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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 November 2001 (22.11.2001)

PCT

(10) International Publication Number
WO 01/89145 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/SE01/00972

(22) International Filing Date: 4 May 2001 (04.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/570,997 15 May 2000 (15.05.2000) US

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor: **FOTI, Georges**; 163 Mozart, Dollard des Ormeaux, Quebec H9G 2Z8 (CA).

(74) Agent: **MAGNUSSON, Monica**; Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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 01/89145 A2

(54) Title: METHOD OF MONITORING CALLS IN AN INTERNET PROTOCOL (IP)-BASED NETWORK

(57) Abstract: A method of monitoring a call with a mobile terminal (MT) (11) in an Internet Protocol (IP)-based network (10) having a Gatekeeper (17) that controls the network, a plurality of access routers (12, 14) that provide access to the network, and a Monitoring Station (18) having monitoring facilities and a database of MTs to be monitored. When the MT sends an Admission Request message (21) to the Gatekeeper, the Gatekeeper sends a query (23) to the Monitoring Station asking whether the MT is to be monitored. The Monitoring Station sends a reply (25) to the Gatekeeper indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. The Gatekeeper then sends a monitoring request message (28) to the access router (12) associated with the MT. The request identifies the MT to be monitored, instructs the access router to monitor the MT, and provides a unique call identification (Call ID) and the IP address where monitored packets are to be sent. When the access router detects a packet associated with the MT, the router sends all packets associated with the MT to the Monitoring Station. The method also controls monitoring during intra-domain and inter-domain handoffs of the MT.

T-Mobile Exhibit 1025

METHOD OF MONITORING CALLS IN AN INTERNET PROTOCOL (IP)-BASED NETWORK

BACKGROUND OF THE INVENTION

Technical Field of the Invention

This invention relates to telecommunication systems and, more particularly, to a method of monitoring calls in an Internet Protocol (IP)-based network.

Description of Related Art

In existing circuit-switched telecommunications networks such as the Public Switched Telephone Network (PSTN) and the legacy Public Land Mobile Network (PLMN), law enforcement agencies are able to easily monitor telephone calls because the calls, once established, are routed over a dedicated path from one subscriber to another. In an IP-based telecommunications network, this is not the case.

For IP calls that originate in a circuit-switched network, a gateway provides an interface between the circuit-switched network and the packet-switched IP network. The gateway takes bits of digitized voice, packetizes them, puts on a header, and ships them over the IP network. The packetized call may enter the core IP network at any access (edge) router near the originating subscriber. Thereafter, the individual packets follow any available route to the destination address. At that point, all of the packets exit the core network through a single access router near the destination subscriber. The same principle applies if both the calling terminal and the called terminal are IP-based. Since one or both of the subscribers involved in the call may be mobile, calls between the same subscribers may enter and leave the IP network through different access routers at different times. As a result of the changing access routers and the independent routing of the packets in the IP network, law enforcement agencies are not able to monitor real-time IP applications such as Voice-over-IP (VoIP) calls.

It would be advantageous to have a method of monitoring calls in an Internet Protocol (IP)-based network. The present invention provides such a method.

T-Mobile Exhibit 1025

SUMMARY OF THE INVENTION

In one aspect, the present invention is a method of monitoring a call from a mobile terminal (MT) in an IP-based network having a Gatekeeper that controls the network, a plurality of access routers that provide access to the network, and a Monitoring Station having monitoring facilities and a database of MTs to be monitored. The method includes the steps of sending an access request from the MT to the Gatekeeper, sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored, and sending a reply from the Monitoring Station to the Gatekeeper indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. This is followed by sending a monitoring request from the Gatekeeper to the access router associated with the monitored MT, the request identifying the MT to be monitored, instructing the access router to monitor the MT, and providing the IP address where monitored packets are to be sent. When the access router detects a packet associated with the MT, the router sends all packets associated with the MT to the Monitoring Station.

When the monitored MT is handed off from a first base station to a second base station, and each of the base stations is controlled by a single Radio Network Controller (RNC), the RNC sends a monitoring request to the second base station. The monitoring request identifies the MT to be monitored, instructs the second base station to monitor the MT, and provides a unique call identification (Call ID) and the IP address where monitored packets are to be sent. The unique Call ID is assigned by the Gatekeeper. The RNC also sends a notification to the Gatekeeper that the MT is being served by the second base station, and includes the unique Call ID and a new transport address for the MT, if any.

When the monitored MT is handed off from a first base station controlled by a first RNC to a second base station controlled by a second RNC, and both RNCs are in a single Gatekeeper domain, the method performs the steps of sending identifying information regarding the MT being monitored from the first RNC to the second RNC, and sending a monitoring request from the second RNC to the second base station, the request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing the unique Call ID and the IP address where monitored

T-Mobile Exhibit 1025

packets are to be sent. The second RNC also sends a notification to the Gatekeeper that the MT is being served by the second base station, and includes the Call ID and the new transport address for the MT. Whenever there is a change to the transport address of the MT, the Gatekeeper forwards the Call ID and the new transport address to the Monitoring Station.

When the monitored MT is handed off from a first base station controlled by a first RNC in a first Gatekeeper domain, to a second base station controlled by a second RNC in a second Gatekeeper domain, the method performs the steps of sending a notification from the first RNC to the second RNC that the MT is being monitored, and sending a monitoring request from the second RNC to the second base station. The monitoring request identifies the MT to be monitored, instructs the base station to monitor the MT, and provides the unique Call ID and the IP address of a Monitoring Station where monitored packets are to be sent. The second base station then begins sending media packets having the MT address as a source address or destination address to the Monitoring Station. Then, the second RNC sends the unique Call ID it received and a new transport address for the MT to the second Gatekeeper. The second Gatekeeper forwards this information to the Monitoring Station. This is followed by sending an access request from the MT to the second Gatekeeper, and allocating bandwidth to the MT by the Gatekeeper.

In another aspect, the present invention is a method performed within a Gatekeeper in an IP-based network. The method monitors a call from an MT and routes the monitored call to a Monitoring Station having monitoring facilities and a database of MTs to be monitored. The method includes the steps of receiving in the Gatekeeper, a network access request from the MT, sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored, and receiving in the Gatekeeper, a reply from the Monitoring Station indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent. This is followed by sending a monitoring request from the Gatekeeper to the access router that is associated with the monitored MT and is providing access to the network. The request identifies the MT to be monitored, instructs the access router

to send any packets associated with the MT to the Monitoring Station, and provides the unique Call ID and the IP address where monitored packets are to be sent.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood and its numerous objects and advantages will become more apparent to those skilled in the art by reference to the following drawings, in conjunction with the accompanying specification, in which:

FIG. 1 is an illustrative drawing of an IP network modified in accordance with the teachings of the present invention to monitor a call between two IP terminals;

FIG. 2 is a message flow diagram illustrating the flow of messages when setting up a call for monitoring in the IP network of FIG. 1 in accordance with the teachings of the present invention;

FIG. 3 is an illustrative drawing of an IP network modified in accordance with the teachings of the present invention to monitor a call between an IP terminal and a terminal in the Public Switched Telephone Network (PSTN);

FIG. 4 is a message flow diagram illustrating the flow of messages when a monitored mobile terminal is handed off from an old base station to a new base station controlled by the same Radio Network Controller (RNC) as the old base station;

FIG. 5 is a message flow diagram illustrating the flow of messages when a monitored mobile terminal roams into a new subnet within the same domain, and acquires a new RNC, a new base station, and a new transport address; and

FIG. 6 is a message flow diagram illustrating the flow of messages when the mobile terminal roams into a new domain and acquires a new Gatekeeper, a new RNC, a new base station, and a new transport address.

DETAILED DESCRIPTION OF EMBODIMENTS

The present invention is described herein primarily in terms of the International Telecommunications Union (ITU) H.323 protocol, but is equally applicable to both H.323 and the Session Initiation Protocol (SIP) developed by the Internet Engineering Task Force (IETF). In particular, the term "Gatekeeper" which

is used herein refers to both an H.323 Gatekeeper and a SIP proxy server and registry. In addition, reference to an H.245 address herein also refers to a SIP address.

In a typical IP network, PC clients or IP telephony terminals (fixed or mobile) are identified and addressed by an e-mail address (proxy/alias), or an IP address, or both. Prior to making any calls, such terminals register with a Gatekeeper in an H.323 network, or with a SIP proxy server in a SIP network. If the registration is accepted by the Gatekeeper, the Gatekeeper handles incoming calls to the terminal as well as outgoing calls from the terminal. The Gatekeeper maintains a subscriber profile that includes, among other things, the services to which the subscriber is entitled. For simplicity, the term "mobile terminal (MT)" is used herein to refer generically to IP clients, both fixed and mobile since the most challenging monitoring tasks involve intra-domain and inter-domain handoff of MTs.

FIG. 1 is an illustrative drawing of an IP network 10 modified in accordance with the teachings of the present invention to monitor a call between two IP terminals. IP Terminal-1 11, which may be originating a call, is connected to the IP network through Access Router-1 12. Media traffic (i.e., data) 13 is carried by independent paths through the network to Access Router-2 14 through which IP Terminal-2 15 has accessed the network. IP Terminal-2 may be the terminating (destination) terminal. Control signaling between the two subscribers is carried in a control plane 16 which passes through a Gatekeeper 17, and from the Gatekeeper to a Monitoring Station 18 which may be operated by a law enforcement agency.

In order for the two IP subscribers 11 and 15 to communicate over the IP-based network 10, they have to go through the Gatekeeper 17 which can be likened to a mobile switching center (MSC) in a circuit-switched network. The Gatekeeper is the brain of the network regarding the routing of calls. The Gatekeeper manages the bandwidth (with the help of other network entities), generates the accounting data, etc.

In a first scenario, the calling and called subscribers are within the same domain. In that case, when a subscriber wants to make or receive a call, an Admission Request (ARQ) message (when using H.323) is sent to the Gatekeeper. In response to the ARQ message, the Gatekeeper allocates the bandwidth for the call or, if none is available, the Gatekeeper denies the call. The present invention extends the

procedure performed by the Gatekeeper when a bandwidth allocation request (i.e., ARQ) is received from a device that is originating or receiving a call. Additionally, new mandatory parameters are introduced in the ARQ message.

The Gatekeeper does not know which subscribers need to be monitored. Only the law enforcement Monitoring Station has this information. The Monitoring Station includes a database of all subscribers who should be monitored for security reasons. So for each call that is originated by or terminated to a subscriber in its domain, the Gatekeeper queries the Monitoring Station to determine whether the subscriber should be monitored.

FIG. 2 is a message flow diagram illustrating the flow of messages when setting up a call for monitoring in the IP network of FIG. 1 in accordance with the teachings of the present invention. In the illustrated example, IP Terminal-1 11 is the subscriber to be monitored. After Terminal-1 sends an ARQ message 21 to the Gatekeeper 17, the Gatekeeper performs the bandwidth allocation function at 22, and then sends a monitor query message 23 to the Monitoring Station 18. The monitor query message includes the H.245 source address and the H.245 destination address for the call, if available, as well as subscriber addressing information (e-mail/proxy) and the unique Call ID that it generates for the call. The Monitoring Station checks the database at 24 and returns a monitor reply message 25 to the Gatekeeper indicating whether any of the parties in the call should be monitored, as well as the IP address of the Monitoring Station to which the monitored conversation should be sent. In the illustrated example, the message indicates that Terminal-1 is to be monitored. If none of the terminals is being monitored, the Gatekeeper then returns an Admission Confirm (ACF) message 26 to Terminal-1. If any of the subscribers is being monitored, the Gatekeeper sets a flag in the subscriber record at 27 indicating that fact.

The Gatekeeper finds, through normal IP routing protocols, the path for the media to follow. The Gatekeeper obtains this information in the course of allocating bandwidth since the policy related to the QoS of the call must be downloaded to all of the routers in the media path. The routers, in this case, act as policy enforcement points to ensure that the subscribers are respecting the QoS agreements. However, for

the sake of monitoring, it suffices that the Gatekeeper identifies only the access router associated with IP Terminal-1.

Hence, the Gatekeeper is able to identify the access router for this call. The Gatekeeper then sends a Monitoring Request message 28 to the access router associated with the subscriber (for example, Access Router-1), and includes the Monitoring Station IP address and the unique Call ID for that call. Access Router-1 sends back an Acknowledgment message 29. Once the Gatekeeper receives the Acknowledgment message from the Access Router, the Gatekeeper sends an ACF message 31 to Terminal-1.

It should also be noted that in IP networks, addressing is different in each media direction. Therefore, the IP address to be monitored is the source address in the IP header while the monitored subscriber is initiating the conversation, and is the destination field in the IP header while the monitored subscriber is listening. Thus, while the Access Router performs its normal routing functions, it has to monitor both the source and the destination addresses in the IP headers that it handles in order to identify addresses that match the monitored address. Media packets then begin to flow from the IP Terminal to Access Router-1 at 32, and Access Router-1 sends the packets to the Monitoring Station at 33.

To send media packets to the Monitoring Station, the Access Router encapsulates every identified packet with a new header that includes the router's address as the source address, and the Monitoring Station's address as the destination address. The unique Call ID is also included in the IP header. This enables the Monitoring Station to correlate packets belonging to the same conversation. Other parameters may be included in the header as well. Upon receipt, the Monitoring Station strips away the header and recovers the original packets. When the call is cleared, the connection from the access router to the Monitoring Station is also cleared.

In another scenario, the calling and called subscribers are in different domains. In that case, two different Gatekeepers must deal with the calling and called subscribers. Additional information must be exchanged between the Gatekeepers as

part of the call setup for the management and coordination of monitoring a call. Otherwise, both Gatekeepers may end up monitoring the same call.

In this scenario, the originating Gatekeeper will likely not know the IP address of the destination. Thus, the originating Gatekeeper follows the same procedure previously described. However, the query that the originating Gatekeeper sends to the Monitoring Station includes only the calling subscriber identity. If the calling subscriber is not the one being monitored, then the originating Gatekeeper returns an ACF message and proceeds with normal call setup. During the setup, the originating Gatekeeper forwards to the Gatekeeper that deals with the destination terminal, a special flag informing the destination Gatekeeper that the calling subscriber is not the one being monitored. The destination Gatekeeper follows the previously described procedure, including the monitoring procedure, when the called terminal sends an ARQ message to accept the incoming call.

On the other hand, if the calling subscriber is the one being monitored, the originating Gatekeeper follows the same procedure described previously when it receives an ARQ message from the calling subscriber. The originating Gatekeeper then sends a flag to the destination Gatekeeper identifying the calling subscriber as a subscriber to be monitored. The destination Gatekeeper follows the same procedure previously described when the called terminal sends an ARQ message to accept the call, but bypasses the monitoring procedure.

It should also be noted that in this scenario, the originating Gatekeeper receives only the destination IP address as part of the call setup procedure. Therefore, the originating Gatekeeper must send a second Monitoring Request Message to the Access Router to convey the destination IP address.

FIG. 3 is an illustrative drawing of an IP network 20 modified in accordance with the teachings of the present invention to monitor a call between an IP terminal (IP Terminal-3) 41 and a terminal in a circuit-switched network (PSTN Terminal) 42 such as the Public Switched Telephone Network (PSTN) 43. If the subscriber to be monitored is in a circuit-switched network such as the PSTN, the call goes through a Gateway 44 to the IP subscriber in the IP network. If the subscriber to be monitored is on the PSTN side, then existing procedures in the PSTN ensure that monitoring

takes place. However, if the subscriber to be monitored is on the IP side, the procedure described previously is invoked when the called subscriber (to be monitored) sends an ARQ message to the Gatekeeper to accept an incoming call.

Again in this case, coordination is needed to ensure that no double monitoring occurs when both subscribers are to be monitored. Therefore, for an H.323 endpoint of the gateway type (as opposed to a terminal type of endpoint), the ARQ message sent to the Gatekeeper from the Gateway 44 includes a flag to indicate whether an incoming call is already being monitored from the PSTN side. The Gatekeeper then bypasses the monitoring procedure. The PSTN, of course, must convey this information to the Gateway so that it can be passed to the Gatekeeper. In one embodiment, Integrated Services User Part (ISUP) signaling is extended to carry this information. Optionally, specialized control messages can convey the information to the Gateway from the entity that is coordinating the monitoring in the PSTN. In all cases, the globally unique Call ID must be transferred to uniquely identify the impacted call.

Mobility/Handoff Scenarios

Mobility adds another level of complexity to the task of IP monitoring due to the potential changing of the point of attachment of the MT to the network. In this case, the base stations serve as Access Routers since they are the closest point of attachment to the subscriber. However, Gatekeepers do not communicate directly with base stations since base stations belong to the Radio Access Network (RAN). Therefore, the Gatekeepers must go through the Radio Network Controller/Base Station Controller (RNC/BSC) that controls these base stations for all requests to the base stations regarding the monitoring of subscribers.

Therefore, the same procedures described above for monitoring fixed subscribers still apply for mobile subscribers except that all Gatekeeper requests that are sent directly to the Access Routers for fixed subscribers, are sent instead to the RNC. The RNC, in turn, sends them to the base stations.

FIG. 4 is a message flow diagram illustrating the flow of messages when the monitored mobile terminal (MT) is handed off from an old base station (BS-1) 51 to a new base station (BS-2) 52 controlled by the same RNC 53 as the old base station.

When the MT does not change its transport address, but roams in a new base station, the link layer in the base station ensures delivery of the call to the MT. After handoff occurs at 54, the RNC instructs BS-2 to monitor the subscriber at 55 and includes the address of the Monitoring Station and the unique Call ID. The RNC then informs the Gatekeeper 17 of the new base station at 56, and includes the unique Call ID to identify the impacted call. If there is a change in the transport address of the mobile terminal as a result of the handoff, the new address is also sent to the Gatekeeper by the RNC. The RNC learns the new address during the handoff procedure. In the preferred embodiment, this information is passed only for monitored subscribers in order to minimize the signaling load. At 57, the Gatekeeper forwards the Call ID and the new transport address, if any, to the Monitoring Station 18. At 58, media is passed from BS-2 to the Monitoring Station.

FIG. 5 is a message flow diagram illustrating the flow of messages when the monitored MT is handed off from an old base station (BS-1) 61 controlled by an old RNC (RNC-1) 62 to a new base station (BS-3) 63 controlled by a new RNC (RNC-2) 64 within the same Gatekeeper domain. Thus, in this scenario, the MT roams into a new subnet within the same domain, and acquires a new RNC, a new base station, and a new transport address. At 65, the MT is handed off from BS-1 to BS-3. At 66, RNC-1forwards to RNC-2 all of the pertinent information regarding the subscriber being monitored, including the unique Call ID for the call being monitored. At 67, the new RNC (RNC-2) instructs the new base station (BS-3) to monitor the subscriber, and includes the unique Call ID and the address of the Monitoring Station.

Since the mobile terminal changed transport addresses, it is required to register its new transport address with the Gatekeeper 17. Therefore, at 68, RNC-2 informs the Gatekeeper of the new base station and the new transport address assigned to the mobile terminal. The unique Call ID is also included. At 69, the new transport address and the Call ID are passed by the Gatekeeper to the Monitoring Station 18 so that all the packets belonging to the same monitored call can be correlated. Thereafter, media packets are forwarded from BS-3 to the Monitoring Station at 70.

FIG. 6 is a message flow diagram illustrating the flow of messages when the mobile terminal roams into a new domain and acquires a new Gatekeeper, a new RNC,

a new base station, and a new transport address. The monitored MT 71 is initially operating in IP Network-1 which includes Gatekeeper-1 72. RNC-1 73 and BS-1 74 are in RAN-1 which provides radio access for IP Network-1. At handoff 75, the monitored MT is handed off from BS-1 to a new base station (BS-2) 76 controlled by a new RNC (RNC-2) 77. RNC-2 and BS-2 are in RAN-2 which provides radio access for IP Network-2 which includes Gatekeeper-2 78. Monitoring Station 18 is monitoring the call with the MT.

At 79, the new RNC (RNC-2) is informed by RNC-1 that the MT is being monitored. At 81, the RNC-2 instructs the new base station (BS-2) to monitor the subscriber, and includes the unique Call ID and the address of the Monitoring Station. Media then begins to flow from BS-2 to the Monitoring Station at 82. RNC-2 then informs Gatekeeper-2 at 83 that a new subscriber is now roaming in its service area, and that the new subscriber needs to be monitored. RNC-2 includes the IMSI for the MT, the unique Call ID, and the MT's new transport address in the message to Gatekeeper-2. Every time there is a change in the transport address of a monitored mobile terminal, the controlling Gatekeeper must inform the Monitoring Station of the new transport address. Thus, at 84, the new transport address and the Call ID are passed to the Monitoring Station. The unique Call ID is used by the Monitoring Station to track all packets belonging to the same conversation. In addition, the Call ID is used by any Gatekeeper that handles a portion of the call (other than the original Gatekeeper) to report the same call to the Monitoring Station. Thus, during a handoff scenario, the RNC passes the Call ID to the same Gatekeeper if there is no change of domain, and to the new Gatekeeper when there is a change of domain.

At 85, Gatekeeper-2 sets a flag in the subscriber record for MT 71 indicating that the MT is in its area and is being monitored. The flag also indicates that a subscriber will soon have to register with his transport address. Since the MT changed its transport address, the MT is required to register with the new Gatekeeper and report its new transport address. A registration timer is started when the flag is set in case the registration never arrives (registration is lost, subscriber hangs up, etc.).

At 86, an ARQ message is sent from the MT to Gatekeeper-2. When the ARQ arrives, the registration timer in Gatekeeper-2 is stopped at 87, and bandwidth is

allocated. Gatekeeper-2 then returns an ACF message 88 to the MT. Gatekeeper-2 knows that the MT is being monitored because Gatekeeper-2 was informed by RNC-2. Therefore, Gatekeeper-2 does not perform the monitoring procedure associated with the new registration. Thus, double monitoring of the conversation is avoided.

Whenever any monitored subscriber hangs up, a De-Admission Request is sent to the Gatekeeper. The Gatekeeper clears the flag for monitoring the subscriber and sends a message to the Monitoring Station to stop the monitoring of the call. This message is also propagated to the Access Router performing the monitoring.

It is thus believed that the operation and construction of the present invention will be apparent from the foregoing description. While the method shown and described has been characterized as being preferred, it will be readily apparent that various changes and modifications could be made therein without departing from the scope of the invention as defined in the following claims.

WHAT IS CLAIMED IS:

1. A method of monitoring a call with an Internet Protocol (IP) client in an IP-based network having a Gatekeeper that controls the network, a plurality of access routers that provide access to the network, and a Monitoring Station having monitoring facilities and a database of IP clients to be monitored, said method comprising:

sending an access request from the IP client to the Gatekeeper;

sending a query from the Gatekeeper to the Monitoring Station asking whether the IP client is to be monitored;

sending a reply from the Monitoring Station to the Gatekeeper indicating that the IP client is to be monitored and providing an IP address where monitored packets are to be sent;

sending a monitoring request from the Gatekeeper to an access router associated with the IP client, said request identifying the IP client to be monitored, instructing the access router to monitor the IP client, and providing the IP address where monitored packets are to be sent;

detecting by the access router, a packet associated with the IP client; and

routing by the access router, all packets associated with the IP client to the Monitoring Station.

2. The method of monitoring a call with an IP client in an IP-based network of claim 1 further comprising, before the step of sending a query from the Gatekeeper to the Monitoring Station asking whether the IP client is to be monitored, the step of performing bandwidth allocation functions by the Gatekeeper to determine whether network access can be granted to the IP client.

3. The method of monitoring a call with an IP client in an IP-based network of claim 2 further comprising, after the step of sending a reply from the Monitoring Station to the Gatekeeper indicating that the IP client is to be monitored,

the step of setting a flag in the Gatekeeper identifying the IP client as a monitored IP client.

4. The method of monitoring a call with an IP client in an IP-based network of claim 3 further comprising, after the step of sending a monitoring request from the Gatekeeper to the access router, the steps of:

sending an acknowledgment message from the access router to the Gatekeeper; and

sending an admission confirm message from the Gatekeeper to the IP client when the acknowledgment message has been received from the access router.

5. The method of monitoring a call with an IP client in an IP-based network of claim 4 wherein the step of detecting a packet associated with the IP client includes detecting a packet that has the IP client as its source address.

6. The method of monitoring a call with an IP client in an IP-based network of claim 4 wherein the step of detecting a packet associated with the IP client includes detecting a packet that has the IP client as its destination address.

7. The method of monitoring a call with an IP client in an IP-based network of claim 3 further comprising the steps of:

sending a de-admission request from the IP client to the Gatekeeper;

clearing the flag in the Gatekeeper that identifies the IP client as a monitored IP client;

sending a message from the Gatekeeper to the Monitoring Station to stop the monitoring of the call; and

sending a message from the Gatekeeper to the access router to stop the routing of packets to the Monitoring Station.

8. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the IP client is a mobile terminal (MT), and the method further comprises the steps of:

handing off the MT from a first base station to a second base station, each of said base stations being controlled by a single radio network controller (RNC);

sending a monitoring request from the RNC to the second base station, said request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing a unique call identification (Call ID) and the IP address where monitored packets are to be sent; and

sending a notification from the RNC to the Gatekeeper that the MT is being served by the second base station, said notification including the unique Call ID and a new transport address for the MT.

9. The method of monitoring a call with an IP client in an IP-based network of claim 8 further comprising sending the Call ID and the new transport address from the Gatekeeper to the Monitoring Station.

10. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the IP client is a mobile terminal (MT), and the method further comprises the steps of:

handing off the MT from a first base station to a second base station, the first base station being controlled by a first radio network controller (RNC), and the second base station being controlled by a second RNC, and both RNCs being in a single Gatekeeper domain;

sending identifying information regarding the MT being monitored from the first RNC to the second RNC, said information including a unique call identification (Call ID);

sending a monitoring request from the second RNC to the second base station, said request identifying the MT to be monitored, instructing the second base station to monitor the MT, and providing the unique Call ID and the IP address where monitored packets are to be sent;

sending a notification from the second RNC to the Gatekeeper that the MT is being served by the second base station, said notification including the unique Call ID and a new transport address for the MT; and

sending the Call ID and the new transport address from the Gatekeeper to the Monitoring Station.

11. The method of monitoring a call with an IP client in an IP-based network of claim 1 wherein the step of detecting a packet associated with the IP client includes detecting a media having the IP client address as either a source address or destination address.

12. The method of monitoring a call with an IP client of claim 11 wherein the step of routing all packets associated with the IP client to the Monitoring Station includes encapsulating each packet associated with the IP client with a new header that includes the router's address as a source address, and the Monitoring Station's address as a destination address.

13. A method of handing off a monitored mobile terminal (MT) in an Internet Protocol (IP)-based network, said method comprising:

handing off the MT from a first base station to a second base station, the first base station being controlled by a first radio network controller (RNC) in a first Gatekeeper domain, and the second base station being controlled by a second RNC in a second Gatekeeper domain,

sending a notification from the first RNC to the second RNC that the MT is being monitored, said notification including a unique call identification (Call ID) and an IP address of a Monitoring Station where monitored packets are to be sent;

sending a monitoring request from the second RNC to the second base station, said request identifying the MT to be monitored, instructing the base station to monitor the MT, and providing the Call ID and the IP address of the Monitoring Station;

sending by the second base station, media packets having the MT address as a source address or destination address to the Monitoring Station;

sending the unique Call ID and a new transport address for the MT from the second RNC to the second Gatekeeper;

sending the unique Call ID and the new transport address for the MT from the second Gatekeeper to the Monitoring Station;

sending an access request from the MT to the second Gatekeeper; and

allocating bandwidth to the MT by the Gatekeeper.

14. The method of handing off a monitored MT in an IP-based network of claim 13 further comprising, after the step of sending a unique Call ID and a new transport address for the MT from the second RNC to the second Gatekeeper and to the Monitoring Station, the steps of:

setting a flag in the second Gatekeeper indicating that a monitored MT is in the second Gatekeeper's area, and that the MT will soon register with the second Gatekeeper; and

starting a registration timer in the second Gatekeeper.

15. The method of handing off a monitored MT in an IP-based network of claim 14 further comprising the steps of:

sending a de-admission request from the monitored MT to the second Gatekeeper;

clearing the flag in the second Gatekeeper that identifies the MT as a monitored MT;

sending a message from the second Gatekeeper to the Monitoring Station to stop the monitoring of the call; and

sending a message from the second Gatekeeper to the second base station to stop the routing of packets to the Monitoring Station.

16. The method of handing off a monitored MT in an IP-based network of claim 13 further comprising, after the step of sending an access request from the MT to the second Gatekeeper, the step of stopping the registration timer.

17. The method of handing off a monitored MT in an IP-based network of claim 13 wherein the step of sending media packets having the MT address as a source address or destination address to the Monitoring Station includes encapsulating each packet associated with the MT with a new header that includes the second base station's address as a source address, and the Monitoring Station's address as a destination address.

18. A method of monitoring a call with a mobile terminal (MT) and routing the monitored call to a Monitoring Station having monitoring facilities and a database of MTs to be monitored, said method being performed within a Gatekeeper in an Internet Protocol (IP)-based network, and comprising the steps of:

receiving in the Gatekeeper, a network access request from the MT;

sending a query from the Gatekeeper to the Monitoring Station asking whether the MT is to be monitored;

receiving in the Gatekeeper, a reply from the Monitoring Station indicating that the MT is to be monitored and providing an IP address where monitored packets are to be sent; and

sending a monitoring request from the Gatekeeper to an access router providing the MT with access to the network, said request identifying the MT to be monitored, instructing the access router to send any packets associated with the MT to the Monitoring Station, and providing a unique call identification (Call ID) and the IP address where monitored packets are to be sent.

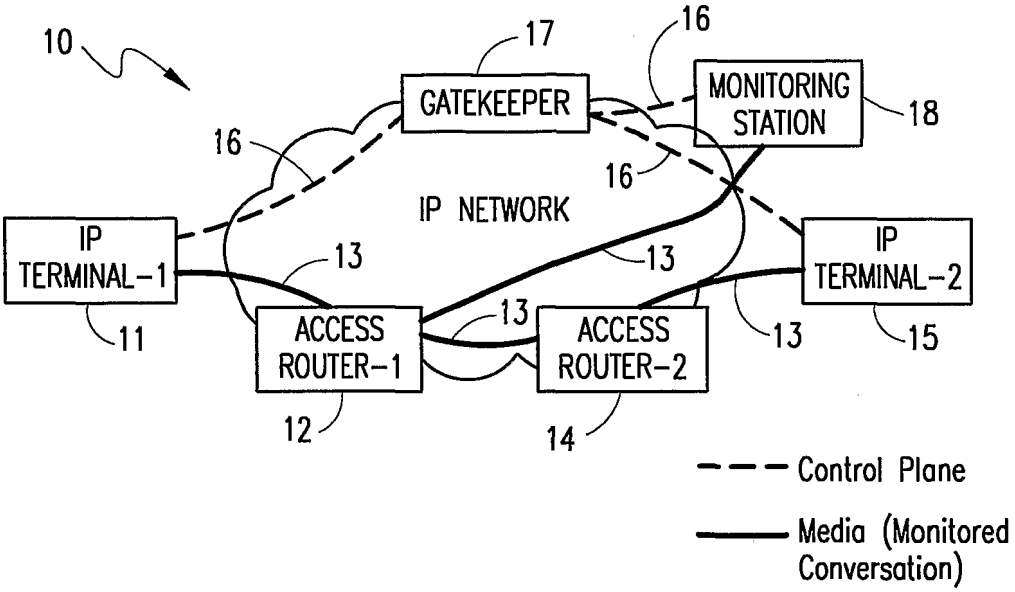
10
17
16
GATEKEEPER
MONITORING STATION
18
16
16
IP NETWORK
IP TERMINAL-1
13
13
IP TERMINAL-2
11
ACCESS ROUTER-1
13
ACCESS ROUTER-2
13
15
12
14
Control Plane
Media (Monitored Conversation)

FIG. 1

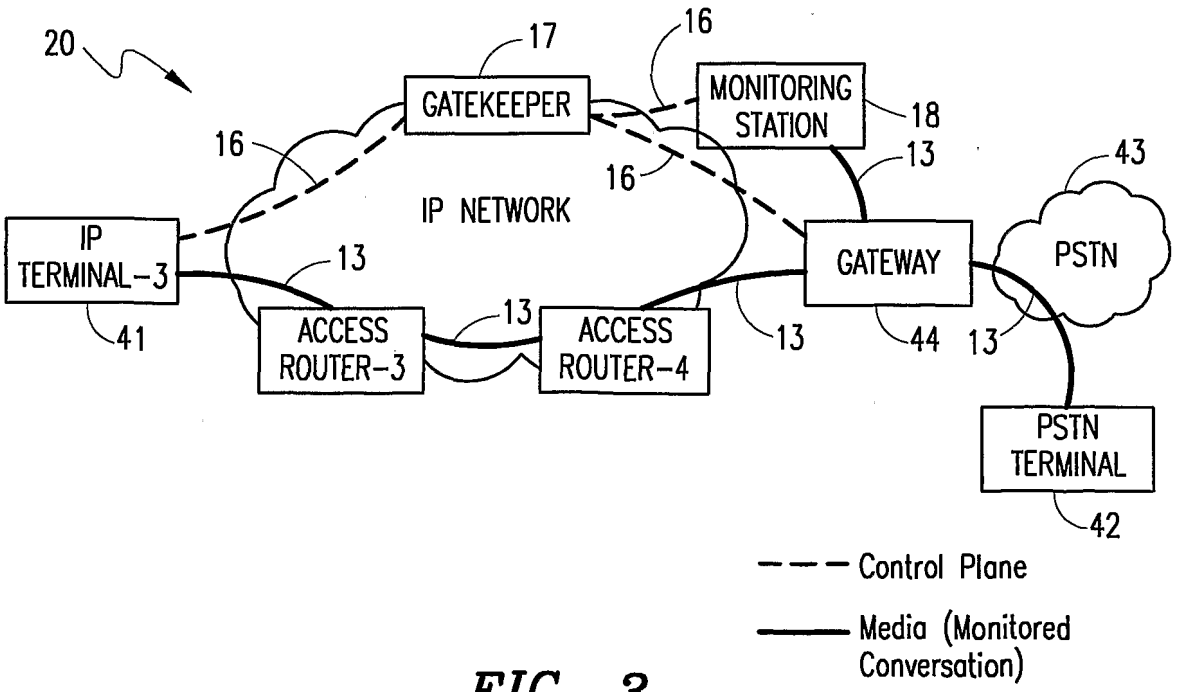
20
17
16
GATEKEEPER
MONITORING STATION
18
16
13
43
16
IP NETWORK
IP TERMINAL-3
13
GATEWAY
PSTN
41
ACCESS ROUTER-3
13
ACCESS ROUTER-4
13
44
13
PSTN TERMINAL
42
Control Plane
Media (Monitored Conversation)

FIG. 3

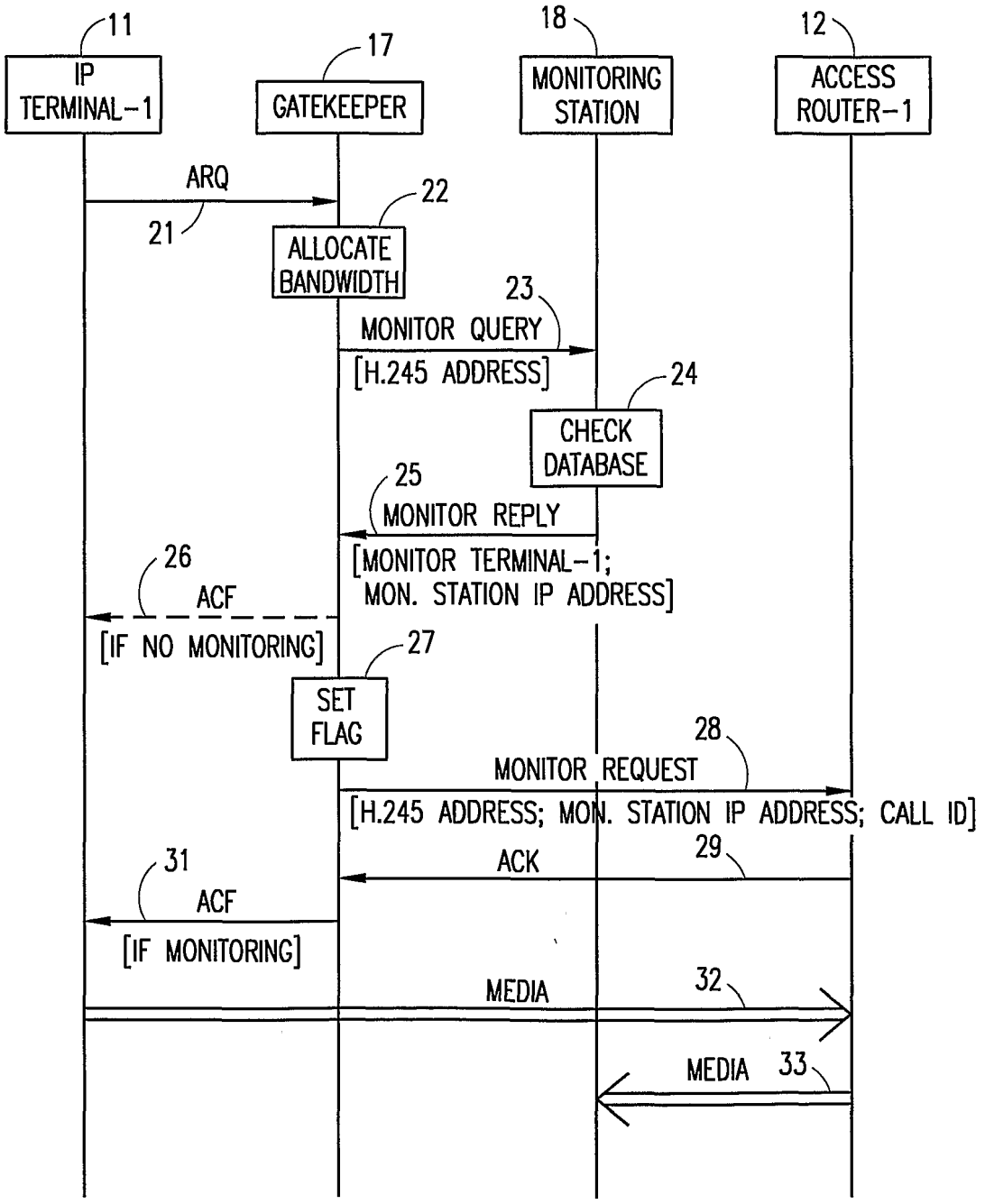
11
IP TERMINAL-1
17
GATEKEEPER
18
MONITORING STATION
12
ACCESS ROUTER-1
ARQ
21
22
ALLOCATE BANDWIDTH
23
MONITOR QUERY
[H.245 ADDRESS]
24
CHECK DATABASE
25
MONITOR REPLY
[MONITOR TERMINAL-1;
MON. STATION IP ADDRESS]
26
ACF
[IF NO MONITORING]
27
SET FLAG
28
MONITOR REQUEST
[H.245 ADDRESS; MON. STATION IP ADDRESS; CALL ID]
29
ACK
31
ACF
[IF MONITORING]
32
MEDIA
33
MEDIA

FIG. 2

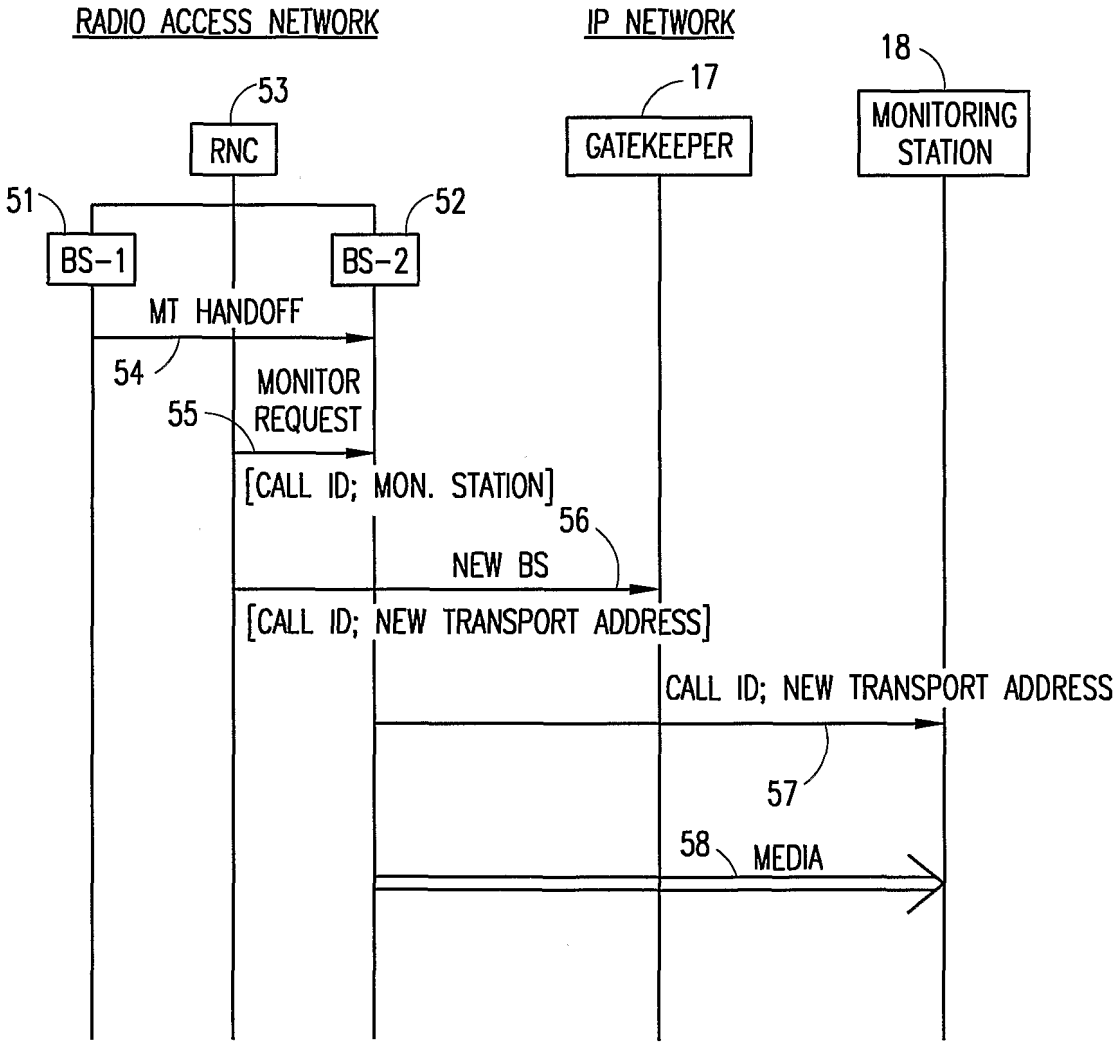
RADIO ACCESS NETWORK
IP NETWORK
53
RNC
17
GATEKEEPER
18
MONITORING STATION
51
BS-1
52
BS-2
MT HANDOFF
54
MONITOR REQUEST
55
[CALL ID; MON. STATION]
56
NEW BS
[CALL ID; NEW TRANSPORT ADDRESS]
CALL ID; NEW TRANSPORT ADDRESS
57
58
MEDIA

FIG. 4

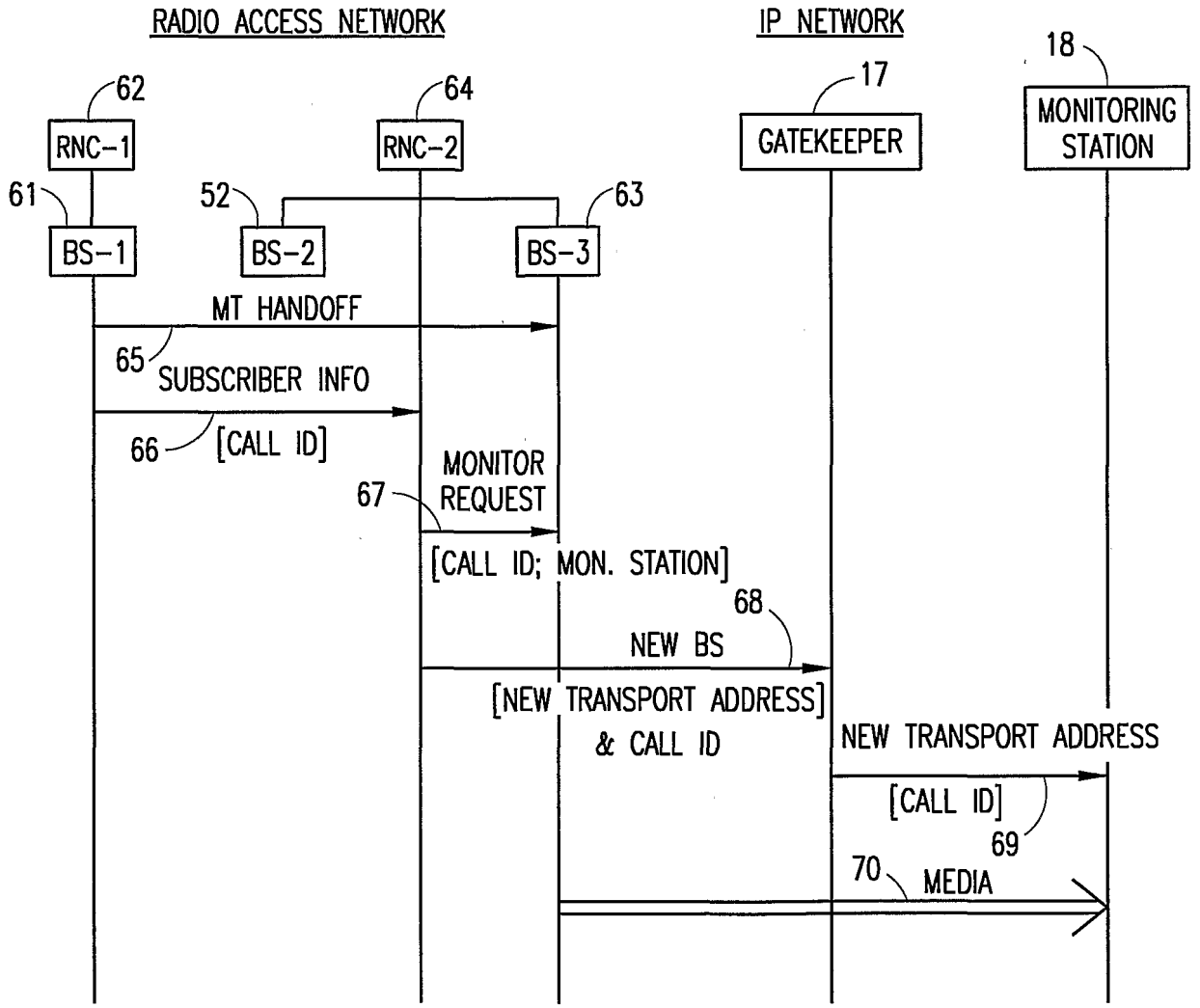
RADIO ACCESS NETWORK
IP NETWORK
62
RNC-1
64
RNC-2
17
GATEKEEPER
18
MONITORING STATION
61
BS-1
52
BS-2
63
BS-3
MT HANDOFF
65
SUBSCRIBER INFO
66
[CALL ID]
MONITOR REQUEST
67
[CALL ID; MON. STATION]
68
NEW BS
[NEW TRANSPORT ADDRESS] & CALL ID
NEW TRANSPORT ADDRESS
[CALL ID]
69
70
MEDIA

FIG. 5

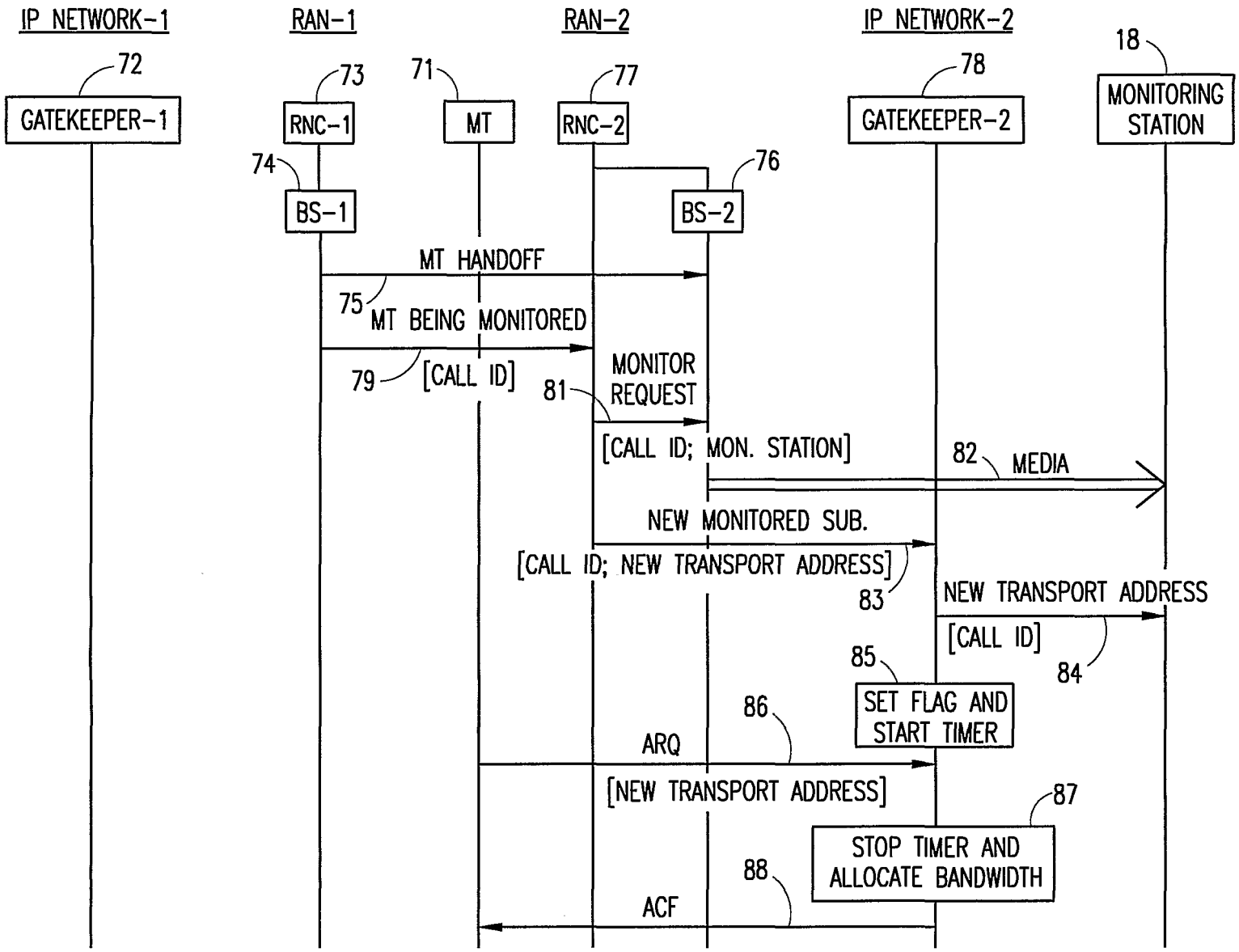
IP NETWORK-1
RAN-1
RAN-2
IP NETWORK-2
72
GATEKEEPER-1
73
RNC-1
71
MT
77
RNC-2
78
GATEKEEPER-2
18
MONITORING STATION
74
BS-1
76
BS-2
MT HANDOFF
75
MT BEING MONITORED
79
[CALL ID]
MONITOR REQUEST
81
[CALL ID; MON. STATION]
82
MEDIA
NEW MONITORED SUB.
[CALL ID; NEW TRANSPORT ADDRESS]
83
NEW TRANSPORT ADDRESS
[CALL ID]
84
85
SET FLAG AND START TIMER
86
ARQ
[NEW TRANSPORT ADDRESS]
87
STOP TIMER AND ALLOCATE BANDWIDTH
88
ACF

FIG. 6