

Exhibit 17

(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 Classification⁷: 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.

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

BACKGROUND OF THE INVENTION

5 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

10 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.

15 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
20 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
25 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.

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

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
5 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,
10 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
15 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.

20 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
25 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
30 network. The request identifies the MT to be monitored, instructs the access router

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.