 106 may make a handover decision for handover from the WLAN 102 to a selected one of the other wireless networks identified from the received network identifications. Note that, in some embodiments, the communications for obtaining the neighboring network information are facilitated via proxy
15 server 190 of LAN 110, which is described in more detail later below.

[0043] In one embodiment, the procedures are performed in accordance with Media Independent Handover (MIH) defined by IEEE 802.21. The IEEE 802.21 standard defines a transport agnostic protocol for MIH and three services: a command service to co-ordinate handover between mobile terminals and networks; an event server to exchange link state information
20 between mobile terminals and networks; and an information service to exchange information on neighboring network handover candidates.

[0044] Thus, the request/response for the neighboring network information may be an IEEE 802.21 information request/response. For a wireless network that is a WLAN, the

request/response may be communicated in accordance with IEEE 802.11u or an extensible authentication protocol (EAP). Under IEEE 802.11u, a mobile terminal requests information from the WLAN in order to obtain network service information using the defined generic access service (GAS) procedures. IEEE 802.11u specifies two mechanisms to obtain the information, one for unicast and one for multicast. In both mechanisms, the mobile terminal initiates service discovery by sending a GAS Initial Request frame. The mobile terminal sends a GAS Initial Request frame since the service information is not included in the beacon or probe response(s). For a wireless network that is a WiMAX network, the request/response may be communicated in accordance with IEEE 802.16g.

[0045] FIG. 5 is a process flow diagram for describing a technique for use in facilitating communication of neighboring network information to a mobile terminal, which may be utilized in the environment described above in relation to FIGs. 1-4. The technique of the present disclosure may be embodied in a server (e.g. a network access server, an information server which may be an AAA server, RADIUS server, etc.) having one or more processors. Other techniques may be embodied in a mobile terminal having one or more processors adapted to execute the technique. The technique may be further embodied in a computer program product having a computer readable medium and computer instructions stored in the computer readable medium, where the one or more processors are operative to execute the computer instructions in accordance with the method. In the present discussion, it is assumed that the NAS is part of AP 112, even though it may be an entity in WLAN 102 that is separate from AP 112.

[0046] The method of FIG. 5 begins where mobile terminal 106 performs a discovery and attachment procedure with AP 112 of WLAN 102 (step 502 of FIG. 5). The discovery procedure with AP 112 involves scanning to identifying available wireless networks in the coverage region

of mobile terminal 106. The discovery procedure may include the mobile terminal's sending of a probe request and the receiving of a probe response. If the probe request/response is successful, an authentication request and response is exchanged. Successful authentication permits further specified data exchange, for example, to the attachment procedure. During the attachment
5 procedure, an association request and response is exchanged. Successful association permits further specified data exchange such as data frames, management frames, and control frame. The association request data frame may, for example, include capability information, listen interval, SSID of WLAN 102, and supported rates. The association response data frame may, for example, include capability information, status codes, association ID, and supported rates.

10 **[0047]** After its association with AP 112, mobile terminal 106 produces and causes a request for neighboring network information to be transmitted via WLAN 102 (step 504 of FIG. 5). The request may include various information including an identification of mobile terminal 106 (e.g. telephone number, personal identification number or PIN, e-mail address, etc.) and an identification of WLAN 102 (e.g. set service identification or SSID, extended SSID or ESSID,
15 etc.). This request may be or include an IEEE 802.21 information request for the neighboring network information. In the case of IEEE 802.11, for example, the request may be communicated in accordance with IEEE 802.11u or, more specifically, IEEE 802.11u generic access service (GAS). In the case of IEEE 802.16, for example, the request may be communicated in accordance with IEEE 802.16g.

20 **[0048]** AP 112 identifies this request to be for obtaining neighboring network information (e.g. it may identify it as an IEEE 802.21 information request). In response, AP 112 performs certain processing to obtain this information on behalf of mobile terminal 106. In particular, AP 112 produces a corresponding request for the neighboring network information in accordance with a

remote access dial-in user server (RADIUS) compatible protocol. The RADIUS compatible protocol utilized may be a RADIUS protocol. As another example, the RADIUS compatible protocol may be a Diameter NASREQ protocol, which is backward-compatible with RADIUS. Note that, as a NAS function may be part of AP 112, this NAS function may include a RADIUS or RADIUS compatible (e.g. Diameter or Diameter NASREQ) client to serve these purposes. AP 112 sends the corresponding request in accordance with the RADIUS compatible protocol to AAA server 180 of core network 136 (step 506 of FIG. 5), which receives it. AP 112 addresses the corresponding request to AAA server 180 based on a network access identifier (NAI) of mobile terminal 106 and a NAS Port of the NAS in AP 112, which are supplied in the request. In one embodiment, a RADIUS type-length value (TLV) may be utilized in the communication of the corresponding request. The TLV may include a type indicative of "interworking-request", a length which is variable, and a value which is the string containing the request in accordance with IEEE 802.21 M1H or IEEE 802.11u GAS.

[0049] In response to receiving the request of step 506, AAA server 180 retrieves neighboring network information corresponding to an indication provided in the request. In the present example, the indication is provided to AAA server 180 by the identification of WLAN 102 (e.g. SSID or ESSID), and/or cell identifications (Cell IDs), and/or the NAS ID of the AAA client, as supplied from the request. The neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within the coverage region of WLAN 102. The wireless networks identified may be any type of suitable wireless networks, including GSM, GPRS/EDGE, UMTS, WLANs, WiMAX, etc. AAA server 180 may selectively retrieve neighboring network information that is unique to each given location as indicated in such requests. At least some of the networks indicated by the

neighboring network information are networks that mobile terminal 106 may be handed over to in the event mobile terminal 106 exits from WLAN 102. The one or more neighboring wireless communication networks may be compatible with cellular telecommunications, IEEE 802.11, or IEEE 802.16 standards, as examples.

5 [0050] AAA server 180 may retrieve the neighboring network information from a locally-stored table, or a database, using a request/response protocol with the indication or location from the request as an input or key. In one embodiment, AAA server 180 may retrieve the neighboring network information from a different server, such as an outside, external mobility server. In this example, AAA server 180 may submit a request to the mobility server with the indication or
10 location (step 508 of FIG. 5) and, in response, receive a response which includes the neighboring network information (step 510 of FIG. 5).

[0051] Note that the mobility server may be adapted to receive and serve requests from many different similarly-situated servers (one of which is AAA server 180) deployed in different networks at different locations. The mobility server may have access to one or more databases
15 which store local, regional, or global network information (such as a global network map), information which may be retrieved request/response protocol which utilizes an indication or location as an input or key, for example.

[0052] After such retrieval, AAA server 180 sends the neighboring network information to AP 112 in accordance with the RADIUS compatible protocol, and AP 112 receives this information
20 in response (step 512 of FIG. 5). AP 112 then suitably formats and sends, to mobile terminal 106, a response to the initial request which includes the neighboring network information (step 514 of FIG. 5). The response may be or include an IEEE 802.21 information response having the neighboring network information. In the case of IEEE 802.11, for example, the response

may be communicated in accordance with IEEE 802.11u. In the case of IEEE 802.16, for example, the response may be communicated in accordance with IEEE 802.16g.

[0053] Again, the neighboring network information includes one or more network identifications of one or more wireless networks located within the coverage region of WLAN 102. The neighboring network information may thereafter be utilized by mobile terminal 106 to perform a handover to another neighboring network different from and neighboring the coverage region of mobile terminal 106 or WLAN 102, without the need to perform exhausting scanning operations to locate various different neighboring networks.

[0054] FIG. 6 is another process flow diagram for describing another technique for use in facilitating communication of neighboring network information to the mobile terminal, which also may be utilized in the environment described above in relation to FIGs. 1-4. Again, the technique of the present disclosure may be embodied in a server (e.g. a network access server, an information server such as an AAA server, etc.) having one or more processors. Other techniques may be embodied in a mobile terminal having one or more processors adapted to execute the technique. The technique may be further embodied in a computer program product having a computer readable medium and computer instructions stored in the computer readable medium, where the one or more processors are operative to execute the computer instructions in accordance with the method. In the present discussion, it is assumed that the NAS is part of AP 112, even though it may be an entity in WLAN 102 that is separate from AP 112.

[0055] Similar to that described in relation to FIG. 5, the method of FIG. 6 begins where mobile terminal 106 performs a discovery and attachment procedure with AP 112 of WLAN 102 (step 602 of FIG. 6). The discovery procedure with AP 112 involves scanning to identify available wireless networks in the coverage region of mobile terminal 106. The discovery procedure may

include the mobile terminal's sending of a probe request and the receiving of a probe response. An authentication request and response is exchanged once the probe request/response is successful. Successful authentication permits further specified data exchange, for example, to the attachment procedure. During the attachment procedure, an association request and response
5 is exchanged. Successful association permits further specified data exchange such as data frames, management frames, and control frame. The association request data frame may, for example, include capability information, listen interval, SSID of WLAN 102, and supported rates. The association response data frame may, for example, include capability information, status codes, association ID, and supported rates.

10 **[0056]** After its association with AP 112, mobile terminal 106 performs an authentication procedure with the network. The authentication procedure may be performed in accordance with an extensible authentication protocol (EAP). During this procedure, mobile terminal 112 causes a request for neighboring network information to be transmitted to AP 112 in an EAP frame (step 604 of FIG. 6). The request may include various information including an identification of
15 mobile terminal 106 (e.g. telephone number, personal identification number or PIN, e-mail address, etc.) and an identification of WLAN 102 (e.g. set service identification or SSID, extended SSID or ESSID, etc.). This request may be or include an IEEE 802.21 information request for the neighboring network information.

[0057] AP 112 identifies this request to be for obtaining neighboring network information (e.g. it
20 may identify it as an IEEE 802.21 information request) and, in response, performs certain processing to obtain this information on behalf of mobile terminal 106. In particular, AP 112 produces a corresponding request for the neighboring network information in accordance with a RADIUS compatible protocol. The RADIUS compatible protocol utilized may be a RADIUS

protocol or a Diameter NASREQ protocol (which is backward-compatible with RADIUS), as examples. Note that, as a NAS function may be part of AP 112, this NAS function may include a RADIUS or RADIUS compatible client (e.g. Diameter NASREQ client) to serve these purposes. In the present embodiment, AP 112 encapsulates the EAP request for the neighboring
5 network information into the corresponding RADIUS-compatible request and sends it to AAA server 180 of core network 136 (step 606 of FIG. 6), which receives it. AP 112 addresses the corresponding request to AAA server 180 based on a network access identifier (NAI) of mobile terminal 106 and a NAS Port of the NAS in AP 112, which are supplied in the request.

[0058] In one embodiment, the request is embedded as a type-length value (TLV) in an EAP
10 frame from mobile terminal 106, and the corresponding request includes a RADIUS attribute set to an EAP-message (e.g. value of 79). In general, this messaging may be viewed as an EAP TLV embedded in a RADIUS TLV. Any suitable implementation or protocol may be utilized for such messaging, such as EAP-FAST TLV based on RFC 4851, Protected EAP Protocol (PEAP) (e.g. Palekar et al., "Protected EAP Protocol (PEAP) Version 2", EAP Working Group,
15 15 October 2004, Internet-Draft: draft-josefsson-pppext-eap-tls-cap-10.txt), or EAP-TTLS described as AVPs in RFC 5281, as examples.

[0059] In response to receiving the request of step 606, AAA server 180 decapsulates the message to reveal the underlying EAP request for the neighboring network information. Then, AAA server 180 retrieves neighboring network information corresponding to an indication
20 provided in the request. In the present example, the indication provided to AAA server 180 by the identification of WLAN 102 (e.g. SSID or ESSID), and/or cell identifications (Cell IDs), and/or the NAS ID of the AAA client, as supplied in the request. As described above in relation to FIG. 5, the neighboring network information of FIG. 6 includes one or more network

identifications corresponding to one or more wireless communication networks neighboring the WLAN 102. The wireless networks identified may be any type of suitable wireless networks, including GSM, GPRS/EDGE, UMTS, WLANs, WiMAX, etc. AAA server 180 may retrieve the neighboring network information from the locally-stored table or the database using the request/response protocol, or from a different server such as the mobility server, where AAA server 180 submits a request to the mobility server with the indication of the location (step 608 of FIG. 6) and receives a response which includes the neighboring network information (step 610 of FIG. 6).

[0060] After such retrieval, AAA server 180 produces an EAP response which includes the neighboring network information. The EAP response is encapsulated in the RADIUS compatible protocol and sent to AP 112; AP 112 receives this information in response (step 612 of FIG. 6). Upon receipt, AP 112 decapsulates the message to reveal the underlying EAP response having the neighboring network information. AP 112 sends, to mobile terminal 106 in response to the EAP request of step 604, the EAP response which includes the neighboring network information (step 614 of FIG. 6). The EAP response may be or include an IEEE 802.21 information response having the neighboring network information. The neighboring network information may thereafter be utilized by mobile terminal 106 to perform a handover to another neighboring network different from and neighboring the coverage region of mobile terminal 106 or WLAN 102 (e.g. based on RSSI, SNR, or other signal conditions or events), without the need to perform exhausting scanning operations to locate various different neighboring networks.

[0061] In the processes described in relation to FIGs. 5 and 6, it may be assumed that a single service provider manages PLMN 104/core network 136, mobile terminal 106, and WLAN 102; therefore, no AAA proxying in WLAN 102 may be required for the communications. Here,

mobile terminal 106 may be identified by and associated with the NAI of "user@abc.com", WLAN 102 may be an "ABC" hotspot, and AAA server 180 may be addressable or identifiable by the domain of "abc.com". Again, communications between the NAS of WLAN 102 and AAA server 180 of core network 136 may be direct without the need for proxying.

5 [0062] In alternate embodiments, however, different service providers may be involved where proxying in WLAN 102 is utilized. For example, a first service provider may manage PLMN 104/core network 136 and mobile terminal 106, whereas a second different service provider may manage WLAN 102. In such alternate embodiment, AAA "proxy" server 190 is provided in LAN 110, for proxying the communications between the NAS and AAA server 180 (see FIGs. 1
10 and 4). Here, mobile terminal 106 may be identified by and associated with the NAI of "user@abc.com", AAA server 180 of core network 136 may be addressable or identifiable at "abc.com", WLAN 102 may be a "DEF" hotspot, and proxy server 190 of LAN 110 may be addressable or identifiable at the domain of "def.com". In the technique, mobile terminal 106 submits its request to the NAS, providing its NAI which includes the realm of "abc.com". The
15 NAS provides the request to proxy server 190, which identifies the realm of "abc.com" in the request and directs the request to AAA server 180 of core network 136 associated with "abc.com". AAA server 180 processes the request accordingly and submits a response back to proxy server 190, which provides it back to the NAS of WLAN 102 and thereafter to mobile terminal 106. As apparent, NAIs and realms may be utilized to facilitate the communication of
20 proper neighboring network information for mobile terminals. Also as apparent, mobile terminal 106 may cause the request to be transmitted to the proper AAA server in different ways.

[0063] Thus, according to the present disclosure, the communication of neighboring network information to mobile terminals is efficiently facilitated for handover purposes, without requiring

excessive scanning by the mobile terminal, and without burdensome and difficult deployment of network components or modules in existing networks.

[0064] As described herein, a technique in a radio access network (e.g. in a network access server or NAS) involves receiving, from a mobile terminal, a request for neighboring network
5 information; producing, in response to receiving the request, a corresponding request for the neighboring network information in accordance with a remote access dial-in user server (RADIUS) compatible protocol; sending the corresponding request to an information server (e.g. an AAA server, a RADIUS server, a Diameter NASREQ server, etc.) of a core network of a public land mobile network (PLMN) associated with the mobile terminal; receiving, from the
10 information server, in response to sending the corresponding request, the neighboring network information in accordance with the RADIUS compatible protocol; and sending, in response to the request, the neighboring network information to the mobile terminal. The request/response for the neighboring network information may be an IEEE 802.21 information request/response. If the radio access network is a wireless local area network (WLAN) adapted in accordance with
15 IEEE 802.11, the request/response may be communicated in accordance with IEEE 802.11u or an extensible authentication protocol (EAP). If the radio access network is a WiMAX network adapted in accordance with IEEE 802.16, the request/response may be communicated in accordance with 802.16g.

[0065] As further described herein, a technique in the information server of the core network of
20 the PLMN involves receiving, from the radio access network, a request for neighboring network information in accordance with a RADIUS compatible protocol (e.g. RADIUS or Diameter NASREQ); retrieving, in response to receiving the request, neighboring network information corresponding to an indication provided in the request; and sending, to the radio access network,

in response to receiving the request, the retrieved neighboring network information in accordance with the RADIUS compatible protocol.

[0066] As described, the techniques of the present disclosure may be embodied in a server (e.g. a network access server, an information server such as an AAA server, etc.) having one or more processors. Other techniques may be embodied in a mobile terminal having one or more processors adapted to execute the technique. The technique may be further embodied in a computer program product having a computer readable medium and computer instructions stored in the computer readable medium, where the one or more processors are operative to execute the computer instructions in accordance with the method. Further, the technique described assumes that the mobile terminal is a mobile communication device of the dual-mode type, having both WLAN and WWAN radio interfaces. In an alternative embodiment, however, mobile terminal 106 may have only a single (radio) interface for access (e.g. only WLAN radio interface 122) and operates accordingly without the other interface.

[0067] The above-described embodiments of the present application are intended to be examples only. Those of skill in the art may affect alterations, modifications and variations to the particular embodiments without departing from the scope of the application. For example, the embodiments of the present disclosure are generally directed to an example where the WLAN is an IEEE 802.11-based network and the WWAN is a cellular telecommunications network. However, the WLAN and WWAN may be networks different from those networks. The WLAN may be a WiMAX-based network (i.e. IEEE 802.16), an Ultra-WideBand (UWB)-based network (i.e. IEEE 802.15), a Bluetooth-based network, as a few examples. The WWAN may be a Long-Term Evolution (LTE)-based network, an EVolution-Data Only (EV-DO)-based network, or a

UMTS-based network, as a few examples. The embodiments described herein in the recited claims intend to cover and embrace all suitable changes in technology.

5

10

What is claimed is:

[Claim 1]

A method performed by a processor for accessing neighbor information, the method comprising:

receiving, from a device, a first request for neighboring network information from a network access server;

sending a second request to an authentication server based on the first request, the second request requesting the neighboring network information from the authentication server;

receiving a response to the second request containing the neighboring network information; and

sending a response to the first request including at least the received neighboring network information.

[Claim 2]

The method of claim 1, wherein the first request is transported using an extensible authentication protocol (EAP).

[Claim 3]

The method of claim 1, wherein the second request is transported utilizing an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 4]

The method of claim 1, wherein the neighboring network information is contained in the response to the first request using an IEEE 802.21 format.

[Claim 5]

The method of claim 1, wherein the device is a mobile terminal.

[Claim 6]

The method of claim 1, wherein the second request is sent by an authentication client to the authentication server, and wherein the second request includes an identification of the authentication client.

[Claim 7]

The method of claim 6, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the authentication client.

[Claim 8]

The method of claim 7, wherein the neighboring network information enables the device to perform a hand-off to one or more of the wireless communication networks.

[Claim 9]

A network device for accessing neighbor information, the network device comprising:

a processor configured to:

receive, from a device, a first request for neighboring network information from a network access server;

send a second request to an authentication server based on the first request, the second request requesting the neighboring network information from the authentication server;

receive a response to the second request containing the neighboring network information; and

send a response to the first request including at least the received neighboring network information.

[Claim 10]

The network device of claim 9, wherein the first request is transported using an extensible authentication protocol (EAP).

[Claim 11]

The network device of claim 9, wherein the second request is transported utilizing an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 12]

The network device of claim 9, wherein the neighboring network information is contained in the response to the first request using an IEEE 802.21 format.

[Claim 13]

The network device of claim 9, wherein the device is a mobile terminal.

[Claim 14]

The network device of claim 9, wherein the second request is sent by an authentication client to the authentication server, and wherein the second request includes an identification of the authentication client.

[Claim 15]

The network device of claim 14, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the authentication client.

[Claim 16]

The network device of claim 15, wherein the neighboring network information enables the device to perform a hand-off to one or more of the wireless communication networks.

[Claim 17]

A method performed by a processor for retrieving neighbor information, the method comprising:

receiving a first request for information;

determining that the first request is requesting neighboring network information;

sending a second request requesting the neighboring network information from an authentication, authorization, and accounting (AAA) server;

receiving a response to the second request containing at least the neighboring network information; and

sending a response to the first request including at least the neighboring network information from the response to the second request.

[Claim 18]

The method of claim 17, wherein the first request is transported using an extensible authentication protocol (EAP) over at least one of

a RADIUS protocol or a DIAMETER protocol.

[Claim 19]

The method of claim 17, wherein the second request is transported using an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 20]

The method of claim 17, wherein the AAA server retrieves the neighboring network information from a mobility server.

[Claim 21]

The method of claim 17, wherein the first request is received at a network access server from a mobile terminal.

[Claim 22]

The method of claim 21, wherein the second request includes an identification of the network access server.

[Claim 23]

The method of claim 22, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the network access server based on the identification of the network access server.

[Claim 24]

A network access server for retrieving neighbor information, the network access server comprising:

a processor configured to:

receive a first request for information;

determine that the first request is requesting neighboring network information;

send a second request requesting the neighboring network information from an authentication, authorization, and accounting (AAA) server;

receive a response to the second request containing at least the neighboring network information; and

send a response to the first request including at least the neighboring network information from the response to the second request.

[Claim 25]

The network access server of claim 24, wherein the first request is transported using an extensible authentication protocol (EAP) over at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 26]

The network access server of claim 24, wherein the second request is transported using an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 27]

The network access server of claim 24, wherein the neighboring network information is received from a mobility server.

[Claim 28]

The network access server of claim 24, wherein the first request is received from a mobile terminal.

[Claim 29]

The network access server of claim 24, wherein the second request includes an identification of the network access server.

[Claim 30]

The network access server of claim 29, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the network access server based on the identification of the network access server.

[Claim 31]

A method performed by a processor for retrieving neighboring network information at a mobility server, the method comprising:

receiving a request generated by an authentication server;

determining neighboring network information requested via the request;

retrieving the neighboring network information based on the request; and

sending a response to the request including at least the neighboring network information.

[Claim 32]

The method of claim 31, wherein the neighboring network information is stored at an IEEE 802.21-based information server.

[Claim 33]

The method of claim 31, wherein the request and the response are transported utilizing at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 34]

The method of claim 31, wherein the neighboring network information contained in the response utilizes an extensible authentication protocol (EAP).

[Claim 35]

The method of claim 31, wherein the request includes an identification of an authentication client requesting the neighboring network information from the authentication server.

[Claim 36]

The method of claim 35, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the authentication client.

[Claim 37]

The method of claim 36, wherein the neighboring network information enables a mobile terminal to perform a hand-off to one or more of the wireless communication networks.

[Claim 38]

A mobility server for retrieving neighboring network information, the mobility server comprising:

a processor configured to:

receive a request generated by an authentication server;
determine neighboring network information requested via the request;

retrieve the neighboring network information based on the request; and

send a response to the request including at least the neighboring network information.

[Claim 39]

The mobility server of claim 38, wherein the neighboring network information is stored at an IEEE 802.21-based information server.

[Claim 40]

The mobility server of claim 38, wherein the request and the

response are transported utilizing at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 41]

The mobility server of claim 38, wherein the neighboring network information contained in the response utilizes an extensible authentication protocol (EAP).

[Claim 42]

The mobility server of claim 38, wherein the request includes an identification of an authentication client requesting the neighboring network information from the authentication server.

[Claim 43]

The mobility server of claim 42, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of the authentication client.

[Claim 44]

The mobility server of claim 43, wherein the neighboring network information enables a mobile terminal to perform a hand-off to one or more of the wireless communication networks.

[Claim 45]

A method performed by a processor for requesting neighboring network information from a device, the method comprising:

- encoding a request for neighboring network information;

- sending the request to a proxy authentication server associated with a wireless local area network to obtain the neighboring network information from a second authentication server at a second network;

- receiving a response to the request, the response generated by the second authentication server;

- decoding the neighboring network information retrieved from the response; and

- storing the decoded neighboring network information.

[Claim 46]

The method of claim 45, wherein said encoding is in accordance with an extensible authentication protocol (EAP).

[Claim 47]

The method of claim 45, wherein the encoding is based on an IEEE

802.21 format.

[Claim 48]

The method of claim 45, wherein the request and the response are transported utilizing at least one of an IEEE 802.1X format or an IEEE 802.11u format.

[Claim 49]

The method of claim 45, wherein the sending of the request to the proxy authentication server is performed by a mobile terminal.

[Claim 50]

The method of claim 49, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of a network access device in communication with the mobile terminal.

[Claim 51]

The method of claim 50, wherein the neighboring network information enables the mobile terminal to perform a hand-off to one or more of the wireless communication networks.

[Claim 52]

The method of claim 45, wherein the request is transported using an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 53]

A mobile terminal for requesting neighboring network information from a device, the mobile terminal comprising:

a processor configured to:

 encode a request for neighboring network information;

 send the request to a proxy authentication server associated with a wireless local area network to obtain the neighboring network information from a second authentication server at a second network;

 receive a response to the request, the response generated by the second authentication server;

 decode the neighboring network information retrieved from the response; and

 store the decoded neighboring network information.

[Claim 54]

The mobile terminal of claim 53, wherein said encoding is in accordance with an extensible authentication protocol (EAP).

[Claim 55]

The mobile terminal of claim 53, wherein the encoding is based on an IEEE 802.21 format.

[Claim 56]

The mobile terminal of claim 53, wherein the request and the response are transported utilizing at least one of an IEEE 802.1X format or an IEEE 802.11u format.

[Claim 57]

The mobile terminal of claim 53, wherein the neighboring network information includes one or more network identifications corresponding to one or more wireless communication networks neighboring or within a coverage region of a network access device in communication with the mobile terminal.

[Claim 58]

The mobile terminal of claim 57, wherein the neighboring network information enables the mobile terminal to perform a hand-off to one or more of the wireless communication networks.

[Claim 59]

The mobile terminal of claim 53, wherein the request is transported using an EAP within at least one of a RADIUS protocol or a DIAMETER protocol.

[Claim 60]

The method of claim 45, wherein the second network is a core network of a public land mobile network.

[Claim 61]

The mobile terminal of claim 53, wherein the second network is a core network of a public land mobile network.