(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 2007/103481 A2

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

(21) International Application Number:
PCT/US2007/005900

(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)*: **ROSENBERG, Jonathan, D.** [US/US]; 197 Pin Oak Road, Freehold, NJ 07728 (US). **ANDREASEN, Flemming, S.** [DK/US]; 32 Burlington Drive, Marlboro, NJ 07746 (US). **STAMMERS, Timothy, P.** [GB/US]; 4309 Oak Park Road, Raleigh, NC 27612 (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.

WO 2007/103481 A2

(54) **Title:** ESTABLISHING FACETS OF A POLICY FOR A COMMUNICATION SESSION

(57) **Abstract:** Establishing one or more facets of a policy includes facilitating a communication session for an access terminal at a visited network. The access terminal is associated with a home network having a home policy server. The policy is received at a visited policy server of the visited network. The policy comprises the facets. If the facets are unacceptable, the facets are negotiated until a stopping point is reached. The negotiation includes adjusting by the visited policy server at least one facet of the one or more facets, and notifying the home policy server of the adjustment. The facets are established in accordance with the negotiation.

ESTABLISHING FACETS OF A POLICY FOR A COMMUNICATION SESSION

TECHNICAL FIELD

This invention relates generally to the field of telecommunications and more specifically to establishing facets of a policy for a communication session.

BACKGROUND

An endpoint, such as an access terminal, may use a system of communication networks to communicate packets with other endpoints during communication sessions. 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 make policy decisions, such as accounting or quality of service decisions, for these communication sessions. 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, establishing one or more facets of a policy includes facilitating a communication session for an access terminal at a visited network. The access terminal is associated with a home network having a home

policy server. The policy is received at a visited policy server of the visited network. The policy comprises the facets. If the facets are unacceptable, the facets are negotiated between the visited network and the home network until a stopping point is reached. The negotiation includes adjusting by the visited policy server at least one facet of the one or more facets, and notifying the home policy server of the adjustment. The facets are established in accordance with the negotiation.

Certain embodiments of the invention may provide one or more technical advantages. A technical advantage of one embodiment may be that a home policy server of a home network may provide a policy to a visited policy server of a visited network. The policy may include application facets that allow the visited network to make policy decisions for an application without having to execute or otherwise support the application.

Another technical advantage of one embodiment may be that the visited policy server may negotiate with the home policy server to establish policy facets acceptable to the policy servers. The visited policy server need not be forced to use unacceptable policy facets.

Another technical advantage of one embodiment may be that one or more policy facets may be installed on a network element in the home network and/or the visited network. The policy facets may allow the network element to make policy decisions.

Another technical advantage of one embodiment may be that a deep packet inspection (DPI) facet may be dynamically installed on an edge router. The DPI facet may have a scope and rules based on a particular application invocation. The DPI facet may allow the edge

router to perform deep packet inspection of the relevant packets at the edge router.

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 an example of a policy model that may be used with the system of FIGURE 1;

FIGURE 3 illustrates an example of a call flow for establishing policy facets that may be used by the system of FIGURE 1;

FIGURE 4 illustrates an example of a call flow for determining a policy output that may be used by the system of FIGURE 1; and

FIGURE 5 illustrates an example of a call flow for implementing a deep packet inspection policy 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, system 10 includes a visited network 24 and a home network 28. Visited network 24 includes a radio access network (RAN) 32, an Internet Protocol (IP) gateway (IPGW) 36, a visited bearer manager (V-bearer manager) 40a, and a visited policy server (V-policy server) 44a coupled as shown. Home network 28 includes a home bearer manager (H-bearer manager) 40b, a home policy server (H-policy server) 44b, a services data manager 52, and an application manager 56 coupled as shown.

According to certain examples, home policy server 44b may provide a policy to visited policy server 44a. The policy may include application facets that allow visited network 24 to make policy decisions for an application without having to execute or otherwise support the application. Application facets may comprise a set of one or more tokens (such as text-strings) that identify an application and/or components of the application. The tokens are understood by home policy server 44b and visited network policy server 44a. In one example, visited policy server 44a may negotiate with home policy server 44b to establish acceptable policy facets, so visited policy server 44a need not be forced to use unacceptable policy facets. In another example, a policy facet may be installed on a network element to allow the network element to make policy decisions. For example, a deep packet inspection (DPI) facet may be installed on an edge router to allow the edge router to perform deep packet inspection of the packets at the edge router.

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 include voice, data, text, audio, video, multimedia, control, signaling, and/or other information. Information may be communicated in packets, each comprising a bundle of data organized in a specific way for transmission.

System 10 may utilize communication protocols and technologies to provide communication sessions. Examples of communication protocols and technologies include those set by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) standards, the International Telecommunications Union (ITU-T) standards, the European Telecommunications Standards Institute (ETSI) standards, the Internet Engineering Task Force (IETF) standards (for example, IP such as mobile IP), or other standards.

According to the illustrated embodiment, access terminal 20 represents any suitable device operable to communicate with a communication network. For example, a subscriber may use access terminal 20 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, and/or any other device operable to communicate with system 10.

System 10 includes communication networks such as visited network 24 and 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 links, or any combination of any 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 the subscriber using access terminal 20. The subscription for a subscriber may have subscriber identifier that uniquely identifies the subscriber, and 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.

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 IP gateway 36 and radio access network 32, and/or facilitating registration of access terminal 20 to the IP network.

Bearer managers 40 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

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.

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. 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 policies. A policy may include one or more policy rules, where a policy rule specifies an action to be taken if one or more conditions are satisfied. A policy may include facets, which are policy rules that may be installed and executed on a network element. A facet may allow a network element to make policy decisions.

In one embodiment, a deep packet inspection (DPI) facet 60 may be installed on any suitable edge router to allow the edge router to perform deep packet inspection on packets. DPI facet 60 may specify packets to be inspected and rules to be applied to the packets. DPI facet 60 may be used to find SIP packets, verify media (such as Real-Time Transport Protocol (RTP) media) of the media packets, and otherwise inspect the packets sent through the edge router. In one example, DPI facet 60 may be installed on visited bearer manager 40a. Policy

and facets are described in more detail with reference to FIGURE 2.

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 Protocol (RTSP) media operations, proprietary gaming operations, 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.

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. An interface receives input, sends output, processes the input and/or output, and/or performs other suitable operation. 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, and/or other

logic. 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, and/or other logic.

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 2 illustrates an example of a policy model 110 that may be used with system 10 of FIGURE 1. In one embodiment, policy model 110 includes a policy 114, one or more inputs 116 (such as a policy context 118 and a question 122), and one or more outputs 123 (such as application facets 124, network facets 128, and a decision 132). Network facets 128 may include deep packet inspection (DPI) facets 136.

Policy 114 may be embodied by logic that may be executed by policy server 44. Policy 114 may include one or more policy rules, where a policy rule specifies an

action to be taken if one or more conditions are satisfied. Inputs 116 are used to determine whether conditions are satisfied, and outputs 123 describe the actions to be taken.

In the illustrated embodiment, inputs 116 include policy context 118 and question 122. Policy context 118 represents information that may be used to obtain an output 123 from a policy rule. Policy context 118 may include the identity of a subscriber, the application that a subscriber is trying to invoke, the network in which a subscriber is present, and/or other information to which a policy rule may be applied.

Question 122 invokes application of a policy 114. Question 122 may have the form, "Subscriber X has sent a request Y, with policy context Z". In response to question 122, policy server 44 applies policy 114 to the request Y for subscriber X with policy context Z to yield an output 123.

In the illustrated embodiment, outputs 123 include application facets 124, network facets 128, and a decision 132. Decision 132 specifies one or more actions to be taken and are determined in accordance with the application of policy 114. Decision 132 may be determined according to any suitable factor, for example, the requesting provider, current resource usage, and/or other suitable factor.

A facet is itself a policy that may be installed and executed (for example, enforced) on any suitable network component, for example, IP gateway 36, bearer manager 40, and/or application manager 56. In one embodiment, a facet may allow a network element to make policy decisions for a subscriber. For example, bearer manager 40 may be used to make accounting, DPI, roaming, and/or other suitable

policy decisions. IP gateway 36 may be used to make quality of service, accounting, and/or other suitable policy decisions.

Facets may be installed in a push or pull mode. In the push mode, policy server 44 actively pushes a facet to a network element, for example, bearer manager 40. The network element may decide whether the installation can succeed, and either rejects or accepts the installation.

In the pull mode, the network component receives a request from a subscriber. The component asks policy server 44 whether the request can be granted. Policy server 44 provides an output 123, which may include facets. In certain cases, policy server 44 may not be able to provide an immediate response. For example, approval of a request may require additional information that needs to be obtained. In this case, policy server 44 may answer with a pending response.

A facet may include tokens that specify the conditions and actions of the facet. Tokens for the conditions may specify a subscriber identifier and a packet classifier. Tokens for the actions specify actions to be taken for the subscriber with the subscriber identifier and packets that match the packet classifier. In one embodiment, the tokens may be generic, in that home network 28 and visited network 24 agree upon the usage of the tokens.

In one embodiment, a packet may match a packet classifier if characteristics of the packet satisfy conditions of the packet classifier. For example, a packet classifier may include an IP address and/or port range. A packet that has the IP address and uses a port

in the port range may be regarded as matching the packet classifier.

Application facets 124 govern the processing of application requests. Application facets 124 may include a policy decision and one or more tokens. The policy decision may specify whether an application should proceed or terminate, and the tokens may specify actions that the application should perform. Application facets 124 may be installed any suitable network component, for example, application manager 56 and/or bearer manager 44 acting as a application proxy. An application facet 124 may identify an application and application parameters.

Network facets 128 perform network functions such as mobility, access, quality of service, transcoding, accounting, DPI, and/or other functions. A network facet 128 may request network resources for performing the functions. Examples of network facets 128 include mobility, access, quality of service, accounting, transcoding, DPI, and/or other suitable facets.

Mobility facets include rules for mobility decisions. Examples of mobility facets include roaming, handoff, active/dormant reporting, paging filter, and/or other suitable mobility facets. A roaming facet specifies whether roaming is permitted. A handoff facet specifies how handoff is to operate between the same and/or different access technologies. The handoff facet may specify whether handoff is permitted across different network technologies and whether handoff should retrigger authentications. An active/dormant reporting facet indicates whether to report the active/dormant state of access terminal 20 to policy server 44. A paging filter facet specifies packets that initiate paging of client 20.

Access facets include rules for access decisions. A permitted correspondents facet is an example of an access facet. A permitted correspondents facet specifies a set of packets that client 20 is allowed to send or receive. A permitted correspondents facet may be provided to a network element, such as bearer manager 20, statically during mobile IP registration or dynamically in response to a request.

Quality of service facets include rules for quality of service decisions. Examples of quality of service facets include bandwidth reservation, packet marker, traffic shaper/policer, authorization envelope, and/or other suitable quality of service facets. A bandwidth reservation facet specifies the amount of bandwidth for a set of packets. A packet marker facet sets a differential service code point for a set of packets. A traffic shaper/policer facet indicates packets to be dropped, marked, and/or shaped. An authorization envelope facet indicates a maximum authorized bandwidth for an access terminal 20. If access terminal 20 requests more, an authorization request is sent to policy server 44.

Transcoding facets include rules for transcoding decisions. A transcoder facet is an example of a transcoding facet. A transcoder facet identifies a stream, for example, a Real-Time Transport Protocol (RTP) stream, that requires transcoding.

Accounting facets include rules for accounting decisions. Examples of accounting facets include packet counter, threshold, time trigger, and/or other suitable accounting facet. A packet counter facet counts a particular type of packet. A threshold facet specifies a maximum and/or minimum value for a specific counter. If

the threshold is exceeded, then policy server 44 may be notified. A time trigger facet specifies a timer value for a specific packet counter. When the time value is reached, policy server 44 may be notified.

Deep packet inspection (DPI) facets include rules for deep packet inspection decisions. A DPI facet specifies packets to inspect, what to inspect or detect, and actions to take if packets with certain features are detected. An application detection facet is an example of a DPI facet. An application detection facet may be used to inspect packets to detect the presence of an application, and may specify actions to take if the application is detected.

A DPI facet may include a subscriber identifier, application identifier, and/or packet classifiers. The subscriber identifier and application identifier may identify the subscriber and application, respectively, for which packets are to be inspected. The packet classifiers may include the IP address and port range of packets to be inspected. The IP address and port range may be used to validate the usage of applications and their associated packets signaled through protocols such as SIP.

Packets may be inspected for any suitable feature, for example, packet signature, bandwidth used by packets, compression protocol, content, or other suitable feature. For example, packets may be inspected to determine whether the packets include what they are supposed to include, for example, whether the packets include voice and audio instead of copyrighted files. Actions may include terminating an application, allowing the application, or notifying policy server 44 of the

presence of the application. Policy server 44 may then take further action.

According to one embodiment, a particular network facet may include tokens for different types of facets. The tokens may specify, for example, a packet classifier, a network facet state, a quality of service parameter, an authorized quality of service, and/or other suitable parameters. The packet classifier specifies the packets that are allowed through a network element. The network facet state specifies whether packets matching the packet classifier can flow through a gateway. The quality of service parameters specifies the granted quality of service. The authorized quality of service may specify the authorized envelope for the IP flow.

According to one embodiment, network facets 128 may be correlated with application facets 124. A network facet 128 may be correlated with an application facet 124 if a packet either matches the packet classifiers of both the network facet 128 and application facet 124 or matches the packet classifiers of neither. For example, a policy server 44 may match a network facet with a later-arriving application facet to make an application aware policy decision and install the decision on a network element.

Policies 114 may be static or dynamic. The facets of static policies are installed at a particular time, for example, when access terminal 20 registers with a network 24 or 28. Static policies typically depend on policy contexts that are fixed during the lifetime of the registration, such as the identity of the subscriber. The facets of dynamic policies are installed at the time access terminal 20 invokes an application.

Policies 114 may be shared between visited network 24 and home network 28. Visited network 24 and home network 28 may have agreements to recognize specific facets. Accordingly, visited network 24 that receives a policy 114 from home network 28 may make application aware policy decisions based on the policy 114 without having to deploy or otherwise support the application in question. For example, visited network 24 may de-prioritize a quality of service request for one application over another application, even though visited network 24 has not deployed either application.

FIGURE 3 illustrates an example of a call flow for establishing policy facets that may be used by system 10 of FIGURE 1. The method begins at step 150, where visited bearer manager 40a and/or visited policy server 44a facilitate registration for access terminal 20. Facilitating registration may involve receiving and sending messages for registration. Visited policy server 44a and home policy server 44b exchange capabilities at step 154 to establish the facets that each policy server 44 may support.

Visited policy server 44a requests a policy from home policy server 44b at step 158. Home policy server 44b retrieves the requested policy from services data manager 52 at step 160. The policy may include facets, for example, network and application facets. Home policy server 44b sends the policy to visited policy server 44a at step 162.

Steps 164 through 182 describe negotiation of facets. The facets may be acceptable to visited policy server 44a at step 164. In one embodiment, facets may be acceptable if they are not unacceptable. Facets may be unacceptable to a policy server 44 if policy server 44

does not support a facet or if a facet is incompatible with policies present at policy server 44. Facets of different policies may be considered incompatible if policy server 44 cannot satisfy both facets, for example, if the facets are contradictory.

Visited policy server 44a may identify an application from an application identifier of an application facet to determine whether the facets are acceptable. If the facets are acceptable, the method proceeds directly to step 186. If the facets are not acceptable, the method proceeds to step 166, where visited policy server 44a adjusts one or more of the facets. A policy server 44 may adjust a facet by changing a parameter of a facet to make the facet acceptable to policy server 44 or by removing the facet.

Visited policy server 44a notifies home policy server 44b of the adjustment at step 174. A policy server 44 may notify another policy server 44 of an adjustment by sending the adjusted facets 44 or by sending a description of the changes that make the adjustment.

The facets may be acceptable to home policy server 44b at step 178. In one embodiment, if visited policy server 44a does not support facets that apply to particular packets, home policy server 44b may instruct access terminal 20 to tunnel these packets to home bearer manager 44a for application of the facets.

If the facets are not acceptable, the method proceeds to step 182, where home policy server 44b adjusts one or more of the facets and notifies visited policy server 44a of the adjustment. The method then returns to step 164, where facets may be acceptable to visited policy server 44a. If the facets are acceptable, the method proceeds directly to step 186.

Negotiation may continue until a stopping point is reached. A stopping point may be reached when policy servers 44 agree on the facets, that is, when the facets are acceptable to policy servers 44. A stopping point may be reached when a specified number of iterations, for example, one, two, or three iterations, have been performed. If the facets are not acceptable and a stopping point has been reached, policy servers 44 may give up.

Visited policy server 44a determines a policy output according to the policy rules of the facets, and provides the policy output to visited bearer manager 40a at step 186. The policy output may comprise facets or a policy decision. The method then ends.

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 an example of a call flow for determining a policy output that may be used by system 10 of FIGURE 1. Access terminal 20 sends a SIP invite message to visited bearer manager 40a at step 210. The message uses the visited network address as the care-of address. The message includes Session Data Protocol (SDP) specifying that media streams use the visited network address. This indicates that policies may be exchanged between home network 28 and visited network 24. Visited bearer manager 40a forwards the SIP invite to application manager 56 through home bearer manager 40b at step 214.

Application manager 56 determines a policy associated with the subscriber of access terminal 20 at

step 218. The policy may include application facets. For example, an application facet may specify a telephony application with audio and video components. Application manager 56 sends the policy with the facets at step 222.

Home policy server 44b authorizes the policy at step 226. Home policy 44b forwards the policy to visited policy server 44a at step 230. Visited policy server 44a may negotiate the facets with home policy server 44a at step 232. For example, for a video call, visited policy server 44a may inform home policy server 44b that the request may proceed only with audio capabilities, and home policy server 44b may agree. Visited policy server 44a determines policy output for visited bearer manager 40a at step 234. For example, resources are granted for audio, but not for video, capabilities.

Visited policy server 44a sends the policy output to visited bearer manager 40a at step 238. In one embodiment, the policy output may include network facets that bearer manager 40a may implement. In another embodiment, the policy output may include a policy decision such as an authorization to perform the request with only audio capabilities.

Visited bearer manager 40a installs resources according to the network facets at step 242. Visited bearer manager 40a sends an outcome message indicating success at step 246. Visited policy server 44a sends an outcome message indicating that the request was allowed at step 250. Home policy server 44b instructs application manager 56 to proceed at step 254. Application manager 56 forwards the SIP response to access terminal 20 at step 258. The method then ends.

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 an example of a call flow for implementing a deep packet inspection policy that may be used by system 10 of FIGURE 1. Access terminal 20 sends a SIP invite message to visited bearer manager 40a at step 310. Visited bearer manager 40a forwards the SIP invite to application manager 56 at step 314.

Application manager 56 determines a DPI policy associated with the subscriber of access terminal 20 at step 318. The DPI policy includes DPI facets. The facets may, for example, be used to inspect media streams to verify that the streams are sending RTP audio media. A DPI facet may include packet classifiers that specify IP addresses and ports to identify packets to be inspected. Application manager 56 sends the DPI policy with the DPI facets at step 322. Home policy server 44b authorizes the policy at step 326. Home policy server 44b forwards the policy to visited policy server 44a at step 330. Visited policy server 44a determines a policy output that includes the DPI facets at step 334.

Visited policy server 44a sends the DPI facets to visited bearer manager 40a at step 338. In one embodiment, the policy output may include network facets that bearer manager 40a may implement. Visited bearer manager 40a performs deep packet inspection according to the DPI facets at step 242. Visited bearer manager 40a may inspect packets that match the packet classifiers of the DPI facets. The method then ends.

Modifications, additions, or omissions may be made to the method without departing from the scope of the invention. For example, the method may also be applied

to access terminal 20 in home network 28. The method may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order.

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 establishing one or more facets of a policy for a communication session, comprising:

facilitating registration of an access terminal at a visited network, the access terminal associated with a home network having a home policy server;

receiving the policy at a visited policy server of the visited network, the policy comprising the one or more facets;

if the one or more facets are unacceptable, negotiating the one or more facets until a stopping point is reached, the negotiation comprising:

adjusting by the visited policy server at least one facet of the one or more facets; and

notifying the home policy server of the adjustment; and

establishing the one or more facets in accordance with the negotiation.

2. The method of Claim 1, wherein negotiating the one or more facets further comprises:

receiving a notification indicating acceptance of the at least one facet adjusted by the visited policy server.

3. The method of Claim 1, wherein negotiating the one or more facets further comprises:

receiving a response comprising at least one facet adjusted by the home policy server; and

continuing negotiation if:

the at least one facet adjusted by the home policy server is unacceptable; and

the stopping point has not been reached.

4. The method of Claim 1, wherein negotiating the one or more facets further comprises:

determining if the received policy is compatible with a policy at the visited policy server.

5. The method of Claim 1, further comprising:

determining a policy output in accordance with an application identified by an application facet of the one or more facets.

6. The method of Claim 1, wherein the one or more facets further comprises:

a network facet requesting one or more network resources for an application.

7. The method of Claim 1, wherein the stopping point comprises at least one of the following:

a predetermined number of iterations have been performed; and

the one or more facets are acceptable to the home policy server and the visited policy server.

8. A visited policy server of a visited network, comprising:

a memory operable to:

store a policy comprising one or more facets; and

a processor in communication with the memory and operable to:

facilitate registration of an access terminal at the visited network, the access terminal associated with a home network having a home policy server;

receive the policy;

if the one or more facets are unacceptable, negotiate the one or more facets until a stopping point is reached, the negotiation comprising:

adjusting by the visited policy server at least one facet of the one or more facets; and

notifying the home policy server of the adjustment; and

establish the one or more facets in accordance with the negotiation.

9. The visited policy server of Claim 8, the processor further operable to negotiate the one or more facets by:

receiving a notification indicating acceptance of the at least one facet adjusted by the visited policy server.

10. The visited policy server of Claim 8, the processor further operable to negotiate the one or more facets by:

receiving a response comprising at least one facet adjusted by the home policy server; and

continuing negotiation if:

the at least one facet adjusted by the home policy server is unacceptable; and

the stopping point has not been reached.

11. The visited policy server of Claim 8, the processor further operable to negotiate the one or more facets by:

determining if the received policy is compatible with a policy at the visited policy server.

12. The visited policy server of Claim 8, the processor further operable to:

determine a policy output in accordance with an application identified by an application facet of the one or more facets.

13. The visited policy server of Claim 8, wherein the one or more facets further comprises:

a network facet requesting one or more network resources for an application.

14. The visited policy server of Claim 8, wherein the stopping point comprises at least one of the following:

a predetermined number of iterations have been performed; and

the one or more facets are acceptable to the home policy server and the visited policy server.

15. Logic for establishing one or more facets of a policy for a communication session, the logic embodied in a computer-readable storage medium and operable to:

facilitate registration of an access terminal at a visited network, the access terminal associated with a home network having a home policy server;

receive the policy at a visited policy server of the visited network, the policy comprising the one or more facets;

if the one or more facets are unacceptable, negotiate the one or more facets until a stopping point is reached, the negotiation comprising:

adjusting by the visited policy server at least one facet of the one or more facets; and

notifying the home policy server of the adjustment; and

establish the one or more facets in accordance with the negotiation.

16. The logic of Claim 15, further operable to negotiate the one or more facets by:

receiving a notification indicating acceptance of the at least one facet adjusted by the visited policy server.

17. The logic of Claim 15, further operable to negotiate the one or more facets by:

receiving a response comprising at least one facet adjusted by the home policy server; and

continuing negotiation if:

the at least one facet adjusted by the home policy server is unacceptable; and

the stopping point has not been reached.

18. The logic of Claim 15, further operable to negotiate the one or more facets by:

determining if the received policy is compatible with a policy at the visited policy server.

19. The logic of Claim 15, further operable to:

determine a policy output in accordance with an application identified by an application facet of the one or more facets.

20. The logic of Claim 15, wherein the one or more facets further comprises:

a network facet requesting one or more network resources for an application.

21. The logic of Claim 15, wherein the stopping point comprises at least one of the following:

a predetermined number of iterations have been performed; and

the one or more facets are acceptable to the home policy server and the visited policy server.

22. A system for establishing one or more facets of a policy for a communication session, comprising:

means for facilitating registration of an access terminal at a visited network, the access terminal associated with a home network having a home policy server;

means for receiving the policy at a visited policy server of the visited network, the policy comprising the one or more facets;

if the one or more facets are unacceptable, means for negotiating the one or more facets until a stopping point is reached, the negotiation comprising:

adjusting by the visited policy server at least one facet of the one or more facets; and

notifying the home policy server of the adjustment; and

means for establishing the one or more facets in accordance with the negotiation.

FIG. 1

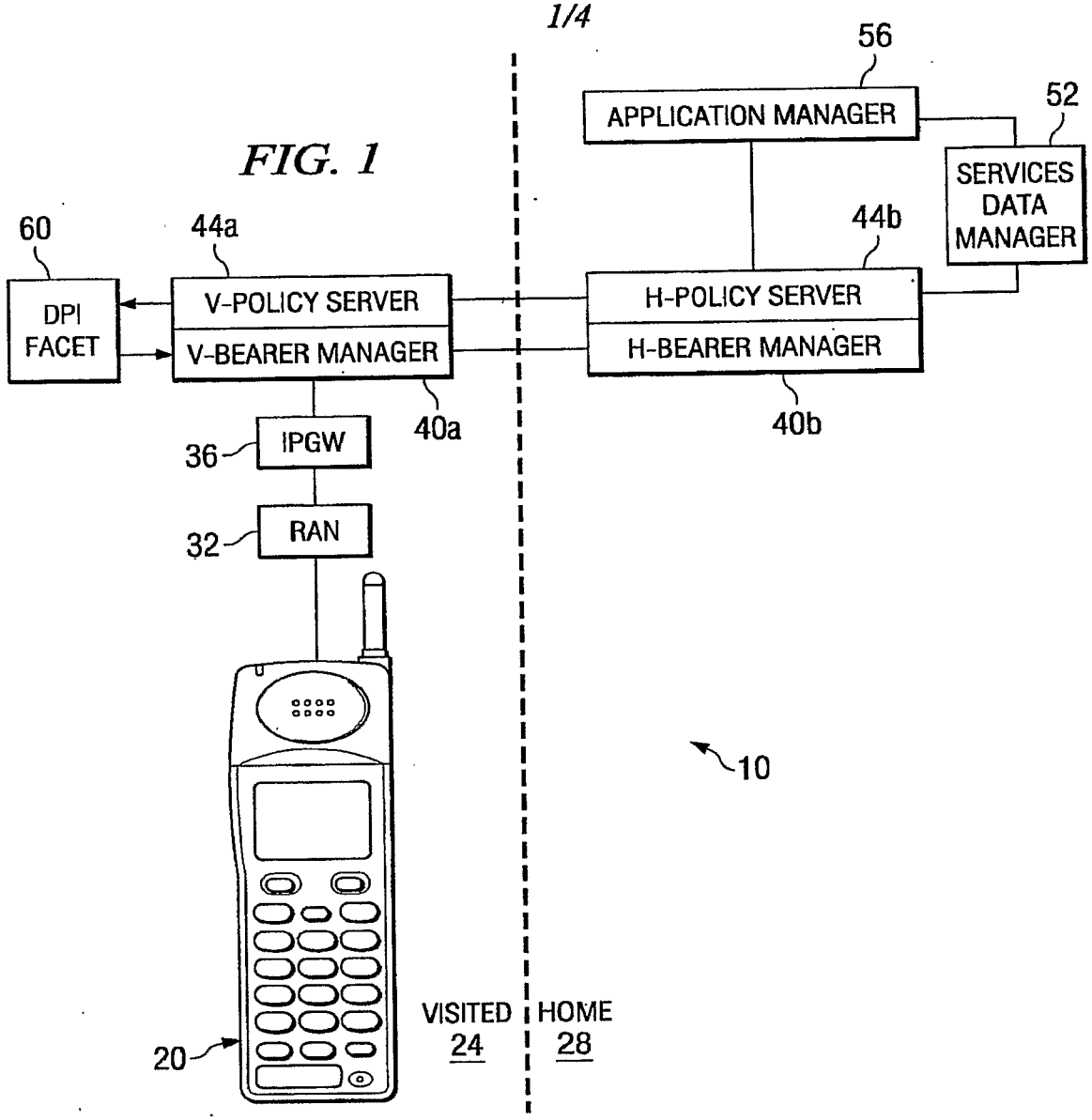

56
APPLICATION MANAGER
52
SERVICES DATA MANAGER
44b
60
44a
DPI FACET
V-POLICY SERVER
V-BEARER MANAGER
H-POLICY SERVER
H-BEARER MANAGER
40a
40b
36
IPGW
32
RAN
10
20
VISITED 24
HOME 28

FIG. 2

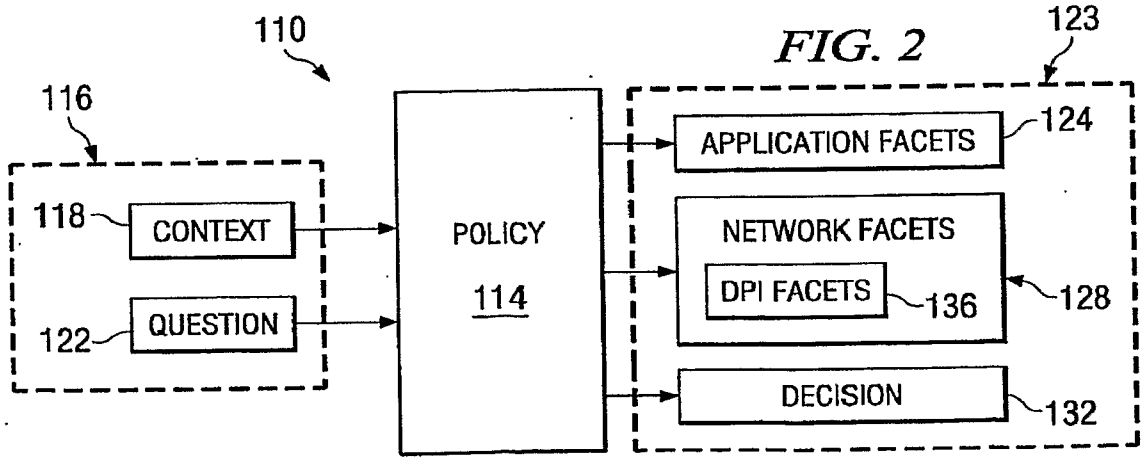
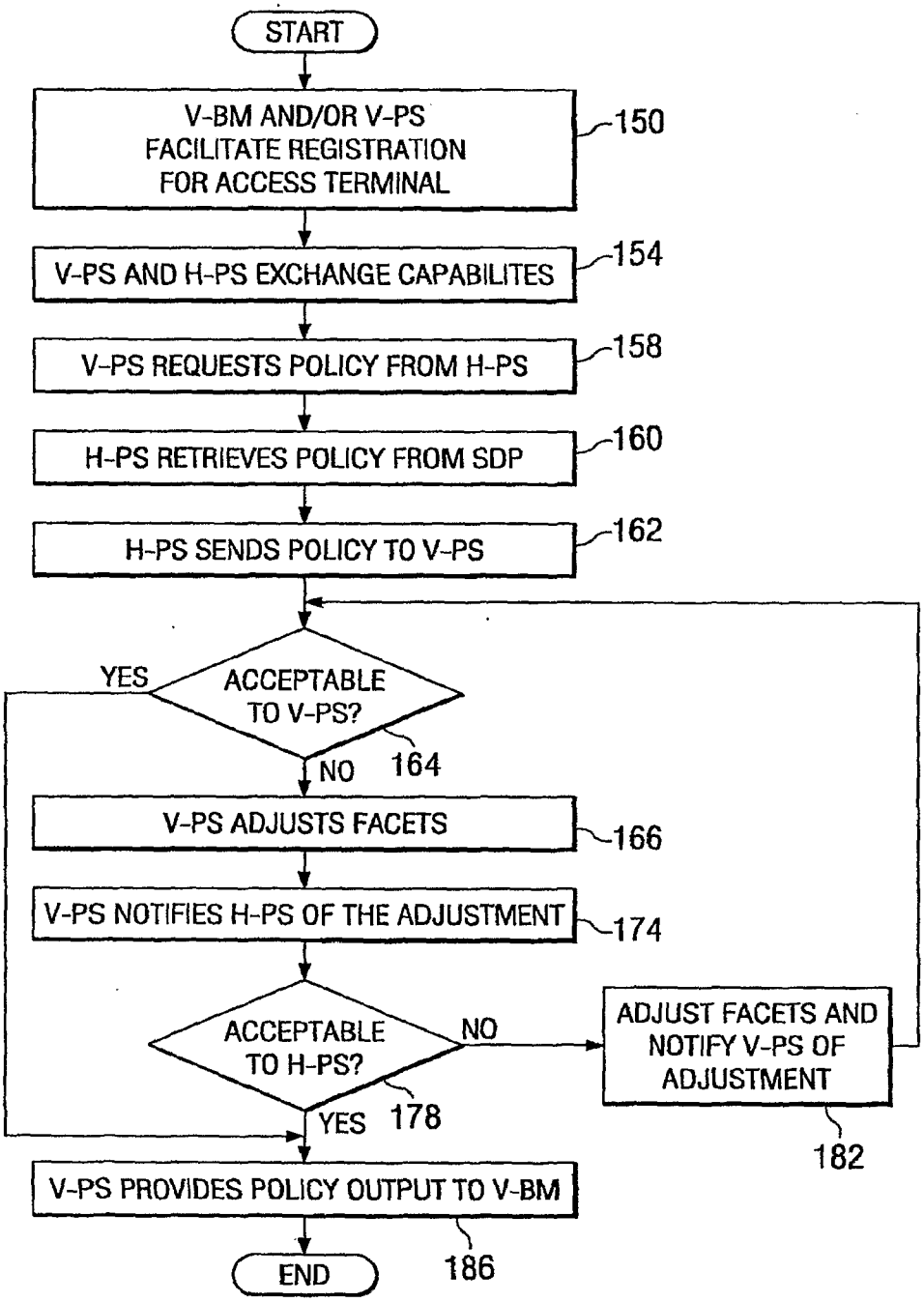

110
123
116
118
CONTEXT
122
QUESTION
POLICY
114
APPLICATION FACETS
124
NETWORK FACETS
DPI FACETS
136
128
DECISION
132

FIG. 3


START
V-BM AND/OR V-PS FACILITATE REGISTRATION FOR ACCESS TERMINAL
150
V-PS AND H-PS EXCHANGE CAPABILITES
154
V-PS REQUESTS POLICY FROM H-PS
158
H-PS RETRIEVES POLICY FROM SDP
160
H-PS SENDS POLICY TO V-PS
162
ACCEPTABLE TO V-PS?
YES
NO
164
V-PS ADJUSTS FACETS
166
V-PS NOTIFIES H-PS OF THE ADJUSTMENT
174
ACCEPTABLE TO H-PS?
NO
YES
178
ADJUST FACETS AND NOTIFY V-PS OF ADJUSTMENT
182
V-PS PROVIDES POLICY OUTPUT TO V-BM
END
186

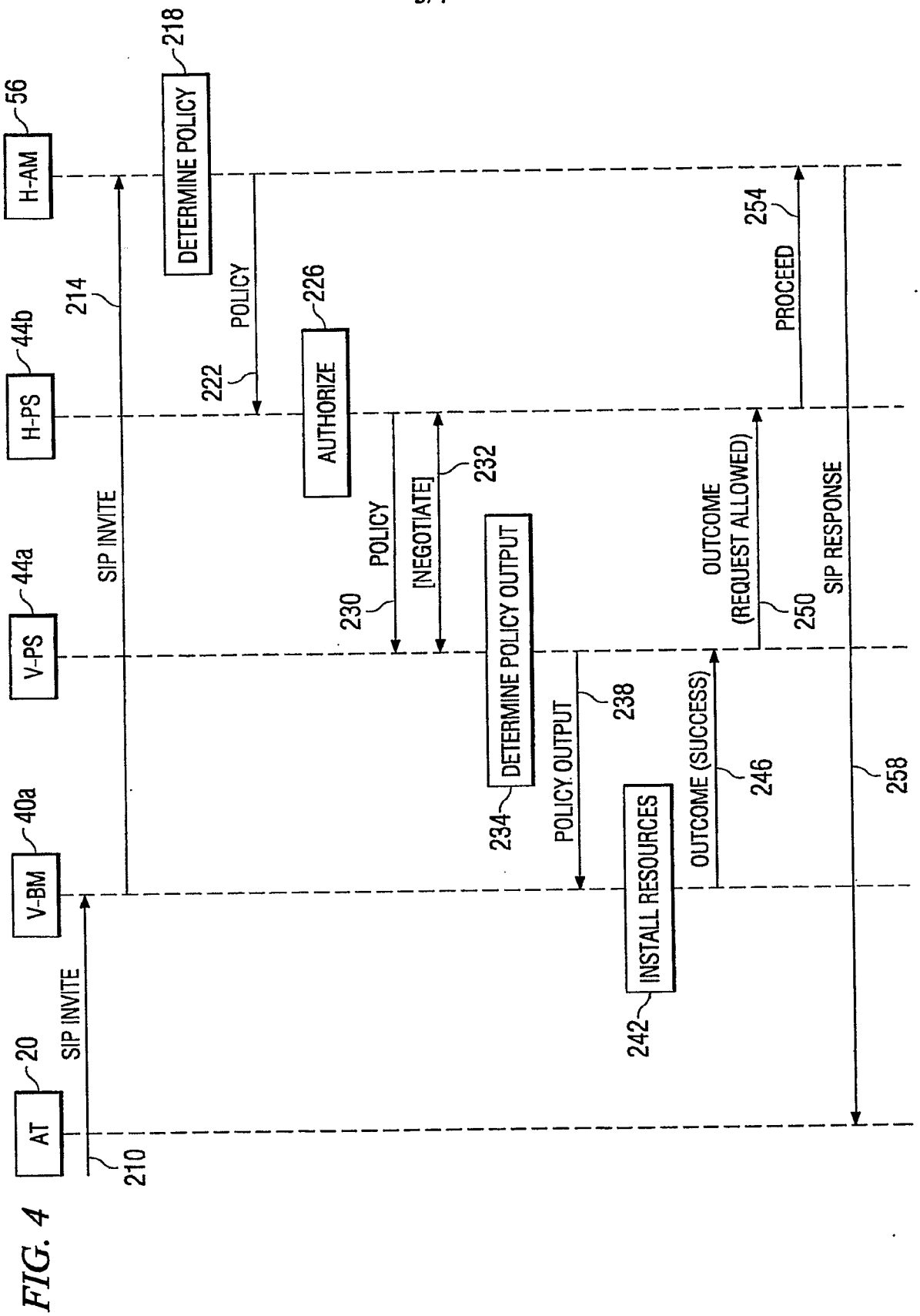

AT
20
V-BM
40a
V-PS
44a
H-PS
44b
H-AM
56
SIP INVITE
210
SIP INVITE
214
DETERMINE POLICY
218
POLICY
222
AUTHORIZE
226
POLICY
230
[NEGOTIATE]
232
DETERMINE POLICY OUTPUT
234
POLICY OUTPUT
238
INSTALL RESOURCES
242
OUTCOME (SUCCESS)
246
OUTCOME (REQUEST ALLOWED)
250
SIP RESPONSE
258
PROCEED
254

FIG. 4

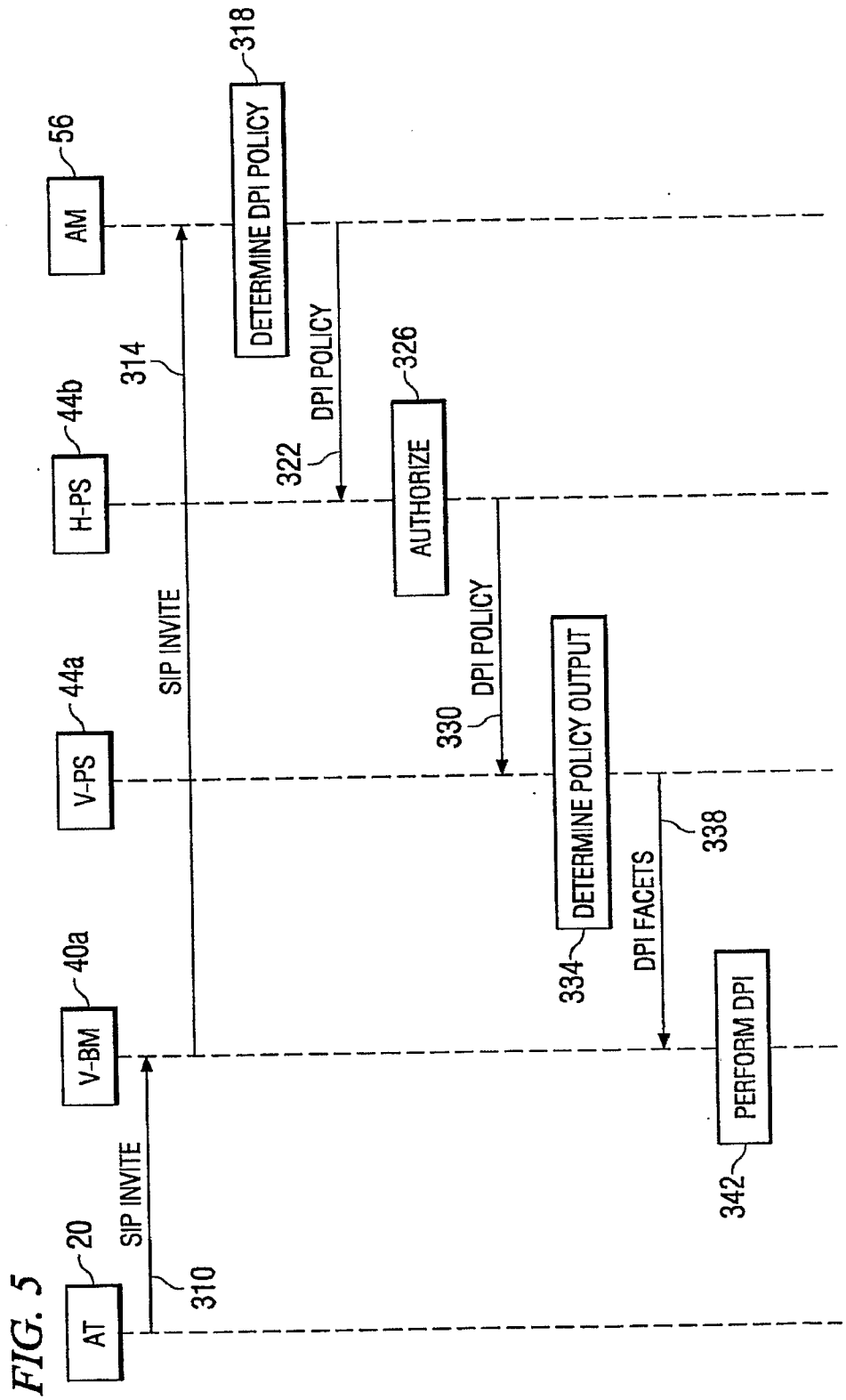

AT
20
V-BM
40a
V-PS
44a
H-PS
44b
AM
56
SIP INVITE
310
SIP INVITE
314
DETERMINE DPI POLICY
318
DPI POLICY
322
AUTHORIZE
326
DPI POLICY
330
DETERMINE POLICY OUTPUT
334
DPI FACETS
338
PERFORM DPI
342

FIG. 5