

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
23 October 2008 (23.10.2008)

PCT

(10) International Publication Number
WO 2008/127516 A2

(51) International Patent Classification:
H04Q 7/22 (2006.01)

(21) International Application Number:
PCT/US2008/002739

(22) International Filing Date:
29 February 2008 (29.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/892,747 2 March 2007 (02.03.2007) US
60/892,990 5 March 2007 (05.03.2007) US
60/977,549 4 October 2007 (04.10.2007) US

(71) Applicant (for all designated States except US): **NORTEL NETWORKS LIMITED** [CA/CA]; 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec H4S 2A9 (CA).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MUHANNA,**

Ahmad [US/US]; P.O. Box 851204, Richardson, TX 75085-1204 (US). **SABOORIAN, Tony** [US/US]; 2713 Schofield Ct., Plano, TX 75093 (US). **KHALIL, Mo-hamed** [US/US]; 118 Briar Oak, Murphy, TX 75094 (US).

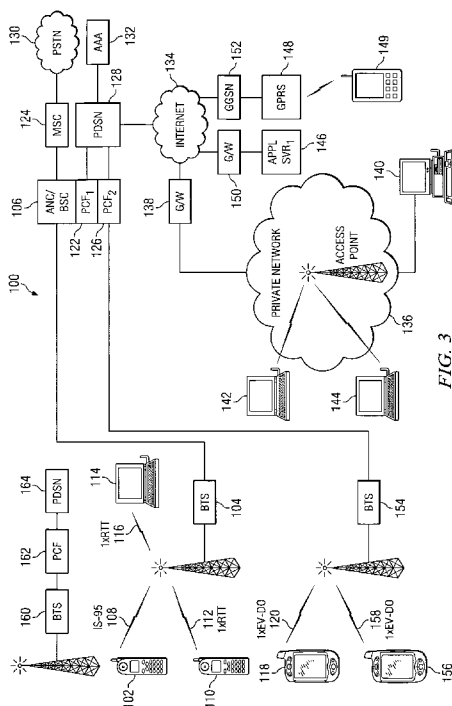
(74) Agent: **HEMINGWAY, Scott, D.**; Hemingway & Hansen, LLP, 1717 Main Street, Comerica Bank Tower, Suite 2500, Dallas, TX 75201 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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,

[Continued on next page]

(54) Title: A MOBILE COMMUNICATION SYSTEM THAT USES SERVING MOBILITY AGENT IDENTIFICATION INFORMATION TO DERIVE ACCESS INFORMATION FOR A MOBILE NODE



(57) Abstract: Packet data serving networks may use different wireless access technology, such as General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), cdma2000, Wireless Local Area Network (WLAN), WiMax, IxEV-DO, I xEV-DV, or other such standards based specification. A wireless local area network technology can also include any one of 802.11 (a), 802.11 (b), 802.11 (g), or Bluetooth. The method and apparatus in accordance with the present invention includes a home mobility anchor receiving a message from a serving mobility agent located on a packet data serving network where the mobile node is located. The present invention relies on the form and content of information packet sent from the serving mobility agent to identify the access technology being used on the packet data serving network. After determining the access technology type used on the packet data serving network, the home mobility anchor takes appropriate actions to authenticate the mobile node user, perform accounting, communicate with a proxy server or an Accounting, Authentication, and Authorization (AAA) server associated with the packet data home network, or perform other necessary actions to process information packets for the mobile node.



ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
- *of inventorship (Rule 4.17(iv))*

Declarations under Rule 4.17:

- *as to the identity of the inventor (Rule 4.17(i))*

Published:

- *without international search report and to be republished upon receipt of that report*

A MOBILE COMMUNICATION SYSTEM THAT USES SERVING MOBILITY
AGENT IDENTIFICATION INFORMATION TO DERIVE ACCESS INFORMATION
FOR A MOBILE NODE

RELATED APPLICATION DATA

[0001] This utility patent application claims the benefit of priority under 35 U.S.C. §119(e) from U.S. Provisional Patent Application Serial Nos. 60/892,747 filed on March 2, 2007, 60/892,990 filed March 5, 2007 and 60/977,549 filed October 4, 2007. The Provisional Patent Applications are also incorporated by reference into this utility patent application.

TECHNICAL FIELD OF THE INVENTION

[0002] A mobile communication protocol and system in a mobile packet based network that derives access information for a mobile node using serving mobility agent identification information.

BACKGROUND OF THE INVENTION

[0003] Present-day Internet communications represent the synthesis of technical developments begun in the 1960s. During that time period, the Defense Department developed a communication system to support communication between different United States military computer networks, and later a similar system was used to support communication between different research computer networks at United States universities.

THE INTERNET

[0004] The Internet grew from research originally performed by the United States Department of Defense. In the 1960s, Defense Department officials wanted to connect different types of military computer networks. These different computer networks could not communicate with each other because they used different types of operating systems or networking protocols.

[0005] While the Defense Department officials wanted a system that would permit communication between these different computer networks, they realized that a centralized interface system would be vulnerable to missile attack and sabotage. To avoid this vulnerability, the Defense Department required the interface system to be decentralized with no vulnerable failure points.

[0006] The Defense Department developed an interface protocol for communication between these different network computers. A few years later, the National Science Foundation (NSF) wanted to connect different types of network computers located at research institutions across the country. The NSF adopted the Defense Department's interface protocol for communication between the research computer networks. Ultimately, this combination of research computer networks would form the foundation of today's Internet.

INTERNET PROTOCOLS

[0007] The Defense Department's interface protocol was called the Internet Protocol (IP) standard. The IP standard now supports communication between computers and networks on the Internet. The IP standard identifies the types of services to be provided to users and specifies the mechanisms needed to support these services. The IP standard also describes the upper and lower system interfaces, defines the services to be provided on these interfaces, and outlines the execution environment for services needed in this system.

[0008] A transmission protocol, called the Transmission Control Protocol (TCP), was developed to provide connection-oriented, end-to-end data transmission between packet-switched computer networks. The combination of TCP with IP (TCP/IP) forms a system or suite of protocols for data transfer and communication between computers on the Internet. The TCP/IP standard has become mandatory for use in all packet switching networks that connect or have the potential for utilizing connectivity across network or sub-network boundaries.

[0009] A computer operating on a network is assigned a unique physical address under the TCP/IP protocols. This is called an IP address. The IP address can include: (1) a network ID and number identifying a network, (2) a sub-network ID number identifying a substructure on the network, and (3) a host ID number identifying a particular computer on the sub-network. A header data field in the information packet will include source and destination addresses. The IP addressing scheme imposes a sensible addressing scheme that reflects the internal organization of the network or sub-network. All information packets transmitted over the Internet will have a set of IP header fields containing this IP address.

[0010] A router is located on a network and is used to regulate the transmission of information packets into and out of computer networks and within sub-networks. A router interprets the logical address of an information packet and directs the information packet to its intended destination. Information packets addressed between computers on the sub-network do not pass through the router to the greater network, and as such, these sub-network information packets will not clutter the transmission lines of the greater network. If an information packet is addressed to a computer outside the sub-network, the router forwards the packet onto the greater network.

[0011] The TCP/IP network includes protocols that define how routers will determine the transmittal path for data through the network. Routing decisions are based upon information in the IP header and entries maintained in a routing table. A routing table possesses information for a router to determine whether to accept the communicated information packet on behalf of a destination computer or pass the information packet onto another router in the network or sub-network. The routing table's address data enables the router to accurately forward the information packets.

[0012] The routing table can be configured manually with routing table entries or with a dynamic routing protocol. In a dynamic routing protocol, routers update routing information with periodic information packet transmissions to other routers on the network. This process sometimes involves a process called advertising. The dynamic routing protocol accommodates changing network topologies, such as the network architecture, network structure, layout of routers, and interconnection between hosts and routers. Internet Control Message Protocol (ICMP) information packets are used to update routing tables with this changing system topology.

THE IP-BASED MOBILITY SYSTEM

[0013] The Internet protocols were originally developed with an assumption that Internet users would be connected to a single, fixed network. With the advent of portable computers and cellular wireless communication systems, Internet users and their computers began to move within a network and across network boundaries. Because of this highly mobile Internet usage, the implicit design assumption of the Internet protocols (e.g. that a user would be located at a fixed, static physical location) needed to be addressed and revised.

[0014] In an IP-based mobile communication system, the mobile communication device (e.g. cellular phone, pager, computer, etc.) is called a mobile node. Different communications protocols may refer to similar mobile node devices by different names depending on the nomenclature adopted for that system. The mobile node may also be referred to as a mobile terminal or user equipment. A mobile node is connected to a packet data home network through a home mobility anchor. The packet data home network (PDHN) can also be called a home network or connectivity services network (CSN), and the home mobility anchor is also known as home agent, local mobility agent (LMA), packet data network gateway (PDN-GW).

[0015] The mobile node can move to another network located outside the packet data home network, and this outside network is called a packet data serving network (PDSN). The packet data serving network can also be called the foreign network or serving network. The connectivity of the mobile node to the home mobility anchor should be maintained even when the mobile node is attached to the packet data serving network, and this connectivity is supported by the serving mobility agent. The serving mobility agent is also known as the foreign agent, mobile access gateway (MAG), serving gateway (S-GW), access server network gateway (ASNGW), or high rate packet data (HRPD) serving gateway (HSGW).

[0016] A mobile node may change its point of attachment to the packet data home network by changing packet data serving networks. As the mobile node moves from one packet data serving network to another packet data serving network, there is a need to maintain the mobile node's connectivity to its packet data home network. The mobile node will always be

associated with its packet data home network and sub-network for IP addressing purposes. A correspondent node may send information packets to the mobile node at the packet data home network, and these information packets will need to be routed to the mobile node by routers located on the home and packet data serving network.

MOBILE NODE MOVEMENT AND IP MOBILITY CARE-OF ADDRESSING

[0017] In an IP-based mobile communications system, the mobile node changes its point of attachment to the networks while maintaining network connectivity to the packet data home network. Each mobile node possesses an associated home mobility anchor on a packet data home network used to route information packets to the remotely located mobile node. Registration and hand-off protocols are used to maintain connectivity between the mobile node and home mobility anchor. Extensions have been defined in the IP protocol, and extensions can be used in similar protocols, to support transmission of variable amounts of data in an information packet. This includes address information for mobile nodes, routers, and networks.

[0018] In a mobile IP network, a mobile node on the packet data serving network will be assigned a care-of address that will be used to route information packets to the packet data serving network and the attached mobile node. In some systems, an advertisement from a router on the packet data serving network will inform a mobile node that is attached to a packet data serving network. The mobile node location will typically be indicated by a care-of address on the packet data serving network, and the care-of address is transmitted to its packet data home network in an information packet to register it.

[0019] When a mobile node travels outside its home administrative domain, however, the mobile node may need to communicate through multiple domains in order to maintain network connectivity with its packet data home network. Different packet data serving networks may use different communication protocols and different communication access technology. During the formative years since the Internet was first established, Internet Protocol version 4 (IPv4) was recognized and adopted as the standard version of the Internet Protocol. With the advent of mobile IP and proliferation of computers and computer systems linked to the Internet, various limitations in the IPv4 standard and associated procedures have developed and emerged. In response, new standards have evolved or are emerging, such as MIPv4, PMIPv4, IPv6, MIPv6, and PMIPv6. The packet data serving networks may also use different wireless access technology, such as General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), cdma2000, Wireless Local Area Network (WLAN), WiMax, 1xEV-DO, 1xEV-DV, or other such standards based specification. A wireless local area network technology can include any one of 802.11(a), 802.11(b), 802.11(g), or Bluetooth.

[0020] One problem that currently exists is the need to identify the wireless access technology used on a packet data serving network where the mobile node is located. All prior

methods of identifying the wireless access technology for the packet data serving network are deemed to lack robustness, involve the mobile node in the identification process, or are considered largely non-functional for their intended purpose. For instance, one solution proposes the recognition of a specific care-of address, and the correlation of that specific address with an associated access type. This solution is not scalable, and would require the constant updating of care-of address tables and their associated access type. Another solution is the use a AAA database information on the packet data home network to determine access type, which is a very slow solution because the home mobility anchor has to wait for the AAA server to determine access type from limited information. This solution increases delays and sometimes results in inaccurate information. Another solution involves adjusting or amending the NAI extensions to indicate access type or using an authentication extension to indicate access type. Both of these solutions are not acceptable because amending the NAI extension is not recommended and there is no requirement that the authentication extensions be used to identify access type, which would result in inconsistent use and analysis of this extension. Accordingly, a need exists for enabling a home mobility anchor to determine access technology based on the content or form of information sent by the serving mobility agent so as to determine the communication access type being used on the packet data serving network.

SUMMARY OF THE INVENTION

[0021] Many different protocols can govern the transmission of information on a home or packet data serving network, such as IPv4, MIPv4, PMIPv4, IPv6, MIPv6, and PMIPv6. The packet data serving networks may use different wireless access technology, such as General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), cdma2000, Wireless Local Area Network (WLAN), WiMax, 1xEV-DO, 1xEV-DV, or other such standards based specification. A wireless local area network technology can also include any one of 802.11(a), 802.11(b), 802.11(g), or Bluetooth.

[0022] The method and apparatus in accordance with the present invention includes a home mobility anchor receiving a message from a serving mobility agent located on a packet data serving network where the mobile node is located. The present invention relies on the form and content of information packet sent from the serving mobility agent to identify the access technology being used on the packet data serving network. That communication from the serving mobility agent is used to facilitate the home mobility anchor becoming aware of the access technology being used on the packet data serving network, so that appropriate actions can be taken to authenticate the mobile node user, perform accounting, communicate with a proxy server or an Accounting, Authentication, and Authorization (AAA) server associated with the packet data home network, or perform other necessary actions to process information packets for the mobile node.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The objects and features of the invention will become more readily understood from the following detailed description and appended claims when read in conjunction with the accompanying drawings in which like numerals represent like elements and in which:

[0024] FIG. 1 is a functional block diagram for a communication network that supports the preferred embodiments of the present invention;

[0025] FIG. 2 is a functional block diagram of a serving mobility agent shown in Figure 1; and,

[0026] FIG. 3 is a functional block diagram that illustrates some of the access types that may be used in conjunction with a communication network that supports the preferred embodiments of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0027] FIG. 1 is a functional block diagram that illustrates the functional components for a communication network supporting the preferred embodiments of the present invention. More specifically, a mobile node 10 registers with serving mobility agent 4, which sends a registration message to the home mobility anchor 8 by way of Internet 28. As part of the registration process, the form and content of the registration message from serving mobility agent 4 identifies the access type used on the network servicing the mobile node 10. The home mobility anchor 8 identifies the access type being used on the packet data serving network based on this information, and the home mobility anchor 8 uses that access type information to perform various authentication, authorization and accounting functions in cooperation with the home AAA server 12 and the home network 24. Also, the home mobility anchor 8 may format the information packets being forwarded to the mobile node 10 in a particular manner based on the access type being used on the packet data serving network.

[0028] Home AAA server 12 may also specify subscriber profile based routing policy based at least in part on access technology. Information stored in home AAA server 12 may be accessed by home mobility anchor 8 during registration. Home mobility anchor 8 and serving mobility agent 4 each have an associated access router contained therein, and the home mobility anchor 8 and serving mobility agent 4 may cooperate in using the information to identify the access technology used on the packet data serving network.

[0029] FIG. 2 is a functional block diagram of a serving mobility agent 40 that illustrates a serving mobility agent 4 depicted in Figure 1. The functional block diagram in Figure 2 can also describe the functional aspects of the home mobility anchor 8 shown in Figure 1. Serving mobility agent 40 includes a processor 42 that is coupled to communicate over a bus 44. A memory 46 further is coupled to bus 44 and is for storing computer instructions that define the operational logic of serving mobility agent 40. Memory 46 specifically includes computer

instructions to cause serving mobility agent 40 to add information indicative of access technology type to registration request messages sent to the home mobility anchor 8 shown in Figure 1. Bus 44 further is coupled to a bus controller 41, which controls the communications and timing of communications thereon. Bus controller 41 is further coupled to a network port 52 that enables serving mobility agent 40 to communicate with a mobile IP network. Network port 52 can be one of any type of transceiver front end, including those used in wireless as well as wireline technologies. Like components would correspond to the functional aspects of the home mobility anchor 8 shown in Figure 1.

[0030] In operation, processor 42 communicates with memory 46 by way of bus 44 to retrieve computer instructions stored therein and to execute the computer instructions to operate according to the logic defined within the computer instructions of memory 46. Memory 46 specifically includes computer instructions that define the logic for performing registration of a mobile node. As incorporated in the home mobility anchor 8 (Fig. 1) functionality, computer instructions stored in memory 46 define logic for determining an access technology based on the content and form of the information packet received from the serving mobility agent 4.

[0031] FIG. 3 is a functional block diagram that illustrates access types that may be used in conjunction with a communication network supporting the preferred embodiments of the present invention. As may be seen, a communication network 100 includes many networks that are coupled to operatively communicate with each other, which enables a user in one type of network to communicate with a user in a different type of network. For example, the communication network 100 supports the ability of a mobile node to communicate through a wireless communication link to a packet data serving network back to its packet data home network. Many different protocols can be utilized by a home or packet data serving network, such as IPv4, MIPv4, PMIPv4, IPv6, MIPv6, and PMIPv6. The packet data serving networks may use different wireless access technology, such as General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), cdma2000, Wireless Local Area Network (WLAN), WiMax, 1xEV-DO, 1xEV-DV, or other such standards based specification. A wireless local area network technology can also include any one of 802.11(a), 802.11(b), 802.11(g), or Bluetooth.

[0032] As shown in Figure 3, a mobile node 102 is located within a geographic area served by a Base Transceiver Station (BTS) 104 that is coupled to an Access Network Controller (ANC)/Base Station Controller (BSC) 106. More specifically, mobile node 102 communicates with BTS 104 by way of an IS-95 CDMA wireless communication network link shown generally at 108. Similarly, a mobile node 110 that is capable of supporting both voice and data calls communicates with BTS 104 over a wireless communication link shown generally at 112 and establishes either voice calls or data calls under cdma2000 1xRTT protocols. In the example

herein, mobile node 110 is engaged in a voice call, as defined by a service option generated by a mobile node during call setup, and thus wireless communication link 112 is transmitting merely voice signals and associated control signaling.

[0033] Similarly, a mobile node 114 is engaged in a data call (data session) according to 1xRTT protocols over a wireless communication link shown generally at 116. Finally, an access terminal 118 is engaged in a data session over a wireless communication link, shown generally at 120, according to 1xEV-DO protocols in a so called "simple-IP" or "mobile-IP" network. In general, simple-IP and mobile-IP networks do not include control-signaling protocols that are as extensive as some existing systems including 1xRTT.

[0034] Further, BTS 104 is generally coupled to communicate with ANC/BSC 106 (or with packet control function cards there within). Access network controllers and base station controllers have similar functionality. Moreover, Packet Control Function (PCF) cards can be installed either within a BSC or within an ANC according to whether the PCF is to communicate with a 1xRTT device or a 1xEV-DO device, respectively. It is to be understood that the BSC and ANC elements may readily be formed as stand alone units, but are shown herein as combined systems for illustration.

[0035] Within ANC/BSC 106, a plurality of different wireless network cards is included to facilitate communications with mobile nodes and mobile nodes of differing protocols and types. For example, in the described embodiment, ANC/BSC 106 includes circuitry to communicate with mobile node 102 over IS-95 CDMA wireless communication network link as shown generally at 108. ANC/BSC 106 further includes a PCF 122 for communicating with mobile nodes 110 and 114 utilizing 1xRTT protocols. As may be seen, PCF 122, which is for communicating with 1xRTT protocol devices, is coupled to a Mobile Switching Center (MSC) 124. A PCF 126, however, is for communicating with 1xEV-DO devices and thus it is coupled directly to a Packet Data Serving Node (PDSN) 128. Thus, access terminal 118 that communicates over wireless communication link 120 according to 1xEV-DO communication protocols, communicates with BTS 154 and with PCF 126 formed within ANC/BSC 106. It is understood, of course, that PCF 126 may readily be formed as a distinct device rather than within a rack of ANC/BSC 106. Moreover, PCF 126 may communicate with access terminal 118 through distinct radio equipment and, thus, through a BTS other than BTS 154 as shown herein.

[0036] MSC 124 further is coupled to a Public Switched Telephone Network (PSTN) 130. Accordingly, calls routed through MSC 124 are directed either to other MSCs (not shown herein) or to external networks by way of PSTN 130. The reference to PSTN herein includes SS7 and other similar "intelligent networks". 1xRTT data and 1xEV-DO calls, which are processed by PCF 126, however, are forwarded through PDSN 128, which, upon authentication by an Authentication, Authorization and Accounting (AAA) server 132, is connected to a data packet

network, which, in this example, comprises Internet 134. As may further be seen, Internet 134 is coupled to a private network 136 by way of a gateway device 138. Private network 136 further is coupled through traditional wire line networks to a user terminal 140.

[0037] Private network 136 is further coupled to mobile nodes 142 and 144 through a wireless network. In one embodiment, private network 136 comprises a wireless local area network with at least one access point which provides access for mobile nodes 142 and 144 and comprises wireless LAN terminals. Private network 136 can include home mobility anchors and serving mobility agents for mobile nodes 142 and 144. Alternatively, a PDSN, such as PDSN 128 or a Gateway GPRS Support Node (GGSN), such as GGSN 152 of a General Packet Radio Service (GPRS) network, may serve as a serving mobility agent or home mobility anchor.

[0038] In this application, the packet data home network is not restricted to any one communication standard, and it can also be called a connectivity services network (CSN). The home mobility anchor (HMA) is also known as a home agent, a local mobility agent (LMA), packet data network gateway (PDN-GW). The mobile node can move to another network outside the packet data home network, and onto a packet data serving network, foreign network or serving network. The serving mobility agent is also known as a foreign agent, mobile access gateway (MAG), serving gateway (S-GW), access server network gateway (ASNGW), or high rate packet data (HRPD) serving gateway (HSGW).

[0039] Internet 134 further is coupled to application server 146 by way of gateway device 150. A Global System for Mobile Communications (GSM) mobile node 149 is coupled to Internet 134 by way of GPRS network 148. GPRS network 148 represents the GPRS architecture, such as base station controller, mobile switching center, and serving support nodes. GGSN 152 is the interface between Internet 134 and GPRS network 148.

[0040] Referring to FIG. 3, ANC/BSC 106 further is coupled to BTS 154, which is in communication with an access terminal 156 by way of a 1xEV-DO communication link 158. As may be seen, access terminal 156 is served by PCF 126, as is access terminal 118. Additionally, a BTS 160 is coupled to a PCF 162 that, in turn, is coupled to communicate with a PDSN 164. Thus, a mobile node, such as mobile node 102, may communicate with BTS 160, BTS 104, or both. PCF 162, as may be seen, is a standalone system rather than being integrated as a card in an ANC or a BSC.

[0041] For each mobile node or access terminal on prior art systems, such as mobile nodes 118 and 156, that becomes coupled to Internet 134 or private network 136 by way of a home mobility anchor or serving mobility agent, the home mobility anchor is not currently able to determine the access technology used on the packet data serving network supporting mobile nodes 118 and 156 in an efficient manner based on the information sent to it from the serving mobility agent (SMA) associated with that packet data serving network. Without knowing the

type of access technology used on the packet data serving network to support communications with the mobile node, the home mobility anchor cannot effectively and efficiently perform various authentication, accounting and authorization functions, as well as configure out-going packets into a format that is compatible with the packet data serving network access technology. The present invention provides a more efficient and effective means of determining the wireless access technology used by the mobile node on the packet data serving network based on the content or form of an information packet sent to the home mobility anchor from the serving mobility agent.

[0042] As will be described in greater detail below, any one of the mobile nodes or access terminals may communicate with a device by way of Internet 134 through a home mobility anchor (HMA) or a serving mobility agent (SMA) depending on the Internet access point. In the described embodiment, the mobile node that is not within the service area of the HMA will register directly with the HMA through the SMA. The HMA will determine communication access type based on the information packet received from the serving mobility agent (SMA), which access type information will be used to perform AAA activities (authentication, authorization and accounting) or to perform required formatting of the transmission packets sent to or received from the mobile node.

[0043] For example, once the access technology is determined by the home mobility anchor, the home mobility anchor can provide this information in the billing records for a particular service that is being requested and even determine whether the requested access is allowed for the device type and/or the access technology. For example, if the device type is a PDA, then according to the type of PDA, it may not be feasible to provide streaming video thereto because the communication link with the PDA cannot support the throughput rates that are required therefor. Accounting, authentication and authorization activities can also be performed with this access technology information.

[0044] A first preferred embodiment of the present invention relates the situation where the serving mobility agent 4 serves only one access type, but it could have multiple care-of addresses. Referring back to Fig. 1, the invention in the present embodiment is initiated when the serving mobility agent 4 receives a registration request message from the mobile node 10, which is meant to be forwarded to the home mobility anchor 8. The serving mobility agent 4 attaches and adds its identity information to the registration request message before transmitting it to the home mobility anchor 8. The identity information appended to the registration request message will also identify to the home mobility anchor 8 the access type information for the communication type used on the packet data serving network. The identity information may also identify the operator information for the serving mobility agent 4. In order for this first

embodiment to be performed, a security association may need to have been established between the home mobility anchor 8 and the serving mobility agent 4.

[0045] After the home mobility anchor 8 receives the registration request message from the serving mobility agent 4, the home mobility anchor 8 will verify and validate the registration request. The home mobility anchor 8 will also tag the traffic coming from care of address for the serving mobility agent 4 with the access type reflected in the identity information provided by the serving mobility agent 4 in the registration request message. The home mobility anchor 8 may confirm the identity information in a registration response message to the serving mobility agent 4 to confirm successful association of the care of address to the access type reflected in the serving mobility agent's 4 identity information. This process can be accomplished every time a registration request is received for the care-of address of the serving mobility agent 4, or the home mobility anchor 8 may conduct this process once as long as the serving mobility agent 4 continues to use the care-of address and service the same access type.

[0046] A second preferred embodiment of the present invention relates the situation where the serving mobility agent 4 serves only one access type and could have multiple care-of addresses, and a security tunnel is established between the serving mobility agent 4 and the home mobility anchor 8. Referring back to Fig. 1, the security tunnel would be established across the Internet 28 connection to support a private communication across a public network. The invention in the present embodiment arises when the serving mobility agent 4 receives a registration request message from the mobile node 10, which is meant to be forwarded to the home mobility anchor 8.

[0047] The serving mobility agent 4, based on operator policy and configuration, will start establishing a security tunnel with the home mobility anchor 8. During the initial negotiation process used to establish the security tunnel, the serving mobility agent 4 communicates its identity to the home mobility anchor 8. The identity information will be used on the security tunnel to direct secure communications to the serving mobility agent 4.

[0048] During the establishment of the security tunnel, the home mobility anchor 8 will tag the traffic on the security tunnel with the access type reflected in the identity information provided by the serving mobility agent 4. The security tunnel will be tagged with the access type, and any traffic arriving on that security tunnel to the home mobility anchor 8 will be considered as arriving from the same access type identified by the serving mobility agent 4 identity information.

[0049] After the security tunnel is established, a registration request may be sent to the home mobility anchor 8 over that tunnel. The home mobility anchor 8 will receive the registration request over the security tunnel, and it will tag that request as originating from the associated access type on the packet data serving network. After receiving the registration

request, the home mobility anchor 8 will execute all functionalities that need to be performed for that access type. The home mobility anchor 8 may confirm the access type in a registration response message to the serving mobility agent 4 to confirm successful association of the access type reflected in the serving mobility agent's 4 identity information.

[0050] A third preferred embodiment of the present invention relates the situation where the serving mobility agent 4 serves only one access type, but it could have multiple care-of addresses. Referring back to Fig. 1, the invention in the present embodiment arises when the serving mobility agent 4 advertises its presence and services to the mobile nodes 10 on the packet data serving network. This advertisement can be in the form regulated by the MIPv4 standard and any other specific Standards Designating Organization.

[0051] The serving mobility agent 4 includes its identity information in the advertisement message as transmitted to the mobile node 10. The mobile node 10 receives the advertisement from the serving mobility agent 4, and the mobile node includes the serving mobility agent 4 identity information in a registration request message sent back to the serving mobility agent 4. The identity information is positioned after all the extensions in the standard transmission packet format, but before any authorization enabling extension.

[0052] The registration request is received by the serving mobility agent 4, and the serving mobility agent 4 confirms the accuracy of its identity information included in the registration request message. The identity information appended to the registration request message will be forwarded to the home mobility anchor 8, and the identity information will identify to the home mobility anchor 8 the access type information for the communication type used on the packet data serving network. The identity information may also identify the operator information for the serving mobility agent 4. In order for this third embodiment to be performed, a security association may need to have been established between the home mobility anchor 8 and the serving mobility agent 4.

[0053] After the home mobility anchor 8 receives the registration request message from the serving mobility agent 4, the home mobility anchor 8 will verify and validate the registration request. The home mobility anchor 8 will also tag the traffic coming from care of address for the serving mobility agent 4 with the access type reflected in the identity information provided by the serving mobility agent 4 in the registration request message. The home mobility anchor 8 may confirm the identity information in a registration response message to the serving mobility agent 4 to confirm successful association of the care of address to the access type reflected in the serving mobility agent's 4 identity information. This process need only be accomplished on the initial registration of the mobile node, and it need not be accomplished with every time a re-registration request is received for the care-of address of the serving mobility

agent 4. After receiving the registration request, the home mobility anchor 8 will execute all functionalities that need to be performed for that access type.

[0054] Where the packet data serving network is serving more than one communication access type, the three embodiments can be used to solve the same problem. Each of the above embodiments can be modified in that context to allow the serving mobility agent 4 so select from different identity information designations depending on the access type needed to be designated. Certain identity information is associated with certain access types, and other identity information is associated with other access types. As such, when the serving mobility agent 4 appended identity information to the registration request (embodiment 1), the security tunnel negotiation (embodiment 2), or the advertisement information (embodiment 3), the serving mobility agent 4 selects from multiple identity information to append to packets depending on the access type that needs to be designated. In the advertisement embodiment, the identity information is also included with matching care-of and access type information.

[0055] There is also the possibility that an additional field could be added to a home network prefix information packet to designate by code or alphanumeric characters the access type being used on the packet data serving network. The designated code may be an eight bit code with 00 designating a reserved access type, 01 designating an LTE access type, and 02 designating a CDMA access type. This home network prefix option would be useful in PMIPv6, when the home mobility anchor 8 receives a binding update message from the serving mobility agent 4 with the access type designated in the home network prefix contained in that communication. The serving mobility agent 4 may always indicate the same home network prefix to the home mobility anchor 8 to similar access types used on the packet data serving network. The designation of "00" may also be used to indicate to the home mobility anchor 8 that the prior access type designation should be used in future communications.

[0056] When a different access type is included in the home network prefix than that already reflected in prior communications, the home mobility agent 8 will allocate a new technology access type designation for that associated mobile node. The new designation can be used for an inter-technology hand-off using the virtual interface at the IPv6 host. With the identification of a new access type, the home mobility agent 8 can perform all necessary functionalities described above.

[0057] Additionally, a unique security parameter index (SPI) can be assigned and associated with particular access types. This solution is useful when the system is using IPv4 and MIPv4 protocols. A registration request is received by the home mobility anchor 8 from the serving mobility agent 4 with SPI information appended thereto, and the SPI information is uniquely associated with a particular access technology. The SPI information is detected by the

home mobility anchor 8, which uses the access type information detected in that communication to perform all necessary functionalities described above.

[0058] While the invention has been particularly shown and described with respect to preferred embodiments, it will be readily understood that minor changes in the details of the invention may be made without departing from the spirit of the invention. Having described the invention, we claim:

Claims:

1. A communication system, comprising:
a packet data home network operating a mobile internet communication protocol having a home mobility anchor;
a communication link to said home mobility anchor, said link receiving communications containing identity information for a packet data serving network supporting communication to a mobile node located on said serving network; said home mobility anchor using said identity information to determine a communication access type used on said packet data serving network to support communications to and from said mobile node.
2. The communication system of Claim 1, wherein said communications containing identity information are registration requests sent to the home mobility anchor.
3. The communication system of Claim 2, wherein said communications containing identity information are responded to by the home mobility anchor with a registration response.
4. The communication system of Claim 1, wherein said communications containing identity information are security tunnel negotiation requests sent to the home mobility anchor.
5. The communication system of Claim 4, wherein said communications containing identity information are responded to by the home mobility anchor with a response.
6. The communication system of Claim 1, wherein said communications containing identity information are part of agent advertisements sent to the home mobility anchor.
7. The communication system of Claim 6, wherein said communications containing identity information are responded to by the home mobility anchor with a response.
8. The communication system of Claim 1, wherein said communications containing identity information possess specific identity information that correlates with one of a plurality of different access types used to communicate to mobile nodes on the packet data serving network.
9. The communication system of Claim 1, wherein said communications containing identity information include an information packet having a network prefix identifier.

10. A communication system, comprising:
 - a packet data serving network operating a mobile internet communication protocol and having a serving mobility agent;
 - a communication link to a mobile node located on said packet data serving network, wherein communications to said mobile node are supported by a communication access type, and said serving mobility agent transmits identity information to a home mobility anchor that uses the identity information to determine the access type supporting communications to and from the mobile node.
11. The communication system of Claim 10, wherein said identity information is transmitted to the home mobility anchor in a registration request.
12. The communication system of Claim 10, wherein said identity information is transmitted to the home mobility anchor in security tunnel negotiation request.
13. The communication system of Claim 10, wherein said identity information is transmitted to the home mobility anchor as part of an agent advertisement.
14. The communication system of Claim 10, wherein said identity information correlates with one of a plurality of different access types used to communicate to mobile nodes on the packet data serving network.
15. The communication system of Claim 10, wherein said identity information is included in an information packet having a network prefix identifier.
16. A method for supporting communication on a communication system, comprising:
 - providing a packet data serving network operating a mobile internet communication protocol and having a serving mobility agent coupled to a mobile node located on the packet data serving network, where communications to and from said mobile node are supported by at least one communication access type used on the packet data serving network;
 - establishing a communication link between the serving mobility agent and a home mobility anchor located on a packet data home network;
 - transmitting a communication to the home mobility anchor from the serving mobility agent containing identity information related to the serving mobility agent; and,

determining at the home mobility anchor the communication access type supported on the packet data serving network based on the identity information transmitted from the serving mobility agent.

17. The communication system of Claim 16, wherein said identity information is transmitted to the home mobility anchor in a registration request.

18. The communication system of Claim 16, wherein said identity information is transmitted to the home mobility anchor in security tunnel negotiation request.

19. The communication system of Claim 16, wherein said identity information is transmitted to the home mobility anchor as part of an agent advertisement.

20. The communication system of Claim 16, wherein said identity information correlates with one of a plurality of different access types used to communicate to mobile nodes on the packet data serving network.

21. The communication system of Claim 16, wherein said identity information is included in an information packet having a network prefix identifier.

1/2

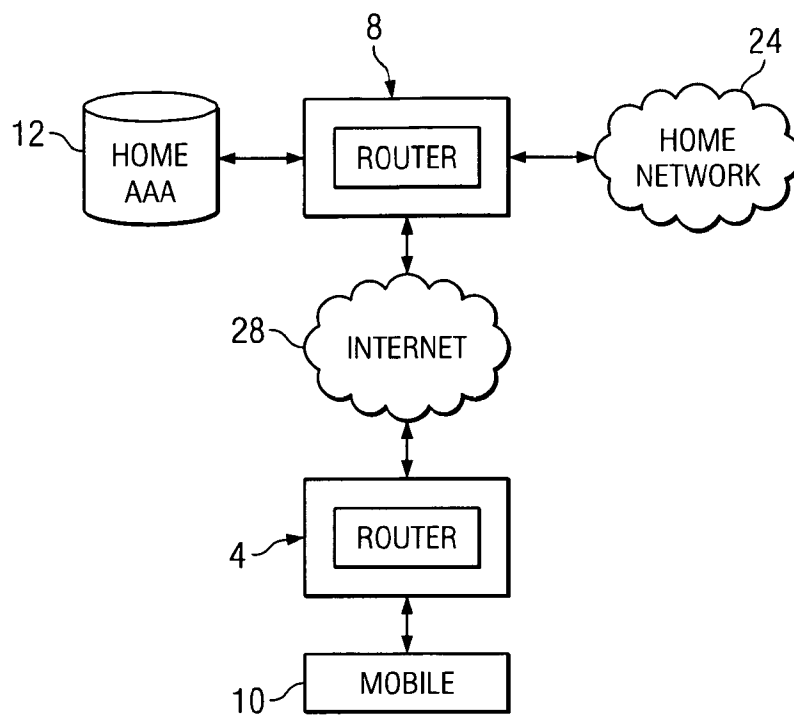


FIG. 1

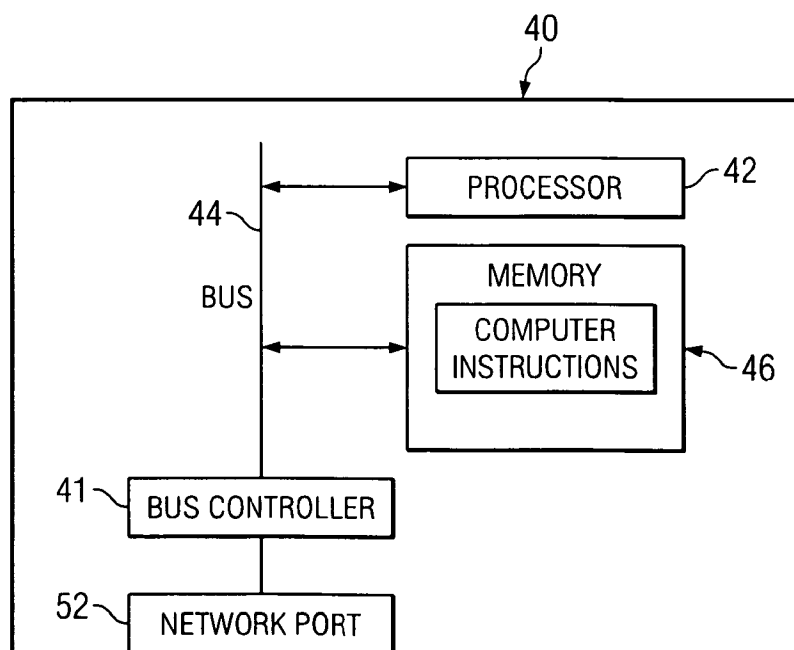


FIG. 2

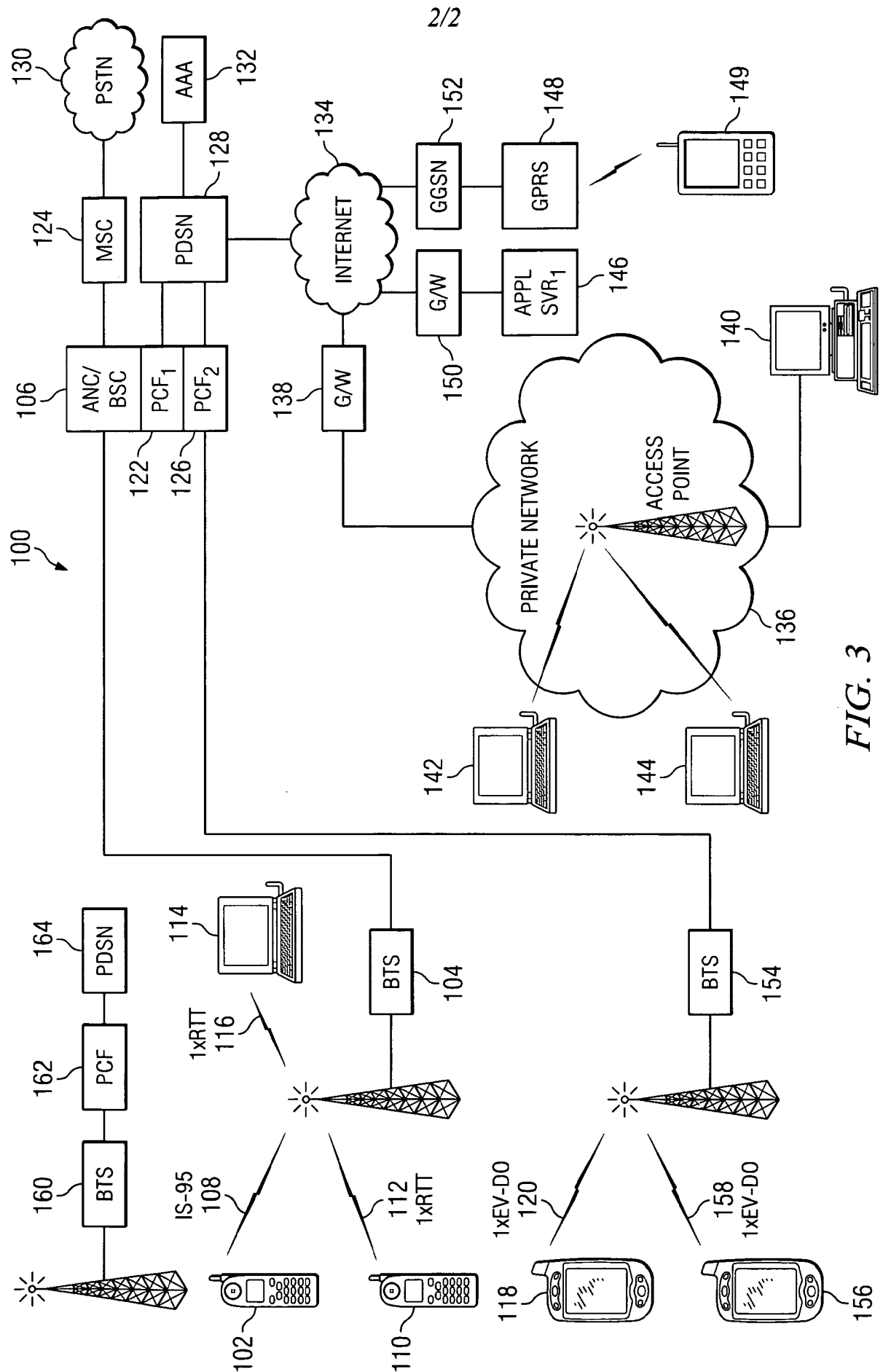


FIG. 3