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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2007 (13.09.2007)

PCT

(10) International Publication Number
WO 2007/103504 A2

(51) International Patent Classification:
H04K 1/00 (2006.01)

(21) International Application Number:
PCT/US2007/005937

(22) International Filing Date: 6 March 2007 (06.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/780,176 6 March 2006 (06.03.2006) US

(71) Applicant *(for all designated States except US)*: **CISCO TECHNOLOGY, INC.** [US/US]; 170 West Tasman Drive, San Jose, CA 95134 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **IYER, Jayaraman, R.** [IN/US]; 1674 Hollenbeck Avenue, Apartment 51, Sunnyvale, CA 94087 (US). **LEUNG, Kent, K.** [US/US]; 625 Jay Street, Los Altos, CA 94022 (US). **STAMMERS, Timothy, P.** [GB/US]; 4309 Oak Park Road, Raleigh, NC 27612 (US). **OSWAL, Anand, K.** [IN/US]; 400 River Side Court, Apt. 114, Santa Clara, CA 95054 (US).

(74) Agent: **THOMAS, Travis, W.**; Baker Botts L.L.P., 2001 Ross Avenue, Suite 600, Dallas, TX 75201 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** ACCESS TERMINAL FOR COMMUNICATING PACKETS USING A HOME ANCHORED BEARER PATH OR A VISITED ANCHORED BEARER PATH

(57) **Abstract:** Communicating packets along a bearer path includes receiving a home network address and a visited network address at an access terminal. The home network address corresponds to a home anchored bearer path anchored at a home network of the access terminal. The visited network address corresponds to a visited anchored bearer path anchored at a visited network. The access terminal determines whether to use the home anchored bearer path or the visited anchored bearer path, and communicates packets using the home network address or the visited network address in accordance with the determination.

WO 2007/103504 A2

ACCESS TERMINAL FOR COMMUNICATING PACKETS USING A HOME ANCHORED BEARER PATH OR A VISITED ANCHORED BEARER PATH

TECHNICAL FIELD

This invention relates generally to the field of telecommunications and more specifically to an access terminal for communicating packets using a home anchored bearer path or a visited anchored bearer path.

BACKGROUND

An endpoint, such as an access terminal, may use a system of communication networks to communicate packets with other endpoints. For example, an access terminal may subscribe to a home network that maintains subscription information for the access terminal. If the access terminal is outside of the serving area of the home network, the access terminal may use a visited network to communicate packets.

Certain known techniques may be used to route packets between endpoints and through networks. These known techniques, however, are not efficient in certain situations. In certain situations, it is generally desirable to be efficient.

SUMMARY OF THE DISCLOSURE

In accordance with the present invention, disadvantages and problems associated with previous

techniques for communicating packets may be reduced or eliminated.

According to one embodiment of the present invention, communicating packets along a bearer path includes receiving a home network address and a visited network address at an access terminal. The home network address corresponds to a home anchored bearer path anchored at a home network of the access terminal. The visited network address corresponds to a visited anchored bearer path anchored at a visited network. The access terminal determines whether to use the home anchored bearer path or the visited anchored bearer path, and communicates packets using the home network address or the visited network address in accordance with the determination.

Certain embodiments of the invention may provide one or more technical advantages. A technical advantage of one embodiment may be that packets from an access terminal can be communicated along a home anchored path or a visited anchored path. The home anchored path includes a home bearer manager of a home network and may include a visited bearer manager of a visited network. The visited anchored path includes the visited bearer manager, but not the home bearer manager.

Another technical advantage of one embodiment may be that the access terminal can be provided with a home network address and a visited network address. The home network address may be used to communicate packets along the home anchored path, and the visited network address may be used to communicate packets along the visited anchored path.

Another technical advantage of one embodiment may be that a home policy server of the home network may provide

policy rules to a visited policy server of the visited network. The policy rules may be used to enforce policies for packets sent along the visited anchored path.

Certain embodiments of the invention may include none, some, or all of the above technical advantages. One or more other technical advantages may be readily apparent to one skilled in the art from the figures, descriptions, and claims included herein.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its features and advantages, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

FIGURE 1 illustrates one embodiment of a system that communicates packets for an access terminal;

FIGURE 2 illustrates examples of bearer paths of the system of FIGURE 1;

FIGURE 3 illustrates one embodiment of a method for sending packets using either a home network address or a visited network address;

FIGURE 4 illustrates one embodiment of a method for establishing a point-to-point session that may be used by the system of FIGURE 1; and

FIGURE 5 illustrates one embodiment of a method for establishing a mobile Internet Protocol (IP) session that may be used by the system of FIGURE 1.

DETAILED DESCRIPTION OF THE DRAWINGS

Embodiments of the present invention and its advantages are best understood by referring to FIGURES 1

through 5 of the drawings, like numerals being used for like and corresponding parts of the various drawings.

FIGURE 1 illustrates one embodiment of a system 10 that communicates packets for an access terminal 20. According to the embodiment, packets from access terminal 20 can be communicated along a home anchored path or a visited anchored path. The home anchored path includes a home bearer manager 40b of a home network 28 of access terminal 20 and a visited bearer manager 40a of a visited network 24. The visited anchored path includes visited bearer manager 40a, but not home bearer manager 40b. In the embodiment, access terminal 20 can be provided with a home network address (H-NA) and a visited network address (V-NA). The home network address may be used to communicate packets along the home anchored path, and the visited network address may be used to communicate packets along the visited anchored path.

According to the illustrated embodiment, system 10 provides services such as communication sessions to endpoints such as access terminal 20. A communication session refers to an active communication between endpoints. Information may be communicated during a communication session. Information may refer to voice, data, text, audio, video, multimedia, control, signaling, other information, or any combination of any of the preceding. Information may be communicated in packets. A packet may comprise a bundle of data organized in a specific way for transmission.

System 10 may utilize communication protocols and technologies to provide the communication sessions. Examples of communication protocols and technologies include those set by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) 822.xx standards, the

International Telecommunications Union (ITU-T) standards, the European Telecommunications Standards Institute (ETSI) standards (for example, General Packet Radio Services (GPRS)), the Internet Engineering Task Force (IETF) standards (for example, IP such as mobile IP), or other standards.

According to the illustrated embodiment, system 10 includes access terminals 20. Access terminal 20 represents any suitable device operable to communicate with a communication network. Access terminal 20 may comprise, for example, a personal digital assistant, a computer such as a laptop, a cellular telephone, a mobile handset, or any other device operable to communicate with system 10. Access terminal 20 may support any suitable protocol, for example, simple IP and/or mobile IP.

System 10 also includes communication networks such as a visited network 24 and a home network 28. In general, a communication network may comprise at least a portion of a public switched telephone network (PSTN), a public or private data network, a local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), a local, regional, or global communication or computer network such as the Internet, a wireline or wireless network, an enterprise intranet, other suitable communication link, or any combination of the preceding.

In the illustrated embodiment, visited network 24 represents a communication network that facilitates a communication session for access terminal 20 within the serving area of visited network 24. Home network 28 represents a communication network that maintains a subscription for access terminal 20. The subscription may include an account that is charged based upon usage by access terminal 20. Visited network 24 and home

network 28 may be part of the same or different communication networks.

Visited network 24 and home network 28 may include any suitable components for facilitating a communication session for access terminal 20. According to the illustrated embodiment, visited network 24 includes a radio access network (RAN) 32, an IP gateway 36, a visited bearer manager (V-BM) 40a, a visited policy server (V-PS) 44a, a visited authentication, authorization, and accounting (AAA) server (V-AAA) 58a. Home network 28 includes a home bearer manager (H-BM) 40b, a home policy server (H-PS) 44b, a services data manager (SDM) 52, an applications manager (AM) 56, and a home AAA server (H-AAA) 58b coupled as shown.

Radio access network 32 provides access services to access terminal 20. For example, radio access network 32 may provide layer 2 mobile access, mobility, and/or handoff services within its area of coverage.

IP gateway 36 operates as a gateway between radio access network 32 and an IP network. IP gateway 36 may perform operations such as authenticating access terminal 20, assigning a bearer manager 40 to access terminal 20, performing handoff functions between two IP gateways 36 or IP gateway 36 and radio access network 32, and/or facilitating registration of access terminal 20 to the IP network. In one embodiment, IP gateway 36 may comprise a packet data serving node (PDSN).

Bearer managers 40 allocate resources and provide bearer paths that communicate packets to and/or from access terminal 20. According to one embodiment, a bearer manager 40 operates as an anchor for a bearer path. Bearer manager 40 may also operate as a home or foreign agent that authorizes use of a network address

that allows access terminal 20 to use the bearer path anchored by bearer manager 40.

In the illustrated embodiment, visited bearer manager 40a of visited network 24 provides services to access terminal 20 in visited network 24. According to one embodiment, a visited bearer manager 40a operates as an anchor for a visited anchored path. In the embodiment, visited bearer manager 40a provides a visited network address that allows access terminal 20 to use the visited anchored path. An example of a visited network address includes a visited IP (V-IP) address.

In the illustrated embodiment, home bearer manager 40b of home network 28 provides services to access terminal 20. According to one embodiment, home bearer manager 40b operates as an anchor for a home anchored path. In the embodiment, home bearer manager 40b provides a home network address that allows access terminal 20 to use the home anchored path. An example of a home network address includes a home IP (H-IP) address. The visited home anchored paths are described in more detail with reference to FIGURE 2.

FIGURE 2 illustrates examples of bearer paths of system 10 of FIGURE 1. The bearer paths include a home anchored path 80 and a visited anchored path 82. Home anchored path 80 is anchored at home bearer manager 40b and passes through visited bearer manager 40a. Home anchored path 80 may allow visited bearer manager 40a to perform operations for packets on path 80, for example, enforce packet policies, account for the packets, and/or perform other operations. The home network address allows access terminal 20 to use home anchored path 80. Packets that have the visited network address as a care-of

address for the home network address may be routed along path 80.

Visited anchored path 82 is anchored at visited bearer manager 40a, and does not pass through home bearer manager 40b. Accordingly, visited anchored path 82 may have a latency that is lower than home anchored path 80. The visited network address allows access terminal 20 to use visited anchored path 82.

Paths 82 and 80 may be utilized in any suitable manner. For example, visited anchored path 82 may be used for situations with stricter latency requirements, but home anchored path 80 may be used for situations that require a more stable path. Home anchored path 80 also enables home network 28 to provide home network specific functions and services that are not supported by visited network 24. In certain cases, both paths 82 and 80 may be used. For example, home anchored path 80 may be used for signaling, and visited anchored path 82 may be used for media. In one embodiment, home anchored path 80 may be the default path.

HBM-VBM tunnel 86 represents a bi-directional tunnel between home bearer manager 40b and visited bearer manager 40a. VBM-IPGW tunnel 88 represents a bi-directional tunnel between visited bearer manager 40a and IP gateway 36. VBM-IPGW tunnel 88 may allow visited bearer manager 40a to forward traffic to access terminal 20 via IP gateway 36, and may comprise, for example, a proxy mobile IP (PMIP) tunnel. Link 92 represents a communication link between IP gateway 36 and access terminal 20. Link 92 may comprise, for example, a point-to-point (PPP), A.10, or A.11 link.

Referring back to FIGURE 1, network addresses may be communicated to access terminal 20 in any suitable

manner. As an example, a network address may be communicated using the Dynamic Host Configuration Protocol (DHCP). As another example, network address may be communicated using the Point-to-Point Protocol (PPP).

Bearer managers 40 may perform other suitable operations to provide services to access terminal 20. Examples of other suitable operations include processing signaling, committing resources, and maintaining gateways for access terminal 20. Other examples include enforcing network policies (such as mobility policies), providing security, detecting application layer traffic; recording network presence, and/or performing other suitable operation.

A bearer manager 40 may comprise any suitable device, for example, a Serving General Packet Radio Services (GPRS) Support Node (SGSN), a GPRS Gateway Support Node (GGSN), a home/foreign agent, a mobile gateway, a mobile IPv6 node, or a Packet Data Serving Node (PDSN). A bearer manager 40 may use any suitable protocol, for example, an IP Multimedia Subsystem (IMS) protocol.

Policy servers 44 manage policy rules and provide the policy rules to bearer managers 40. In the illustrated embodiment, policy server 44a provides policy rules to bearer manager 40a. Policy server 44b provides policy rules to bearer manager 40b, and may also provide policy rules to policy server 44a.

In one embodiment, a policy may include rules that specify an action to be taken in particular situations. Policies may include routing rules and other suitable rules such as charging, quality of service, usage tracking, and/ or other rules. A routing rule may specify how to route a packet. For example, a routing rule may

specify situations in which visited anchored path 82 or home anchored path 80 is to be used. For example, a rule may specify that if packet has a particular source and/or destination, then the packet to be routed along visited anchored path 82. Otherwise, the packet is to be routed along home anchored path 80. In one embodiment, a routing rule that allows the visited network address may be installed for a specific duration, and then revoked.

According to one embodiment, a routing rule may specify that home anchored path 80 is used for certain applications and visited anchored path 82 is used for other applications. For example, home anchored path 80 is used for signaling (such as session initiation protocol (SIP) signaling) and visited anchored path 82 is used for media (such as voice over IP (VoIP)).

Any suitable routing rule may be used. As an example, a routing rule may specify that if access terminals 20 engaged in a real-time communication session are being serviced by the same visited network 24, then use visited anchored path 82. As another example, a routing rule may specify that if there is not an appropriate relationship between visited network 24 and home network 28, then use home anchored path 80. As another example, a routing rule may specify that if high security that can only be provided by home network 28 is required, then use home anchored path 80.

In one embodiment, routing rules may used to provide instructions to access terminal 20 on when to use home anchored path 80 or visited anchored path 82. The instructions may be provided in any suitable manner. For example, the routing rule may be forwarded to access terminal 20. In the example, access terminal 20 may receive a URL to download the routing rules. As another

example, access terminal 20 may be configured with the routing rule. As another example, visited bearer manager 40a may obtain the routing rule and may instruct access terminal 20 in accordance with the routing rule.

Services data manager (SDM) 52 stores subscriber data for access terminals 20. According to one embodiment, services data manager 52 may store policy documents that define policies. One or more subscribers may be associated with a particular policy document that defines the policies for those subscribers.

Application manager 56 manages applications, such as SIP applications and/or other suitable applications. The applications may be used to perform SIP operations (such as SIP registration, authorization, and routing), voice features (such as call routing and call forwarding), services (such as push-to-talk (PTT) and IP Centrex), Service Capabilities Interaction Management (SCIM), user presence services, and/or other operations. A non-SIP application manager may be used to perform non-SIP operations, such as real-time streaming media using Real Time Streaming Protocol (RTSP), gaming applications using proprietary protocols, and/or other operations. Application manager 56 may communicate with policy server 44 to request a policy to be implemented on its behalf for a particular access terminal 20.

AAA servers 58 perform authentication, authorization, and/or accounting operations. Home AAA server 58b performs these operations for access terminal 20. Visited AAA server 58a requests that home AAA server 58b performs these operations for access terminal 20 served by visited network 24.

A component of system 10 may include any suitable arrangement of elements, for example, an interface,

logic, memory, other suitable element, or combination of any of the preceding. For example, access terminal 20 includes an interface 60, logic 62, and a memory 64. An interface receives input, sends output, processes the input and/or output, performs other suitable operation, or performs a combination of any of the preceding. An interface may comprise hardware and/or software.

Logic performs the operations of the component, for example, executes instructions to generate output from input. Logic may include hardware, software, other logic, or combination of any of the preceding. Certain logic, such as a processor, may manage the operation of a component. Examples of a processor include one or more computers, one or more microprocessors, one or more applications, other logic, or a combination of any of the preceding.

A memory stores information. A memory may comprise computer memory (for example, Random Access Memory (RAM) or Read Only Memory (ROM)), mass storage media (for example, a hard disk), removable storage media (for example, a Compact Disk (CD) or a Digital Video Disk (DVD)), database and/or network storage (for example, a server), other computer-readable medium, or a combination of any of the preceding.

Modifications, additions, or omissions may be made to system 10 without departing from the scope of the invention. The components of system 10 may be integrated or separated according to particular needs. Moreover, the operations of system 10 may be performed by more, fewer, or other modules. Additionally, operations of system 10 may be performed using any suitable logic. As used in this document, "each" refers to each member of a set or each member of a subset of a set.

FIGURE 3 illustrates one embodiment of a method for sending packets using either a home network address or a visited network address. The method may be used by system 10 of FIGURE 1.

IP gateway 36 authenticates access terminal 20 at step 110. Access terminal 20 may be authenticated using any suitable protocol, for example, extensible authentication protocol (EAP). Authentication may provide gateway 36 with addresses of home bearer manager 40b and applications manager 56 of access terminal 20.

Access terminal 20 obtains a visited network address at steps 120 through 128. The visited network address may be obtained using any suitable protocol, for example, DHCP and a proxy mobile IP (PMIP). Access terminal 20 sends a DHCP query to IP gateway 36 at step 120. IP gateway 36 obtains the visited network address from visited bearer manager 40a at steps 124 through 126. Gateway 36 sends a proxy mobile IP request to visited bearer manager 40a at step 124. Visited bearer manager 40a sends a visited network address to IP gateway 36 in a proxy mobile IP response at step 126. IP gateway 36 sends the visited network address to access terminal 20 in a DHCP response at step 128. The DHCP response may also include addresses for home bearer manager 40b and applications manager (AM) 56.

Access terminal 20 obtains a home network address at steps 130 through 150. Access terminal 20 registers with home bearer manager 40b at step 130 according to mobile IP registration. During registration, home bearer manager 40b provides access terminal 20 with a home network address. Also, access terminal 20 notifies home bearer manager 40b of the visited network address as a point-of-attachment in order to include visited bearer

manager 40a in home anchored path 80. Home bearer manager 40b authenticates the mobile IP registration at step 134. The authentication may be based on keys derived from the EAP authentication or from shared secret information provisioned for mobile IP authentication.

Home bearer manager 40b obtains policies from home policy server 44b at step 140. Home policy server 44b sends policies to visited policy server 44a at step 142. Visited bearer manager 40a obtains policies from visited policy server 44b at step 144. Home bearer manager 40b sends an mobile IP response to access terminal 20 at step 146. Access terminal 20 performs SIP registration with applications manager 56 at step 150.

Access terminal 20 receives instructions regarding the use of the visited and/or home network addresses at step 160. Access terminal 20 communicates packets using bearer paths 82 and/or 80 according to the policy at steps 164 and 166. Packets may be communicated along bearer path 182 at step 164 using visited network address, and/or packets may be communicated along bearer path 180 using home network address at step 166. Access terminal 20 communicates the packets according to the policy until the policy is revoked at step 170. After the policy is revoked, the method terminates.

Modifications, additions, or omissions may be made to the method without departing from the scope of the invention. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order.

FIGURE 4 illustrates one embodiment of a method for establishing a point-to-point session that may be used by system 10 of FIGURE 1. The method begins at step 210, where a traffic channel (TCh) is set up to authenticate

access terminal 20. The traffic channel may be set up as access terminal 20 powers up. Access terminal 20 may be provisioned with a network access identifier (NAI), a mobile node-authentication, authorization, and accounting (MN-AAA) security association, and a mobile node-home agent (MN-HA) security association. Radio access network 32 initiates establishment of A.10/A.11 link 92 with IP gateway 36 at step 214.

Access terminal 20 initiates a point-to-point (PPP) session with IP gateway 36 at step 218. In the link control protocol (LCP) phase of the PPP establishment, Password Authentication Protocol (PAP) and/or Challenge Handshake Authentication Protocol (CHAP) may be used to authenticate access terminal 20.

IP gateway 36 sends an access request to visited AAA server 58a at step 222, which relays the access request to home AAA server 58b. Home AAA server 58b authenticates access terminal 20 at step 226. Home AAA server 58b sends an access acceptance to visited AAA server 58a at step 230, which forwards the access acceptance to IP gateway 36.

The access acceptance may include authorization parameters inserted by home AAA server 58b and/or visited AAA server 58a. The parameters may describe resources assigned by servers 38. For example, home AAA server 58a may assign home bearer manager 44a for mobile IP service, and visited AAA server 58a may assign visited bearer manager 40a and visited policy server 44a. In one embodiment, the access request and access acceptance may conform to the Remote Authentication Dial In User Service (RADIUS) protocol.

IP gateway 36 informs access terminal 20 that the PPP session has been established at step 234. Access

terminal 20 sends an IP address request to IP gateway 36 at step 238. The address request may be sent during the IP Control Protocol (IPCP) phase of the PPP establishment. IP gateway 36 sends a Proxy Mobile IP (PMIP) registration request to visited bearer manager 40a at step 242. The registration request may indicate that the care of address is IP gateway 36 and that the agent is visited bearer manager 40a, and may be protected by an MN-HA security association.

Visited bearer manager 40a authenticates the registration request and assigns a visited network address (V-NA) from a visited network address pool at step 244. Visited bearer manager 40a sends an authorization request that includes the visited network address to visited policy server 44a at step 248. Visited policy server 44a forwards the authorization request to home policy server 44b.

Home policy server 44b sends a policy request to services data manager 52 at step 252. The policy request requests the policy corresponding to access terminal 20. Services data manager 52 sends the requested policy to home policy server 44b in a policy reply at step 256. Home policy server 44b sends an authorization response to visited policy server 44a at step 260. The authorization response includes the policy. Visited policy server 44a may add its own policy before forwarding the authorization response to visited bearer manager 40b. In one embodiment, the authorization request and authorization response may conform to the Diameter protocol.

Visited bearer manager 40a sets up forwarding for visited network address through VBM-IPGW tunnel 88 at step 264. Visited bearer manager 40 may create a

mobility binding entry for access terminal 20 to set up forwarding. Visited bearer manager 40a sends a PMIP registration reply to IP gateway 36 at step 268. The registration reply may include the visited network address as the home address, and may be protected by an MN-HA authentication extension.

IP gateway 36 sets up forwarding between the PPP session and the VBM-IPGW tunnel 88 at step 272. IP gateway 36 sends the visited network address to access terminal 20 in an PPP configuration message at step 276. Access terminal 20 obtains the visited network address at step 280. Access terminal 20 may use the visited network address to communicate packets along visited anchored path 82.

Modifications, additions, or omissions may be made to the method without departing from the scope of the invention. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order.

FIGURE 5 illustrates one embodiment of a method for establishing a mobile IP session that may be used by system 10 of FIGURE 1. The method begins at step 310, where visited bearer manager 40a sends an agent advertisement to IP gateway 36, which forwards the agent advertisement to access terminal 20.

Access terminal 20 sends a mobile IP (MIP) registration request to visited bearer manager 40a at step 314. The message may include a mobile node-foreign agent (MN-FA) challenge extension, a mobile node-home agent (MN-HA) authentication extension, and a mobile node-AAA (MN-AAA) authentication extension.

Visited bearer manager 40a processes the registration request and maps the MN-FA challenge

extension and MN-AAA authentication extension to an access request. Visited bearer manager 40a sends an access request to visited AAA server 58a at step 318, which forwards the access request to home AAA server 58b. Home AAA server 58b authenticates access terminal 20 and sends an access acceptance to visited AAA server 58a at step 322, which forwards the access acceptance to visited bearer manager 40a. The access acceptance may include authorization attributes from both the visited and home AAA servers 58.

Visited bearer manager 40a relays the registration request to home bearer manager 40b at step 326. In another embodiment, if access terminal 20 knows home bearer manager 40b, access terminal 20 may send the registration request directly to the home bearer manager 40b, which forwards the registration request to home AAA server 58b.

Home bearer manager 40b processes the registration request, and sends an access request to home AAA server 58b at step 330. Home AAA server 58b sends an access acceptance to home bearer manager 40b at step 334. The access acceptance may include authorization attributes for home agent service. Home bearer manager 40b assigns a home network address (H-NA) from a local address pool at step 338.

Home bearer manager 40b may authenticate the registration request according to the MN-HA security association, and then sends an authorization request to home policy server 44b at step 342. Home policy server 44b sends a policy request to services data manager 52 at step 346. The policy request requests the policy corresponding to access terminal 20. Services data manager 52 sends the requested policy in a policy reply

at step 350. Home policy server 44b sends an authorization response with the policy to home bearer manager 40b at step 354. The authorization response includes the address for applications manager 56 assigned to access terminal 20 for SIP service.

Home bearer manager 40b sets up forwarding for home network address through HBM-VBM tunnel 86 at step 358. Home bearer manager 40b may create a mobility binding entry for access terminal 20 to create HBM-VBM tunnel 86. Home bearer manager 40b sends a registration reply to visited bearer manager 40a at step 362. The registration reply includes the assigned home network address.

Visited bearer manager 40a sets up forwarding between VBM-IPGW tunnel 88 and HBM-VBM tunnel 86 at step 360. Visited bearer manager 40a relays the mobile IP registration reply to access terminal 20 at step 370. The registration reply includes the home network address. Access terminal obtains the home network address as the mobile IP address at step 374. Access terminal 20 may use the home network address to communicate packets along home anchored path 80.

To re-register, access terminal 20 may send a re-registration request to visited bearer manager 40a, which forwards the request to home bearer manager 40b. The re-registration request may be a mobile IP registration request that includes the home network address and the visited network address. Home bearer manager 40b updates the mobility binding for access terminal 20. Home bearer manager 40b then sends a registration reply to visited bearer manager 40a, which updates the visitor entry for access terminal 20. Visited bearer manager 40b then sends the registration reply to access terminal 20, which updates its registration state.

To deregister, access terminal 20 sends a deregistration request to visited bearer manager 40a, which forwards the request to home bearer manager 40b. The deregistration request may comprise a registration request with a lifetime of zero. Home bearer manager 40b deletes the mobility binding for access terminal 20, and sends a registration reply to visited bearer manager 40b. Visited bearer manager 40b deletes the visitor entry for access terminal 20. Visited bearer manager 40b then sends a registration reply to access terminal 20, which deletes its registration state.

Modifications, additions, or omissions may be made to the method without departing from the scope of the invention. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order.

Certain embodiments of the invention may provide one or more technical advantages. A technical advantage of one embodiment may be that packets from an access terminal can be communicated along a home anchored path or a visited anchored path. The home anchored path includes a home bearer manager of the home network of the access terminal and may include a visited bearer manager of the visited network. The visited anchored path includes the visited bearer manager, but not the home bearer manager.

Another technical advantage of one embodiment may be that the access terminal can be provided with a home network address and a visited network address. The home network address may be used to communicate packets along the home anchored path, and the visited network address may be used to communicate packets along the visited anchored path.

Another technical advantage of one embodiment may be that a home policy server of the home network may provide policy rules to a visited policy server of the visited network. The policy rules may be used to enforce policies for packets sent along the visited anchored path.

Although this disclosure has been described in terms of certain embodiments, alterations and permutations of the embodiments will be apparent to those skilled in the art. Accordingly, the above description of the embodiments does not constrain this disclosure. Other changes, substitutions, and alterations are possible without departing from the spirit and scope of this disclosure, as defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for communicating a plurality of packets along a bearer path, comprising:

receiving a home network address at an access terminal, the home network address corresponding to a home anchored bearer path anchored at a home network of the access terminal;

receiving a visited network address at the access terminal, the visited network address corresponding to a visited anchored bearer path anchored at a visited network;

determining whether to use the home anchored bearer path or the visited anchored bearer path; and

communicating a plurality of packets using the home network address or the visited network address in accordance with the determination.

2. The method of Claim 1, wherein receiving the visited network address at the access terminal further comprises:

receiving the visited network address in a Dynamic Host Configuration Protocol (DHCP) response.

3. The method of Claim 1, wherein receiving the visited network address at the access terminal further comprises:

receiving the visited network address during initiation of a Packet Data Protocol (PDP) context.

4. The method of Claim 1, wherein determining whether to use the home anchored bearer path or the visited anchored bearer path further comprises:

receiving a policy specifying use of the visited network address; and

determining to use the visited network address according to the received policy.

5. The method of Claim 1, wherein determining whether to use the home anchored bearer path or the visited anchored bearer path further comprises:

determining to use the visited network address according to an instruction stored at the mobile node.

6. The method of Claim 1, wherein determining whether to use the home anchored bearer path or the visited anchored bearer path further comprises:

using the home network address as a default address.

7. An access terminal for communicating a plurality of packets along a bearer path, comprising:

a memory operable to:

store a home network address, the home network address corresponding to a home anchored bearer path anchored at a home network of the access terminal; and

store a visited network address, the visited network address corresponding to a visited anchored bearer path anchored at a visited network; and

a processor coupled to the memory and operable to:

determine whether to use the home anchored bearer path or the visited anchored bearer path; and

communicate a plurality of packets using the home network address or the visited network address in accordance with the determination.

8. The access terminal of Claim 7, wherein the visited network address is received in a Dynamic Host Configuration Protocol (DHCP) response.

9. The access terminal of Claim 7, wherein the visited network address is received during initiation of a Packet Data Protocol (PDP) context.

10. The access terminal of Claim 7, the processor operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

receiving a policy specifying use of the visited network address; and

determining to use the visited network address according to the received policy.

11. The access terminal of Claim 7, the processor operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

determining to use the visited network address according to an instruction stored at the mobile node.

12. The access terminal of Claim 7, the processor operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

using the home network address as a default address.

13. Logic for communicating a plurality of packets along a bearer path, the logic embodied in a computer-readable storage medium and operable to:

receive a home network address at an access terminal, the home network address corresponding to a home anchored bearer path anchored at a home network of the access terminal;

receive a visited network address at the access terminal, the visited network address corresponding to a visited anchored bearer path anchored at a visited network;

determine whether to use the home anchored bearer path or the visited anchored bearer path; and

communicate a plurality of packets using the home network address or the visited network address in accordance with the determination.

14. The logic of Claim 13, further operable to receive the visited network address at the access terminal by:

receiving the visited network address in a Dynamic Host Configuration Protocol (DHCP) response.

15. The logic of Claim 13, further operable to receive the visited network address at the access terminal by:

receiving the visited network address during initiation of a Packet Data Protocol (PDP) context.

16. The logic of Claim 13, further operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

receiving a policy specifying use of the visited network address; and

determining to use the visited network address according to the received policy.

17. The logic of Claim 13, further operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

determining to use the visited network address according to an instruction stored at the mobile node.

18. The logic of Claim 13, further operable to determine whether to use the home anchored bearer path or the visited anchored bearer path by:

using the home network address as a default address.

19. A system for communicating a plurality of packets along a bearer path, comprising:

means for receiving a home network address at an access terminal, the home network address corresponding to a home anchored bearer path anchored at a home network of the access terminal;

means for receiving a visited network address at the access terminal, the visited network address corresponding to a visited anchored bearer path anchored at a visited network;

means for determining whether to use the home anchored bearer path or the visited anchored bearer path; and

means for communicating a plurality of packets using the home network address or the visited network address in accordance with the determination.

20. A method for communicating a plurality of packets along a bearer path, comprising:

receiving a home network address at an access terminal, the home network address corresponding to a home anchored bearer path anchored at a home network of the access terminal;

receiving a visited network address at the access terminal, the visited network address corresponding to a visited anchored bearer path anchored at a visited network, receiving the visited network address further comprising:

receiving the visited network address in a Dynamic Host Configuration Protocol (DHCP) response; or

receiving the visited network address during initiation of a Packet Data Protocol (PDP) context;

determining whether to use the home anchored bearer path or the visited anchored bearer path by:

receiving a policy specifying use of the visited network address, and determining to use the visited network address according to the received policy;

determining to use the visited network address according to an instruction stored at the mobile node; and

using the home network address as a default address; and

communicating a plurality of packets using the home network address or the visited network address in accordance with the determination.

FIG. 1

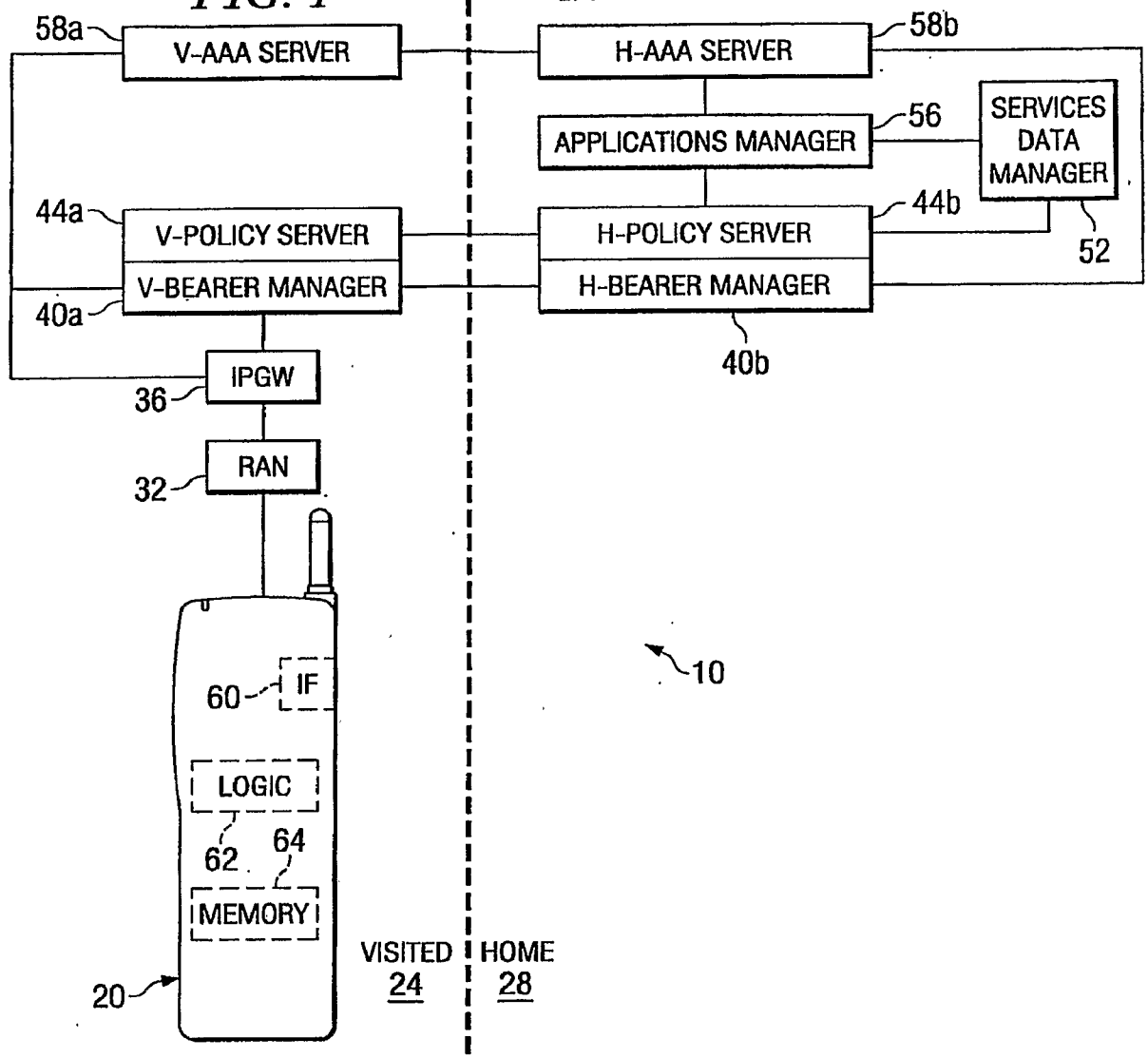
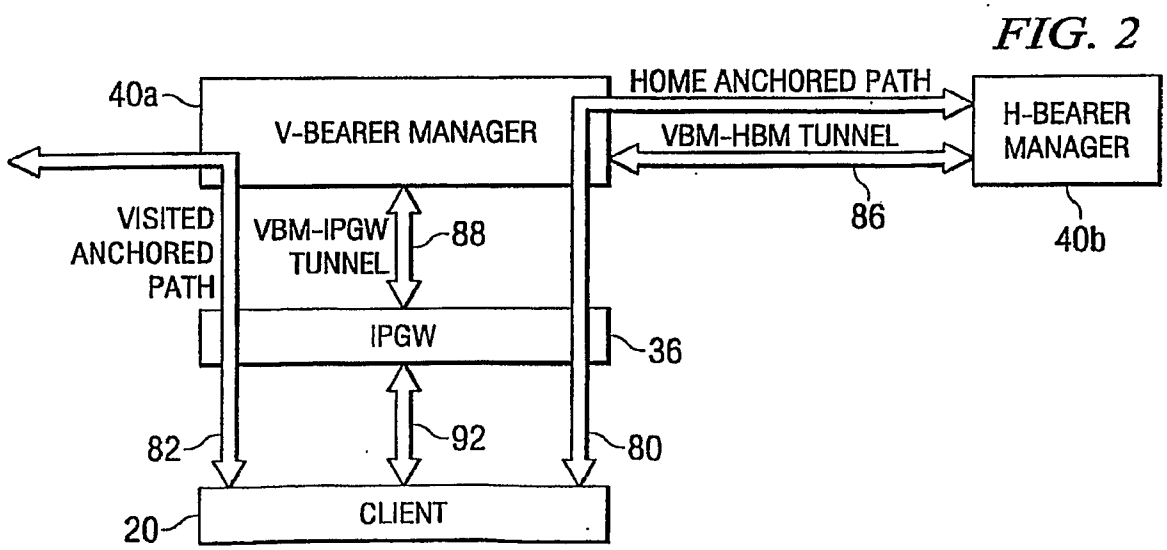

58a
V-AAA SERVER
H-AAA SERVER
58b
APPLICATIONS MANAGER
56
SERVICES DATA MANAGER
52
44a
V-POLICY SERVER
H-POLICY SERVER
44b
V-BEARER MANAGER
H-BEARER MANAGER
40a
40b
IPGW
36
RAN
32
60
IF
LOGIC
62
64
MEMORY
20
10
VISITED
24
HOME
28

FIG. 2


40a
V-BEARER MANAGER
HOME ANCHORED PATH
VBM-HBM TUNNEL
H-BEARER MANAGER
86
40b
VISITED ANCHORED PATH
VBM-IPGW TUNNEL
88
IPGW
36
82
92
80
20
CLIENT

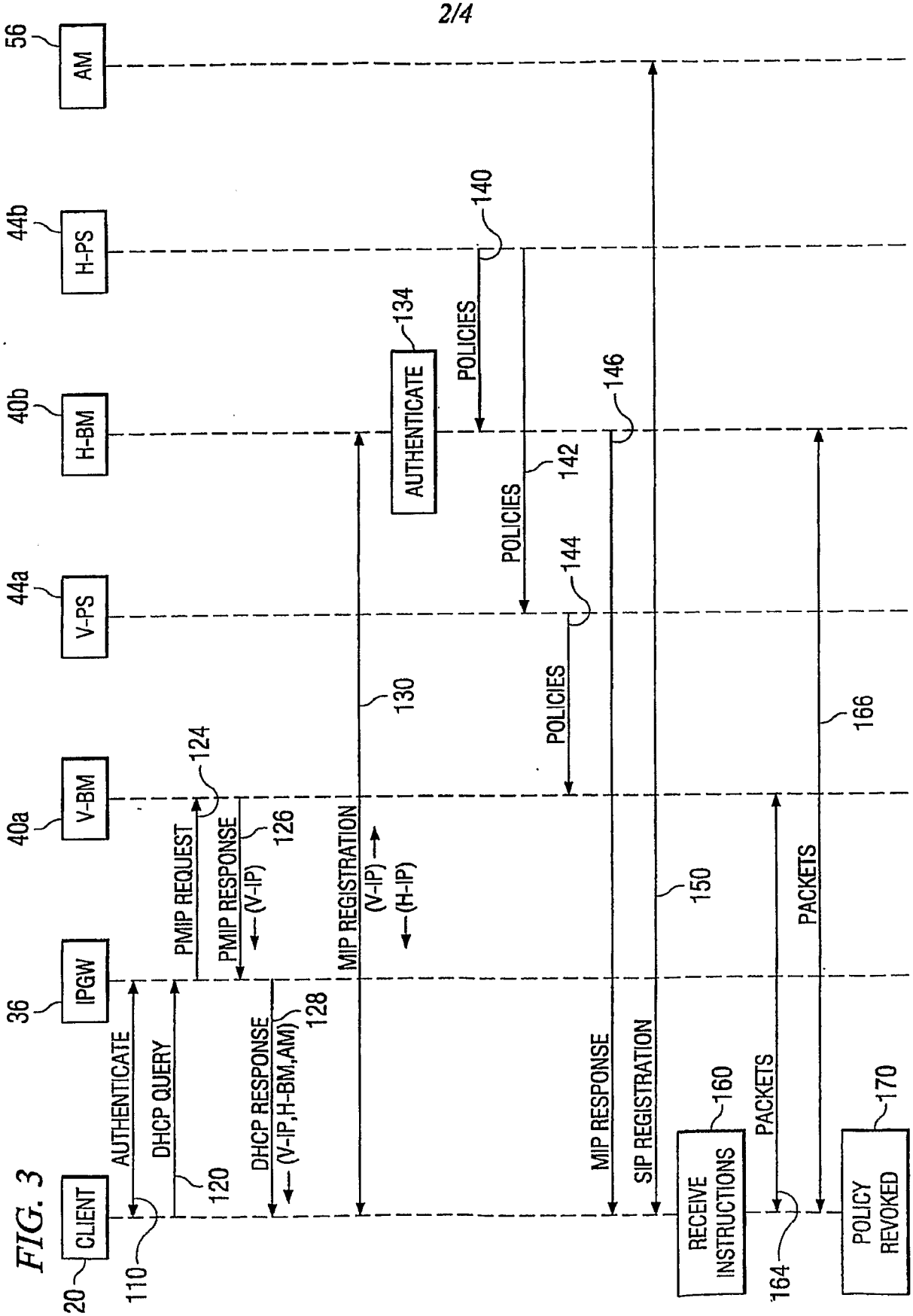

CLIENT
20
IPGW
36
V-BM
40a
V-PS
44a
H-BM
40b
H-PS
44b
AM
56
AUTHENTICATE
110
DHCP QUERY
120
PMIP REQUEST
124
PMIP RESPONSE
(V-IP)
126
DHCP RESPONSE
(V-IP,H-BM,AM)
128
MIP REGISTRATION
(V-IP)
(H-IP)
130
AUTHENTICATE
134
POLICIES
140
POLICIES
142
POLICIES
144
MIP RESPONSE
146
SIP REGISTRATION
150
RECEIVE INSTRUCTIONS
160
PACKETS
164
PACKETS
166
POLICY REVOKED
170

FIG. 3

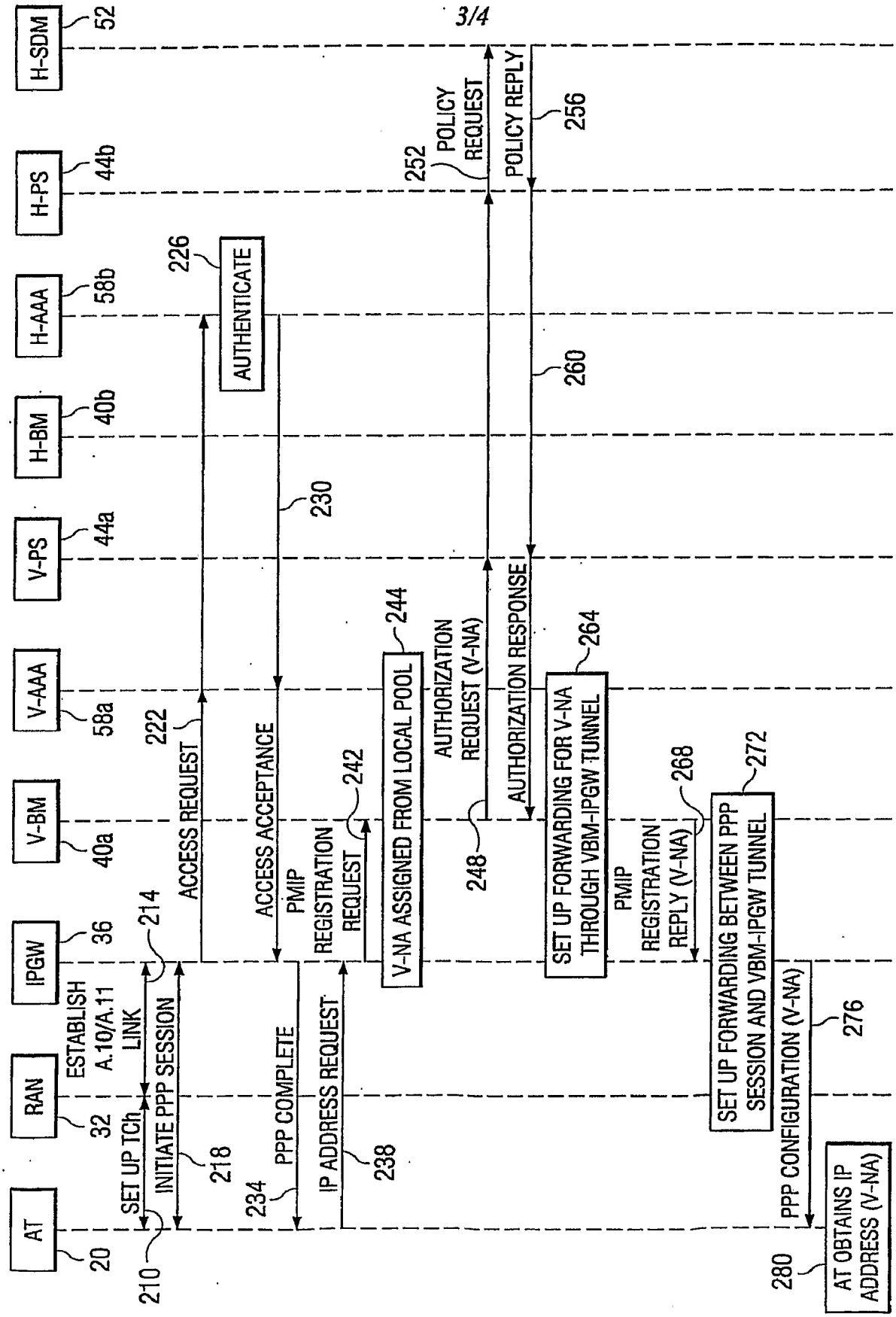

AT
20
RAN
32
IPGW
36
V-BM
40a
V-AAA
58a
V-PS
44a
H-BM
40b
H-AAA
58b
H-PS
44b
H-SDM
52
ESTABLISH A.10/A.11 LINK
214
SET UP TCh
INITIATE PPP SESSION
218
210
ACCESS REQUEST
222
AUTHENTICATE
226
ACCESS ACCEPTANCE
230
PPP COMPLETE
234
IP ADDRESS REQUEST
238
PMIP REGISTRATION REQUEST
242
V-NA ASSIGNED FROM LOCAL POOL
244
AUTHORIZATION REQUEST (V-NA)
248
POLICY REQUEST
252
POLICY REPLY
256
AUTHORIZATION RESPONSE
260
SET UP FORWARDING FOR V-NA THROUGH VBM-IPGW TUNNEL
264
PMIP REGISTRATION REPLY (V-NA)
268
SET UP FORWARDING BETWEEN PPP SESSION AND VBM-IPGW TUNNEL
272
PPP CONFIGURATION (V-NA)
276
AT OBTAINS IP ADDRESS (V-NA)
280

FIG. 4

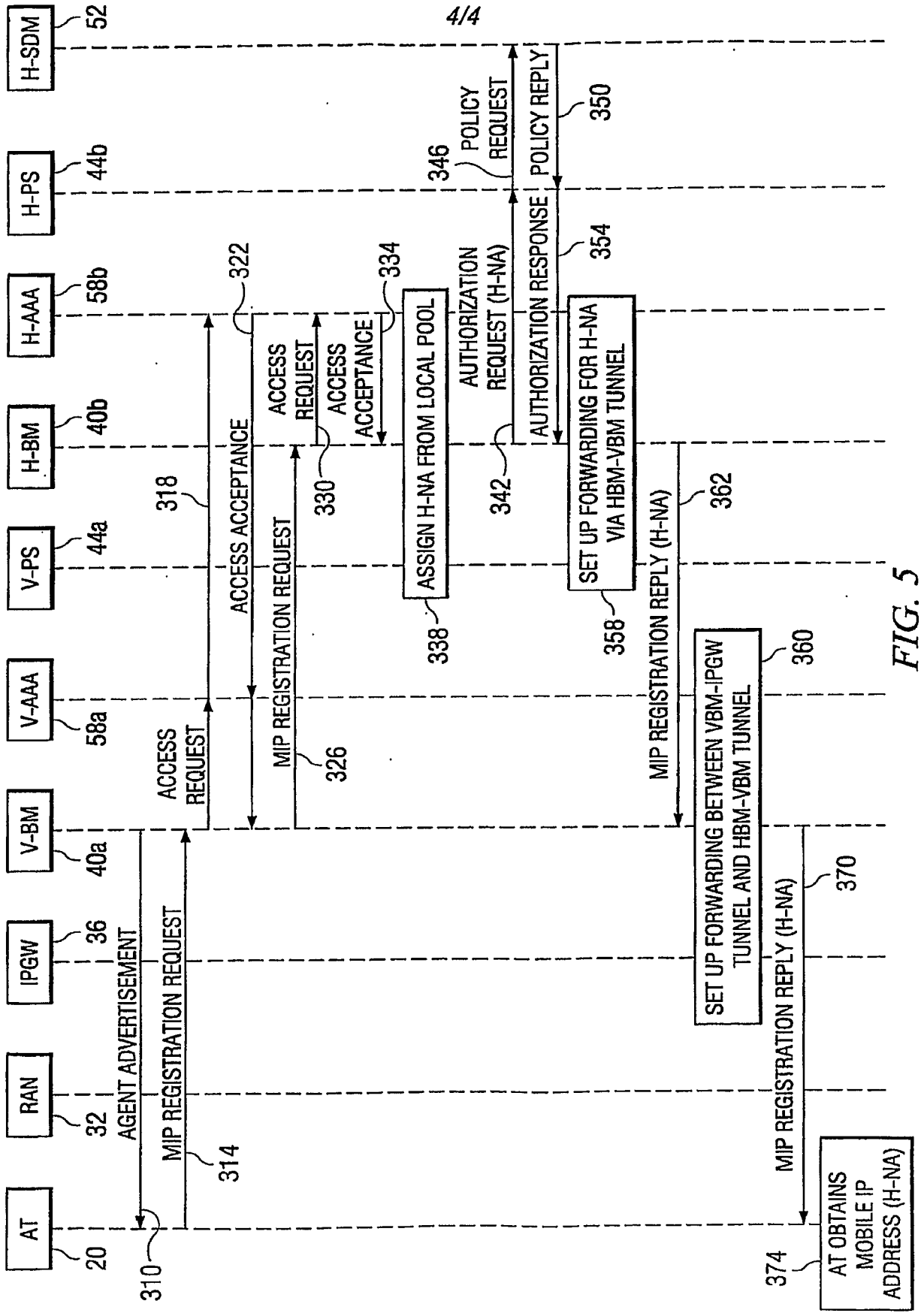

AT
20
RAN
32
IPGW
36
V-BM
40a
V-AAA
58a
V-PS
44a
H-BM
40b
H-AAA
58b
H-PS
44b
H-SDM
52
AGENT ADVERTISEMENT
310
MIP REGISTRATION REQUEST
314
ACCESS REQUEST
318
ACCESS ACCEPTANCE
322
MIP REGISTRATION REQUEST
326
ACCESS REQUEST
330
ACCESS ACCEPTANCE
334
ASSIGN H-NA FROM LOCAL POOL
338
AUTHORIZATION REQUEST (H-NA)
342
POLICY REQUEST
346
POLICY REPLY
350
AUTHORIZATION RESPONSE
354
SET UP FORWARDING FOR H-NA VIA HBM-VBM TUNNEL
358
MIP REGISTRATION REPLY (H-NA)
362
SET UP FORWARDING BETWEEN VBM-IPGW TUNNEL AND HBM-VBM TUNNEL
360
MIP REGISTRATION REPLY (H-NA)
370
AT OBTAINS MOBILE IP ADDRESS (H-NA)
374

FIG. 5