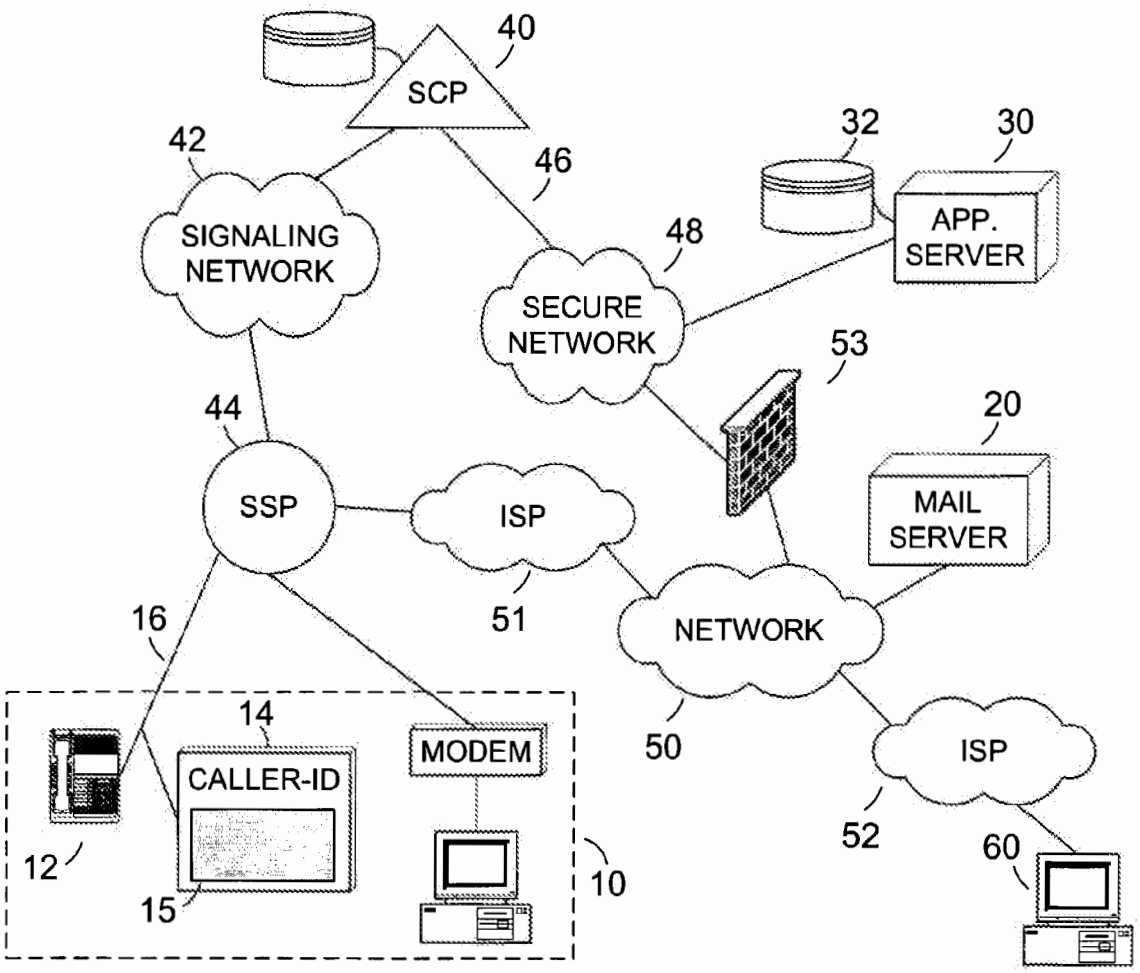


FIG. 1

FIG. 1A

FIG. 1B

FIG. 1C

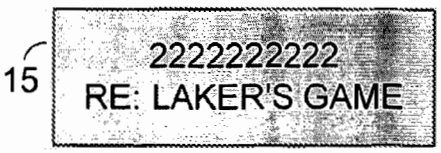


FIG. 1D

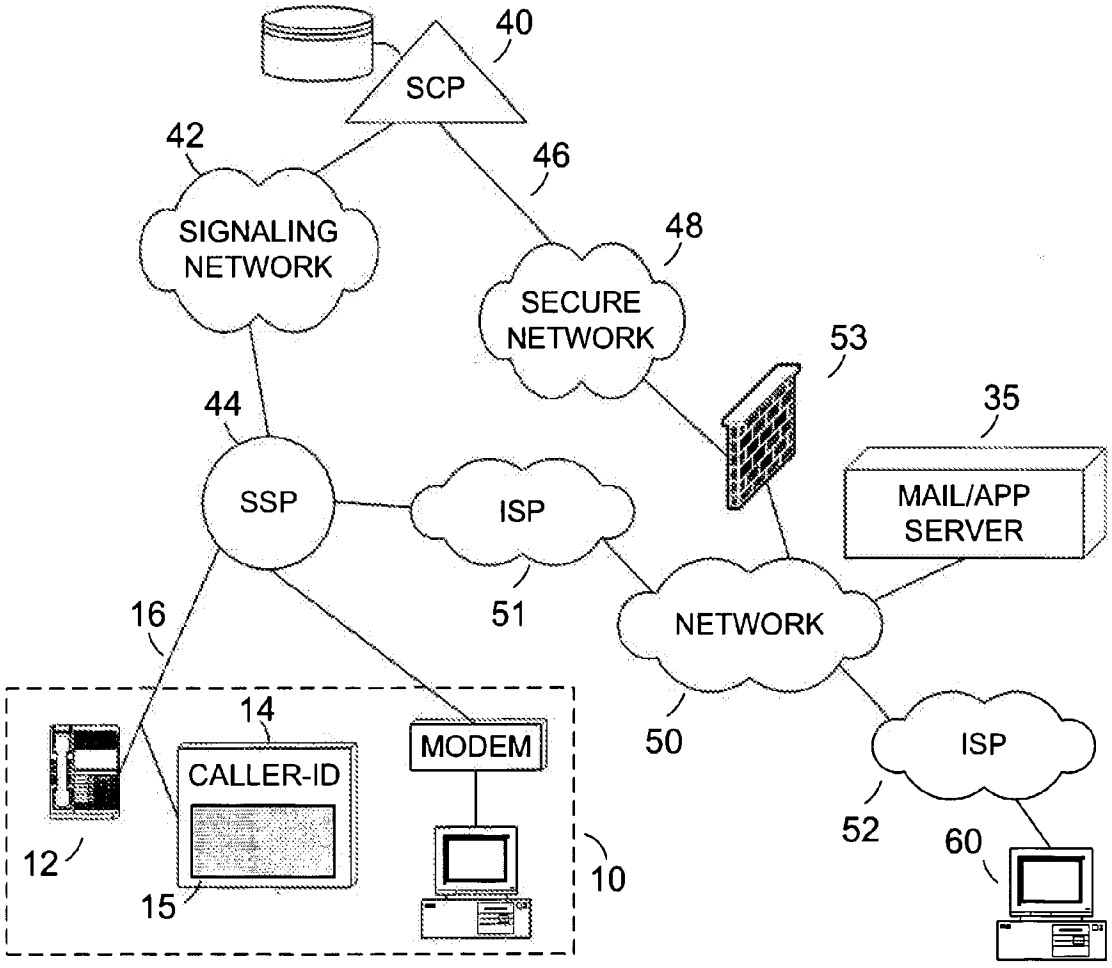

40
SCP
42
46
SIGNALING NETWORK
48
SECURE NETWORK
53
35
44
SSP
ISP
MAIL/APP SERVER
16
51
NETWORK
14
MODEM
50
ISP
CALLER-ID
52
60
12
10
15

FIG. 2

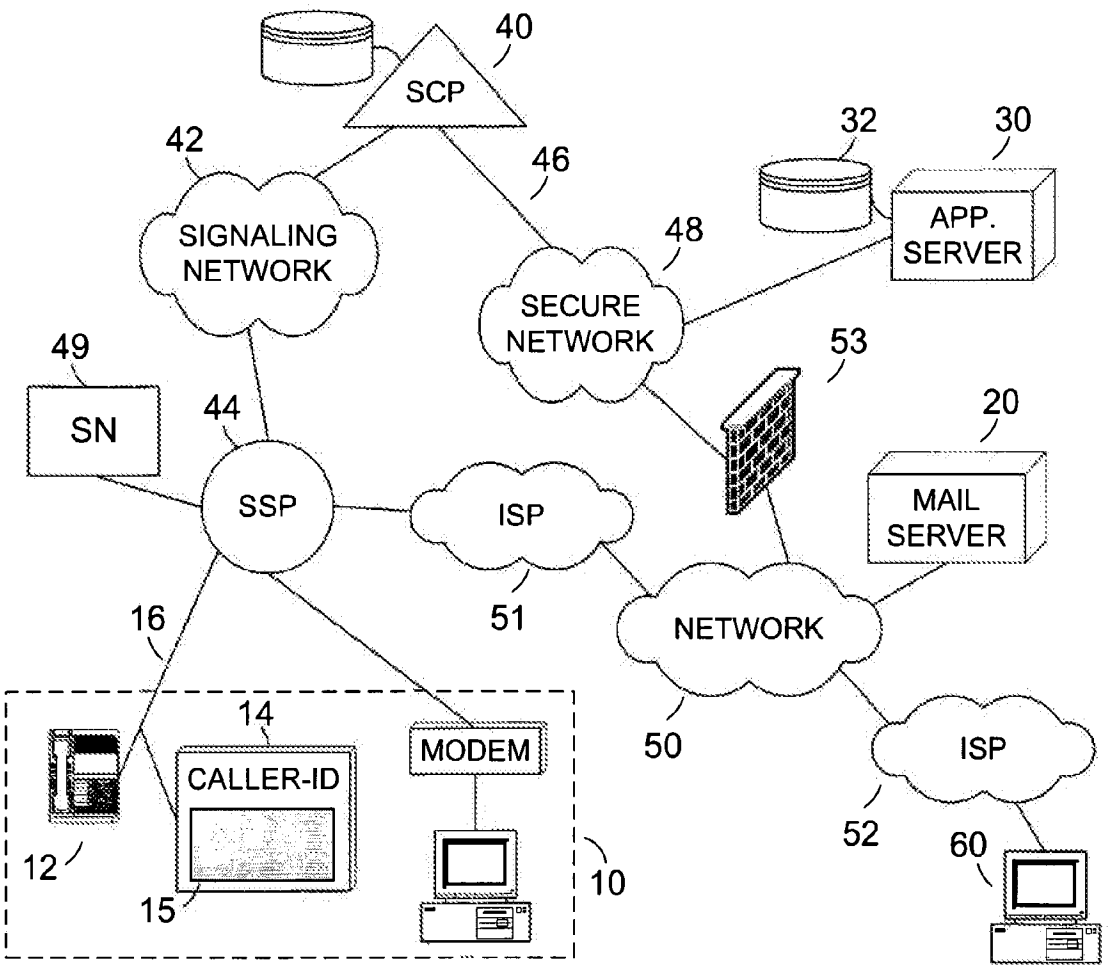

40
SCP
42
SIGNALING NETWORK
46
32
30
APP. SERVER
48
SECURE NETWORK
49
SN
44
SSP
ISP
51
53
20
MAIL SERVER
16
NETWORK
50
14
CALLER-ID
MODEM
12
15
10
ISP
52
60

FIG. 3

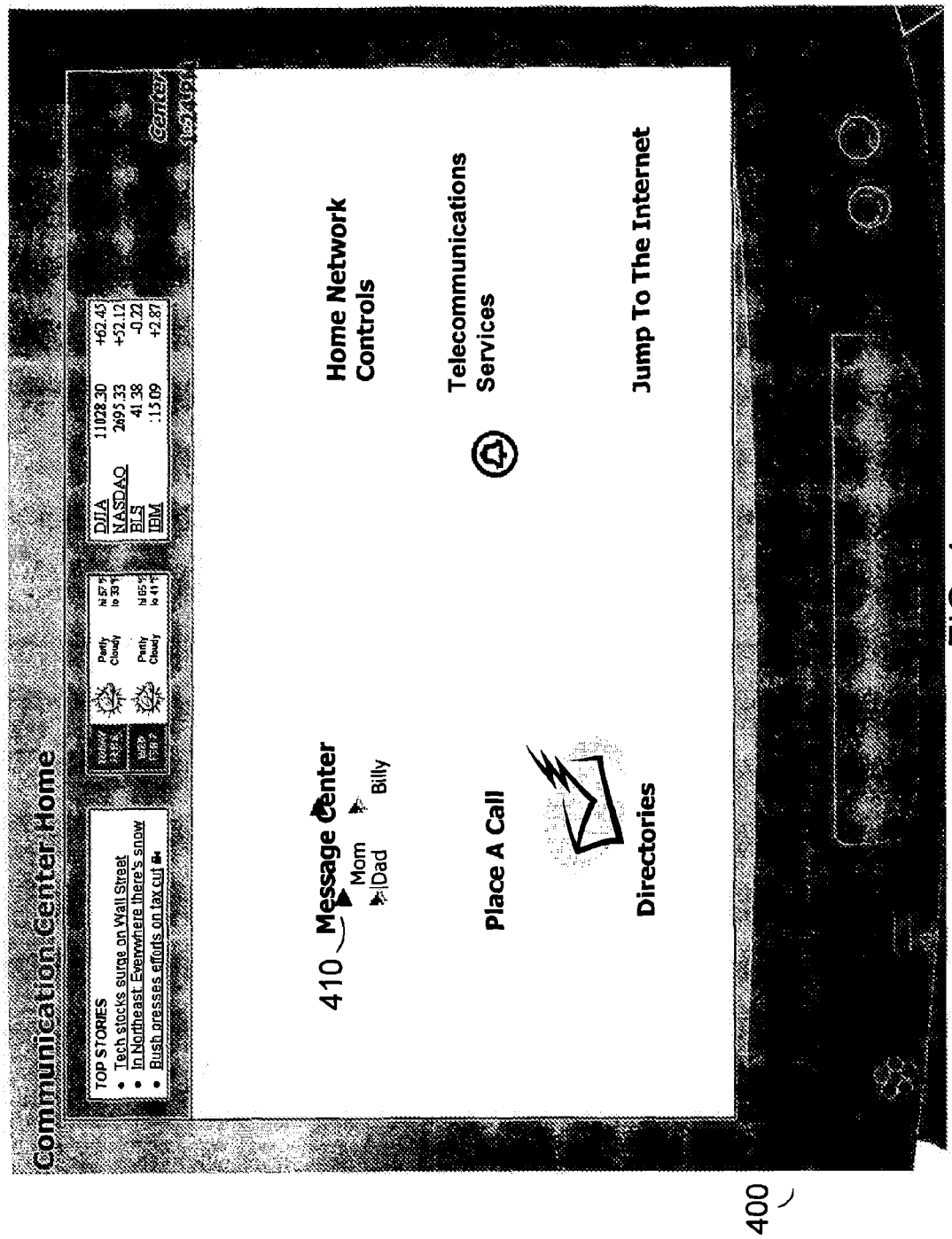

Communication Center Home
TOP STORIES
Tech stocks surge on Wall Street
In Northeast Everywhere there's snow
Bush presses efforts on tax cut
DJIA 11028.30 +62.45
NASDAQ 2695.33 +52.12
BLS 41.38 -0.22
IBM 115.09 +2.87
Message Center
Mom
Dad
Billy
Home Network Controls
Telecommunications Services
Place A Call
Jump To The Internet
Directories
410
400

FIG. 4

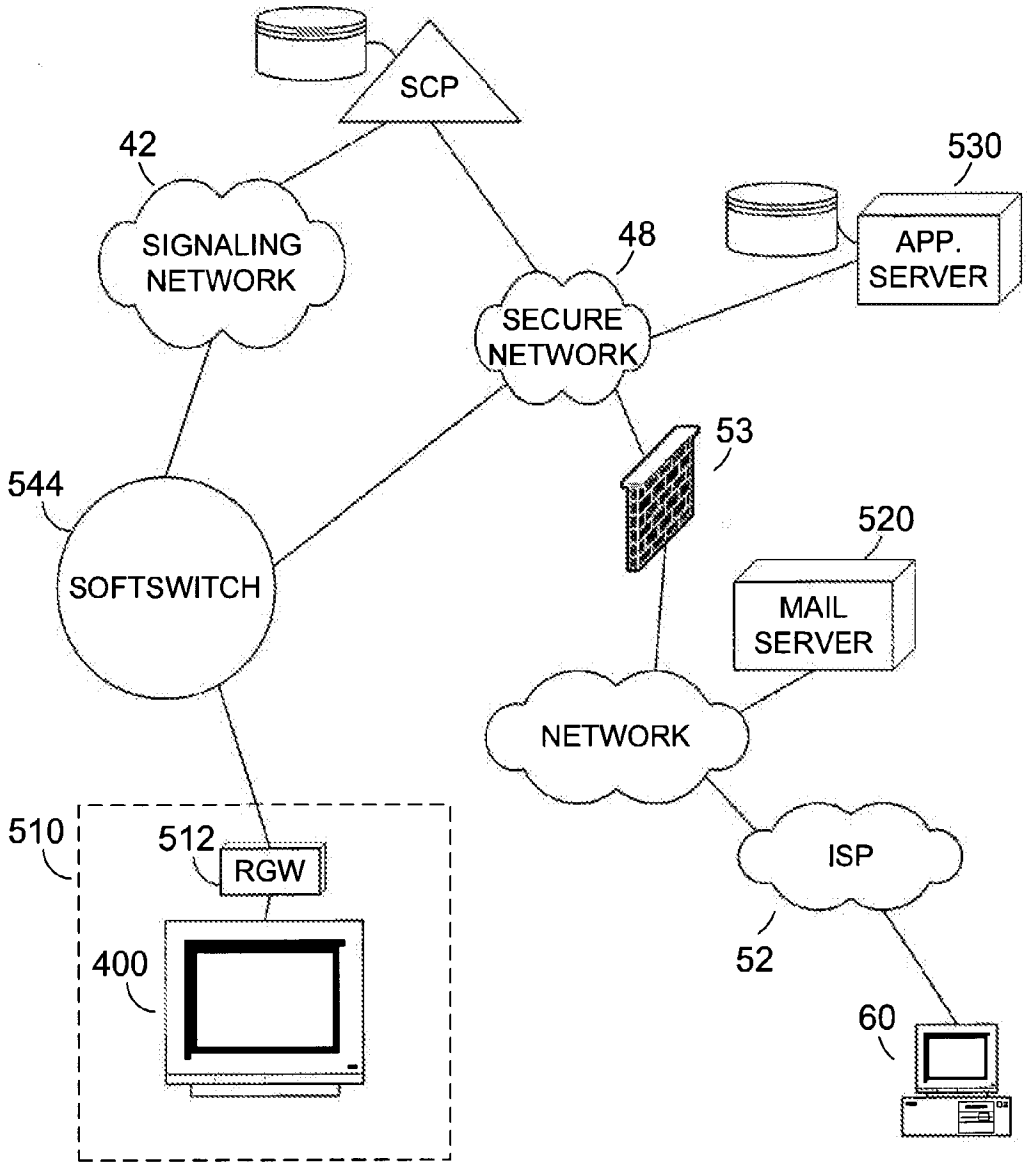

SCP
42
SIGNALING NETWORK
530
APP. SERVER
48
SECURE NETWORK
53
544
SOFTSWITCH
520
MAIL SERVER
NETWORK
510
512
RGW
400
ISP
52
60

FIG. 5

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 August 2013 (15.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/120069 A1

(51) International Patent Classification:
G06F 9/00 (2006.01)

(21) International Application Number:
PCT/US2013/025559

(22) International Filing Date:
11 February 2013 (11.02.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/596,883 9 February 2012 (09.02.2012) US

(71) Applicant: **CONNECTIFY** [US/US]; 2400 Market Street, Suite 411, Philadelphia, PA 19103 (US).

(72) Inventors; and
(71) Applicants : **PRODOEHL, Brian** [US/US]; 2400 Market Street, Suite 411, Philadelphia, PA 19103 (US). **LEWANDA, David** [US/US]; 2400 Market Street, Suite 411, Philadelphia, PA 19103 (US). **GIZIS, Alex** [US/US]; 2400 Market Street, Suite 411, Philadelphia, PA 19103 (US). **LUTZ, Brian** [US/US]; 2400 Market Street, Suite 411, Philadelphia, PA 19103 (US).

(74) Agents: **GOLDSTEIN, Kevin W** et al.; Stradley Ronon Stevens & Young, LLP, 30 Valley Stream Parkway, Malvern, PA 19355 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: SECURE REMOTE COMPUTER NETWORK

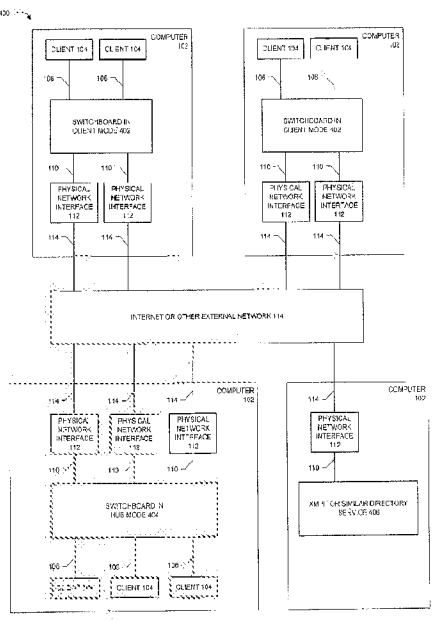


FIG 4

(57) Abstract: Systems and methods to provide improved secure, high speed networking between two or more computers is disclosed. The invention provides a robust and flexible means to readily establish a secure connection between two or more computers using insecure public or private network connections, while eliminating most of the difficulties and issues a user typically experiences with varying virtual private networks ("VPN") and firewall configurations. The inventive system can be adapted to route traffic across multiple network connections based on a variety of criteria, including without limitation, the importance of any given data, the cost of each means of connection, and/or the performance of each possible means of connecting to the client system.

WO 2013/120069 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

SECURE REMOTE COMPUTER NETWORK

Field of the Invention

The present invention relates generally to the field of computer networks, and in more particularity, relates to secure, high speed networking between two or more computers using insecure public or private network connections. The secure, remote network provides for the configuration of an encrypted "tunnel" on a user's private network for data packets to pass through an insecure public network without risk of exposure.

BACKGROUND OF THE INVENTION

Computers can communicate with one another only when connected together using some form of a communications network. The internet is one such network, which has grown extensively over the past decade, and has the distinct advantage of being able to connect computers together from anywhere in the world. Another type of communications network is a local area networks ("LAN"), which are private networks that typically exist between only a few trusted computers, usually in an office or home. A further example of a computer communications network is a wide area network ("WAN"), which is usually used as a means of communications access to the internet via a wireless radio protocol.

There are many possible reasons to want remote computers to join a LAN. A LAN itself is often secure, it may contain or have access to important corporate resources at the office, or access to one's personal media or data files in a residential setting. However, once a user attaches to a LAN via a direct internet connection, the LAN is no longer secure. For this reasons, the Virtual Private Network ("VPN") was created. The VPN is software that appears to be another LAN adapter, but uses encryption technology and methods, and internet connections, to bridge remote computers onto a local area network, without risk of directly connecting the LAN to the public and insecure internet.

Fig. 1 illustrates a prior art classic Virtual Private Network **100**. In such a network, predefined or rolling algorithms allow a secure connection between a computer **102** and a corporate server **116.** This connection is made over any network **114,** which may also be the internet, with security managed by the VPN layer on the client **108** and the server **118**. Any software clients **104** on the client computer **102** will see the VPN layer **108** as a virtual network interface **106**, appearing no different than the driver for a physical network

interface **112**. The VPN encapsulates all traffic sent to it as encrypted, private data, then sends it via a standard network interface and driver **110** to a physical network interface device **112**, such as a Wi-Fi or Ethernet device.

The VPN data is secure over the unsecured network **114**, using strong encryption. This type of encryption is superior to other standard forms of encryption, because even the structure of the data is hidden from any resource outside of the VPN. The classic VPN typically has pre-shared keys; an administrator will create encryption keys for each client computer **102**, which are also known to the server **116**. This prevents unauthorized users of the same VPN technology to connect, and it allows an administrator to de-authorize any given user. Some simple VPNs use only a single shared key for all connections.

The classic prior art VPN routes data to a server **116**, which is also physically interfaced **112** to the external, insecure network **114**. The server **116** communicates via an driver interface **110** to the server part of the VPN **118**. It is only within this part of the system that the encrypted data is decrypted. In the classic VPN, the VPN server **118** is responsible for authenticating VPN clients **108.** It will, of course, reply to said clients with encrypted packets, so the communication and traffic is encrypted in both signal directions and is two-way secure.

On the server **116**, the VPN server **118** will also appear as a normal networking device to the server host operating system ("OS"), allowing access to the server's network software layer **110** and network software clients **104** within the server computer, and usually, out via a physical interface **112** to a secure corporate network **120**.

The effect of the classic prior art VPN is that the remote client computer **104** behaves as if it is in the same building, connected to the secure corporate network **120**, as the server **118** and other client computers **104**. Yet, the data from the client **104** is secure, and the corporate network **120** is not subject to risk of attack via an open internet **114** or other insecure connection. A big disadvantage of a classic VPN is its complexity of use. A network administrator is usually needed, to hand out keys, to manage fire walls, etc. Moreover, it is dependent on the central authority for all VPN certifications. Even in a business scenario, managing a VPN and keeping it functional for all remote users can be a complex and problematic task.

In response to these type of issues, and to enable simpler VPNs for home users, a new kind of VPN management has become popular. This new VPN eliminates some or all aspects of a single central server, replacing it with a central manager for VPN certifications, which will let VPN clients rendezvous with one another, but then, at least to some extent, run peer-to-peer as long as the VPN is operating. **Fig. 2** illustrates an example prior art embodiment of this modified VPN **200**, which has enjoyed some success as a personal VPN. In this architecture, there is no corporate intranet, simply clients **102** that wish to merge their local networks together via a VPN.

This network architecture still enlists a management server **202**, but in this instance the server is only for management purposes. A client **102** will establish a connection to a web or similarly accessible front end **204**, which will allow it to define a VPN connection and other clients. The web front end 204 informs the VPN Manager of the connection, and it proceeds to direct the clients to establishing a peer-to-peer, authenticated VPN connection.

Some VPNs designed this way will continue to route some traffic through the VPN Manager **206**, while others drop the management interface entirely and leave the clients to operate entirely peer-to-peer.

Another limitation of the typical VPN user is the network itself. Some client devices may have multiple internet connections: WAN, LAN, Wi-Fi, etc. But each of these connections are not necessarily useful at all times, particularly over the course of a day for a traveler. For example, while a Wi-Fi connection may be the best communication means at one location, a WAN may be better for signal transmission at a different location. It may be complex to switch the VPN from interface to interface, and there is usually no way to take advantage of the speed of multiple interfaces when they are available.

There is a history for using multiple physical interfaces and treating them as a single faster interface. This has historically been called "network bonding." The use of a bonded set of slower physical interfaces **112** to create one large, virtual interface is fairly well documented. **Fig. 3** shows a typical prior art bonded network interconnect **300**. In this system, there is a computer **102** with client applications **104** and a network interface layer **106** that needs to be connected to the internet or other fast network **114**. However, it only has access to slow connections **304**.

Using either a network layer or a device layer abstraction **302**, such a system splits network traffic in some agreed-upon way over multiple point-to-point connections, such as phone lines, to a service provider **306**. That service provider **306** contains a similar network layer or device layer **302**, which can reassemble the traffic, delivering it to a standard network layer protocol **110**, and ultimately, interfaced **112** to the target network **114**. Examples of this type of architecture include the Integrate Services Digital Network ("ISDN") standard, and various systems for bonding analog phone modems such as Microsoft Modem Bonding, FatPipe, and others.

To improve upon this prior art, a number of additional features can be built into a VPN system. A more flexible means of establishing the VPN connection, with the option of using readily available public resources and standards is a tangible advancement. Using standards allows the user a choice between public or private resources for this connection. A further goal of the inventive system is an even greater simplification of the VPN setup, and taking the need for a proprietary central server out of the system as a further improvement. A further objection and advancement is to establish a novel means by which the VPN can route though firewalls that can often hinder VPN use in the field. And a final advancement allows dynamic use of any and all available interfaces, optimizing performance across all means of connection between two points on the VPN, and allowing rules to factor in the cost of any interface's use as well.

Based on the typical complexity of creating, establishing, and maintaining a VPN, there is plenty of room for improvement in this field. Specifically, a VPN can be created dynamically, without the need for expert configuration of the VPN, firewalls, routers, and other networking components. Coupling this with the ability to intelligently use all available bandwidth, and make the best of potentially faulty connections readily permits the ability to create a more ideal VPN for use by remote clients.

SUMMARY OF THE INVENTION

The primary elements of the secure remote computer network include means to configure an encrypted "tunnel" for data packets on a private network to pass through an insecure public network without risk of exposure. In preferred embodiments, the inventive systems and methods provide a robust and simple configuration mechanism, based on

existing open standards for internet "instant" messaging and media delivery that will remove the complexity and unreliability often associated with current VPNs.

More particularly, the present invention overcomes the disadvantages of the prior art and fulfills the needs described above by providing, in a preferred embodiment, a computer communications network system, comprising (a) at least one switchboard computer in a hub mode in communication connectivity with an external network; (b) at least one switchboard computer in a client mode in communication connectivity with an external network; and (c) a directory service in communication connectivity with an external network; wherein said at least one switchboard computer in a hub mode initiates a connection with said directory service to be registered and made available for said at least one switchboard computer in a client mode to dynamically communicate with said at least one switchboard computer in a hub mode through an external network.

Another embodiment of the present invention is a computer communications network system, comprising (a) at least one switchboard computer in a hub mode in communication connectivity with an external network, said at least one switchboard computer further comprising a discovery server to monitor external activity, a management data base to record current network communication statistics, a plurality of network address translators, a virtual network interface to communicate with a plurality of client computers, and a virtual private network to encrypt data prior to transmitting said encrypted data to one of said network address translators; (b) at least one switchboard computer in a client mode in communication connectivity with an external network, said at least one switchboard computer further comprising a discovery server to monitor external activity, a management data base to record current network communication statistics, a plurality of network address translators, a virtual network interface to communicate with a plurality of client computers, and a virtual switch and router in communication connectivity with a virtual private network to encrypt data prior to transmitting said encrypted data to one of said network address translators; and (c) a directory service in communication connectivity with an external network; wherein said at least one switchboard computer in a hub mode initiates a connection with said directory service to be registered and made available for said at least one switchboard computer in a client mode to communicate with said at least one switchboard computer in a hub mode through an external network.

Still another embodiment of the present invention is a method for creating a flexible and secure network connection between two or more computers, having at least one switchboard computer in a hub mode in communication connectivity with an external network; and at least one switchboard computer in a client mode in communication connectivity with an external network; and a directory service in communication connectivity with an external network; the method comprising the steps of (a)initiating from said at least one switchboard computer in a hub mode a connection with said directory service; and (b) registering said at least one switchboard computer in a hub mode a connection with said directory service as available for said at least one switchboard computer in a client mode to dynamically communicate with said at least one switchboard computer in a hub mode through an external network.

Brief Description of the Drawings

Fig. 1 illustrates an example prior art computer network architecture having a single VPN client and single VPN server;

Fig. 2 illustrates an example prior art computer network architecture having more than one VPN client connected to a management server through the internet;

Fig. 3 illustrates an example prior art computer network architecture having a client computer connected to the internet through a service provider;

Fig. 4 illustrates the main components of a preferred embodiment of a "Switchboard" VPN network;

Fig. 5 illustrates the internal design of a preferred embodiment of the Switchboard module;

Fig. 6A illustrates a preferred embodiment of one mode of client to hub connection via the XMPP or other directory protocol;

Fig. 6B illustrates another preferred embodiment of another mode of client to hub connection via the XMPP or other directory protocol through a two-hop network; and

Fig. 7 illustrates an exemplary embodiment of a large private network with multiple hub access points.

Other features and advantages of the present invention are provided in the following detailed description of the invention, which refers to the accompanying drawings.

Detailed Description Of Preferred Embodiments

The present invention provides in various exemplary embodiments, methods and systems for transmitting data between two computer networks, using multiple, potentially insecure or unreliable connections to deliver the effect of unifying the two networks as one secure network. In addition, it provides an improved method of establishing a virtual private network over insecure or unreliable connections.

An exemplary embodiment of a switchboard network **400** system according to the present invention is illustrated in **Fig. 4**. The network consists of at least one switchboard in hub mode **404**, one or more switchboards in client mode **402**, and at least one an Extensible Messaging and Presence Protocol ("XMPP") or other similar directory service **406**. The switchboard hub mode **404** is similar in some ways to a traditional VPN server, but more so it conceptually functions as a hub, similar to that in an Ethernet network. As such, the hub is not necessarily unique in a switchboard network, and there may be multiple hubs as well as multiple clients. The directory service can be an XMPP **406** or something similar in concept. The directory service can be completely private, hosted on a server appliance computer, or hosted on a public server such as *Google Talk*.

To describe the operation of an exemplary embodiment of the present inventive switchboard network, the computer **102** in hub mode **404** initiates making a connection to a directory service such as an XMPP **406**, and registering that it (the computer **102** in hub mode **404**) is available. The XMPP is an open protocol for real-time (e.g., instant) messaging over computer networks. The switchboard is well suited to using the XMPP protocols for directory-based discovery, but this is not the only possible service. Another similar service that might be used by the Switchboard is the Light Directory Access Protocol ("LDAP"). Potential clients may then access that service based on other security protocols, as applicable, and request connection to the switchboard network **400**, via any number of

independent physical interfaces **112** connected to one or more external public or private networks, such as the internet **114**.

The detailed internals of an exemplary embodiment of the switchboard module **502** are shown in **Fig. 5**. The switchboard interface appears to a host computer as another Network Interface Card, via a virtual network interface **504** for the host operating system. A Management Interface process **512** is presented to adjust the behavior of the switchboard network, based on a local client **104** interface **510**, such as an XML remote procedure call ("XML-RPC"). Behaviors are also modified by changes in the active system, discovery of clients or hubs via the Discovery Server **536**, or statistics and other data, which is tracked in the Management Database **520**.

The purpose of the Discovery Server **536** is to monitor external activity. The Discovery Server **536** will communicate with the centralized XMPP service **406**, record changes to the clients **104** attached to a switchboard in server mode, and complete similar management functions.

The purpose of the Management Database **520** is to record current statistics and other information useful to the network. For example, the database **520** knows the cost, current performance, and expected reliability of every way of connecting between any two nodes in the network. Thus, as illustrated in **Fig. 4**, for a client **402** with two physical interfaces **112** connected to the Internet **114**, communicating to a hub **404** with three physical interfaces **112** also connected to the Internet **114**, the database **520** would track statistics on the six possible ways of establishing a connection between the client **402** and the hub **404**.

The actual switchboard module **502** starts, as mentioned, with the virtual network interface **504**. Traffic is routed **506** through a network address translation layer ("NAT") **508**, which allows the host network address space to be independent of the internal routing decisions made by switchboard. The NAT **508** feeds **514** a virtual router/switch **518**, which in the case of client mode will be bypassed. Data **524** from the Management Database **520** and the discovery server **536** inform the Socket Packet Scheduler **526.** This Scheduler **526** takes into account quality of service, the number of active links between the hub and each client, the efficiency and cost of each link, and the global load on each hub link, to provide an optimal, packet by packet routing to each client over each available interface.

It is important to note that each physical link **114** to a client or hub is inherently dynamic. Interfaces may be added, removed, or simply go unreliable, and the switchboard system quickly adapts to any lost or added interfaces **112**. So in a practical case, a laptop computer running a Switchboard client over Wi-Fi could be plugged into a gigabit Ethernet connection, and immediately boost the performance of on-going transactions. Or, a PC-Card or USB-based 3D modem could be added, and the laptop computer could then be taken mobile, again without disruption in on-going network transactions.

The output of the router **528** passes through an optional compression module **530**. This layer will compress traffic **532** to the VPN **534** that will benefit from compression, and in the other signal direction, expand traffic **532** from the VPN **534** into the router. The VPN **534** itself applies encryption to each packet, then sends it down the appropriate Internet Protocol tunnel **538** to another Network Address Translator **542**. This second NAT translates the VPN packet addresses to match the network conventions of the physical network interfaces **112.** VPN packets are then sent **110** to the appropriate NICs **112**, and then on to each respective network **114**.

A packet being received by a hub **404** or client **402** follows this path in reverse. The external network **114** delivers a packet to one or more of the physical interfaces **112**. These are VPN packets, which contain the encrypted private network packets. These run through a NAT **542** and on to the VPN **534** manager. This layer will dismantle the VPN, decrypt the payload, and collect complete data packets. These are then sent on **532** to the compression module **530** and decompressed if possible.

If operating in a hub mode node, the packet is sent **528** to the router module **518**, and perhaps sent back out to another client node, depending on the routing information for that node. Again, this is optimized in the packet scheduler **526**, by analysis of the performance for all possible links, the quality of service for the particular packet, reliability of each outgoing link, and load balancing of all traffic across the hub.

When the switchboard module is in client mode, the router **518** is bypassed and the packet is sent directly to the local side NAT **508**. Similarly, if this is a packet destined for the hub's local network, the router directs it on **514** to the local side NAT **508**. Network addresses are rationalized here for the local network **106**, and eventually get routed to local client programs, or possibly back to the internet via a hub firewall.

Fig. 6A and **Fig. 6B** illustrate some aspects of the discovery server **536** described above. As shown in **Fig. 6A**, a peer-to-peer **600** network may be established between any two of the multiple connections possible on switchboard enabled devices. The hub **602** registers **604** with an XMPP service **606**, which can be public or private. The client **612** will, at a later time, contact the XMPP or other directory service **606** and ask for a connection to the switchboard hub **602**. These are general purpose protocols inherent in XMPP. In other words, the XMPP service **606** knows nothing specific about the network being established by the switchboard.

In the case of XMPP, the XMPP service **606** will interrogate the client **612** and hub **602**, and attempts to establish a peer-to-peer link **614** between the two computers. This uses the Jingle protocol, which is intended to encapsulate multimedia data between two systems. Since the Jingle protocol itself does not care about specific contents, the switchboard is taking advantage of this mechanism for real-time streaming to make the VPN connection **614** without the usual complexity of setup.

Jingle connections are set up via the open Interactive Connectivity Establishment ("ICE") methodology, which can usually manage the complexities of NAT traversal, and thus create the peer-to-peer connection **614** shown in **Fig. 6A**. But when ICE cannot establish the connection, the XMPP service **606** can act as an intermediary, creating a two-hop network **620**, as shown in **Fig. 6B**. Based on the fact that the client **612** and hub **602** have connected to the XMPP service, the ICE protocols can manage a hop **622** through the XMPP service **606**, because the XMPP service **606** device can be seen by, or be communicating with, both the client **612** and hub **602**.

It is important to note that the Jingle protocol establishes rapid transport protocol ("RTP") connections, which are ideal for media streaming, not Transmission Control Protocol/Internet Protocol ("TCP/IP") connections. TCP/IP connections are normally desired for 2-way data communications, where every data packet sent is acknowledged as received. Such acknowledgement of receipt is not undertaken with RTP connections. This would normally be a problem for a data link such as the switchboard VPN. However, the Switchboard VPN is already managing the possibility of faulty links, and is doing so at a high level. As such, this equates to being an advantage to the switchboard protocol.

The TCP/IP protocol works great for a reliable or mostly reliable connection. But as packet failures increase, a network can get swamped by retry packets. Moving the management of these problems to a higher, multi-network view in a switchboard, more intelligent decisions can be made about lost packets. Such lost packets could get routed via a different network connection. For example, a lower priority connection might receive a request for multiple missing packets, for transmission efficiency. Similarly, a critical channel that has not yet failed may be moved to a more reliable connection, lowering the traffic burden on the failing connection. In short, the media-friendly connection is actually an advantage for switchboard's means of implementing the VPN.

A final aspect of the invention is, as mentioned, the non-uniqueness of the hub, versus a server in some prior VPN systems. As shown in **Fig. 7**, the switchboard architecture can be readily scaled up to very larger networks. A large private network **702** may have many different points of access, via switchboard hubs **602**, to a public network such as the internet **704**. A switchboard client **612** may accordingly gain access to the private network via any hub **602**.

In such a network, the directory service **606** will automate the optimization of this connection. The directory **606** itself is periodically updated with statistical information about each hub it lists, including performance and load statistics. The client **612**, when engaged with the directory service **606** in the discovery process, will be able to select an optimal hub **602**, based on the load of the hub **602** and the cost and performance of connection between client **612** and hub **602**.

As described above, the inventive system and methods are able to improve the performance of the VPN connection. This is in part resulting from the ability of the computer network to dynamically schedule virtual network traffic over any and / or all available network interfaces, on a packet-by-packet basis. Moreover, in preferred embodiments, the inventive computer network is capable of monitoring its own performance, and using point-to-point performance of each system-to-system path, monitor overall load of the entire VPN, as well as cost and reliability of each connection, and priority of each socket connection to automatically create optimized networks that can significantly improve performance, cost, and reliability of the VPN connections.

While the present invention is described herein with reference to illustrative embodiments for particular data communication applications, it should be understood that the invention is not limited to those embodiments described. Those having ordinary skill in the art and access to the teachings provided herein will recognize additional applications and embodiments, further modifications, and certain substitution of equivalents, all of which are understood to be within the scope of the claimed invention. Accordingly, the invention is not to be considered as limited by the foregoing description.

CLAIMS

What we claim is:

1. A computer communications network system, comprising:

   (a) at least one switchboard computer in a hub mode in communication connectivity with an external network;

   (b) at least one switchboard computer in a client mode in communication connectivity with an external network; and

   (c) a directory service in communication connectivity with an external network;

   wherein said at least one switchboard computer in a hub mode initiates a connection with said directory service to be registered and made available for said at least one switchboard computer in a client mode to dynamically communicate with said at least one switchboard computer in a hub mode through an external network.

2. The computer communications network system, as described in claim 1, wherein the external network is a global communications network.

3. The computer communications network system, as described in claim 1, wherein the external network is the internet.

4. The computer communications network system, as described in claim 1, wherein the directory service is an Extensible Messaging and Presence Protocol ("XMPP").

5. The computer communications network system, as described in claim 1, wherein the directory service is a Light Directory Access Protocol.

6. The computer communications network system, as described in claim 1, wherein the directory service is hosted on a server appliance computer.

7. The computer communications network system, as described in claim 1, wherein the directory service is hosted on a public server.

8. The computer communications network system, as described in claim 1, which uses the XMPP-related Jingle protocol to exchange data packets between the at least one

switchboard computer in a client mode client, and the at least one switchboard computer in a hub mode.

9. A computer communications network system, comprising:

(a) at least one switchboard computer in a hub mode in communication connectivity with an external network, said at least one switchboard computer further comprising a discovery server to monitor external activity, a management data base to record current network communication statistics, a plurality of network address translators, a virtual network interface to communicate with a plurality of client computers, and a virtual private network to encrypt data prior to transmitting said encrypted data to one of said network address translators;

(b) at least one switchboard computer in a client mode in communication connectivity with an external network, said at least one switchboard computer further comprising a discovery server to monitor external activity, a management data base to record current network communication statistics, a plurality of network address translators, a virtual network interface to communicate with a plurality of client computers, and a virtual switch and router in communication connectivity with a virtual private network to encrypt data prior to transmitting said encrypted data to one of said network address translators; and

(c) a directory service in communication connectivity with an external network;

wherein said at least one switchboard computer in a hub mode initiates a connection with said directory service to be registered and made available for said at least one switchboard computer in a client mode to communicate with said at least one switchboard computer in a hub mode through an external network.

10. The computer communications network system, as described in claim 9, which uses the XMPP-related Jingle protocol to exchange data packets between the at least one switchboard computer in a client mode client, and the at least one switchboard computer in a hub mode.

11. The computer communications network system, as described in claim 9, wherein the external network is a global communications network.

12. A virtual private network for computer communications, comprising:

(a) at least one switchboard computer in a hub mode in communication connectivity with an external network;

(b) at least one switchboard computer in a client mode in communication connectivity with an external network; and

(c) a directory service in communication connectivity with an external network;

wherein said at least one switchboard computer in a hub mode initiates a connection with said directory service to be registered and made available for said at least one switchboard computer in a client mode to dynamically communicate with said at least one switchboard computer in a hub mode through an external network.

13. The virtual private network for computer communications, as described in claim 12, wherein said directory service is an XMPP and uses at least one Interactive Connectivity Establishment protocol to establish the connection between the at least one switchboard computer in a hub mode, and the at least one switchboard computer in a client mode.

14. The virtual private network for computer communications, as described in claim 12, wherein said directory service is an XMPP and creates a connection between the at least one switchboard computer in a hub mode, and the at least one switchboard computer in a client mode, using the XMPP service as a two-hop relay point.

15. The virtual private network for computer communications, as described in claim 12, which uses the XMPP-related Jingle protocol to exchange data packets between the at least one switchboard computer in a client mode client, and the at least one switchboard computer in a hub mode.

16. The virtual private network for computer communications, as described in claim 12, further comprising protocols that allow said at least one switchboard computer in a client mode to select an optimal access hub from a plurality of access hubs.

17. A method for creating a flexible and secure network connection between two or more computers, having at least one switchboard computer in a hub mode in

communication connectivity with an external network; and at least one switchboard computer in a client mode in communication connectivity with an external network; and a directory service in communication connectivity with an external network; the method comprising the steps of:

(a) initiating from said at least one switchboard computer in a hub mode a connection with said directory service; and

(b) registering said at least one switchboard computer in a hub mode a connection with said directory service as available for said at least one switchboard computer in a client mode to dynamically communicate with said at least one switchboard computer in a hub mode through an external network.

18. The method for creating a flexible and secure network connection between two or more computers, as described in claim 17, further comprising the steps of:

(c) monitoring data for one or more of connection cost, point-to-point performance analysis, point-to-point reliability, packet importance, and overall connection load; and

(d) analyzing said data for one or more of connection cost, point-to-point performance analysis, point-to-point reliability, packet importance, and overall connection load to determine an optimal routing of virtual network traffic across multiple network interfaces.

19. The method for creating a flexible and secure network connection between two or more computers, as described in claim 18, wherein the analyzing step to determine an optimal routing of virtual network traffic across multiple network interfaces is made for each data packet being transmitted.

20. The method for creating a flexible and secure network connection between two or more computers, as described in claim 18, further comprising the step of:

(e) posting to the directory service at least one of the data analyzed in step (d).

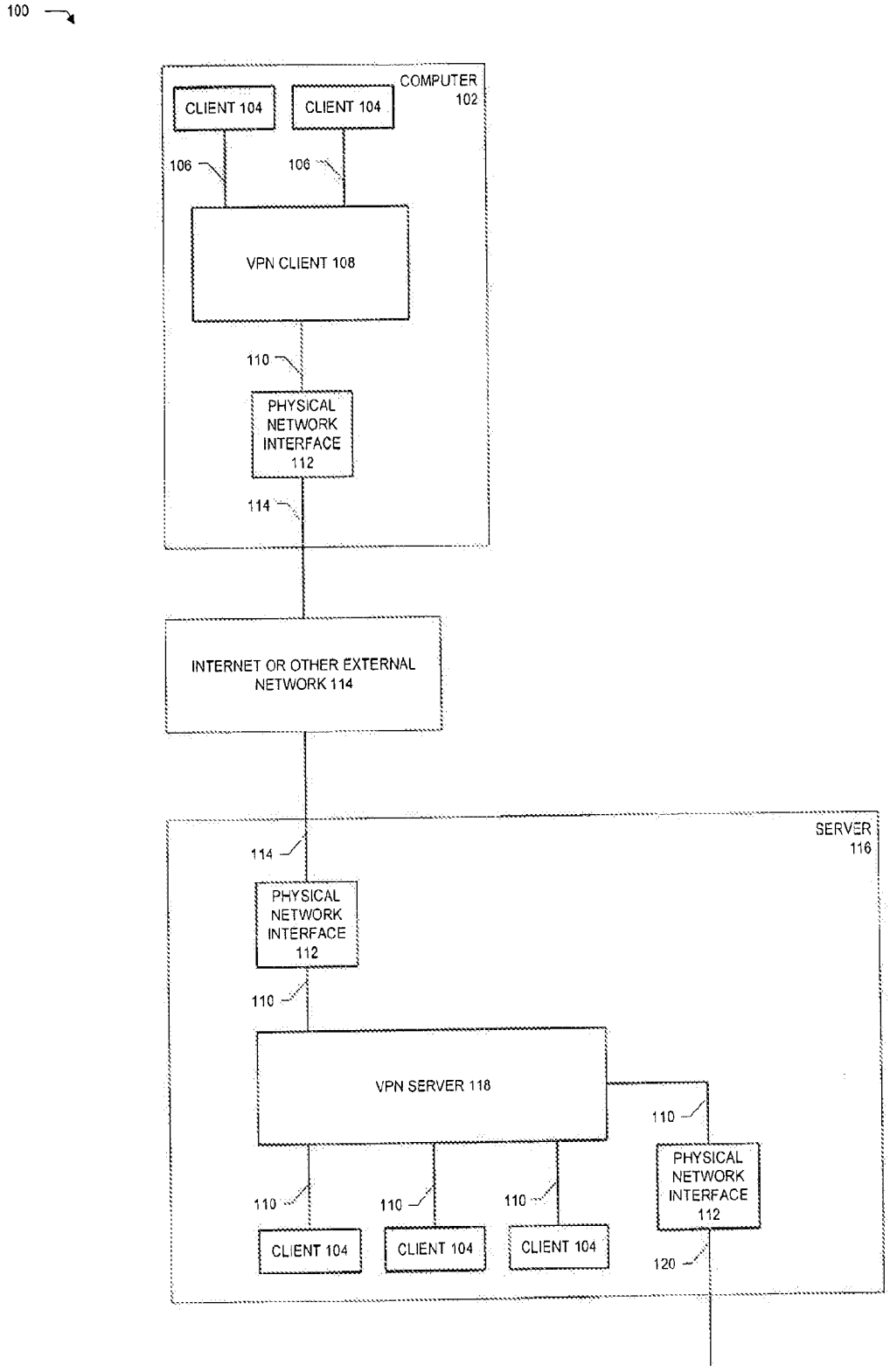


FIG 1. (PRIOR ART)

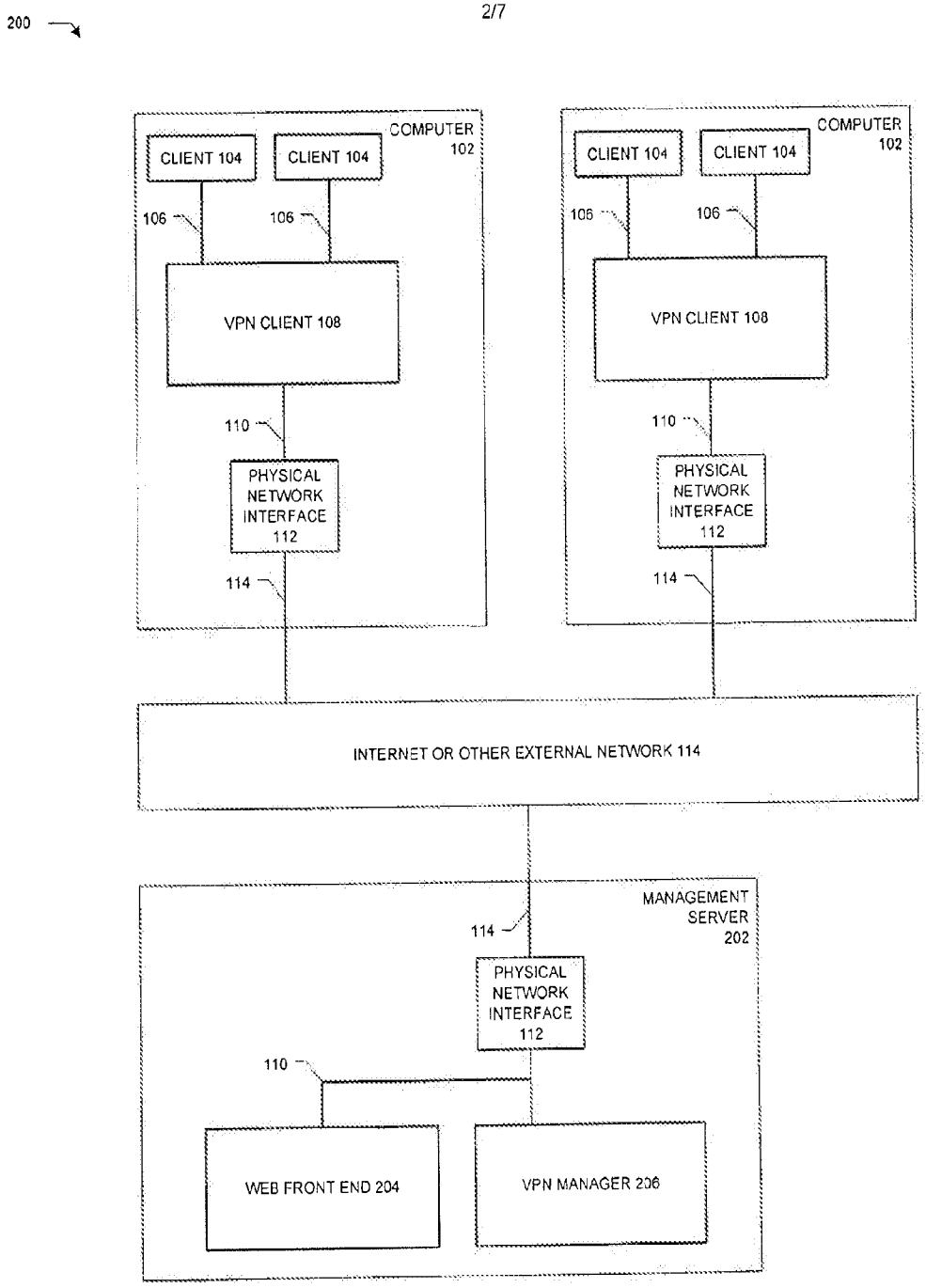


FIG 2. (PRIOR ART)

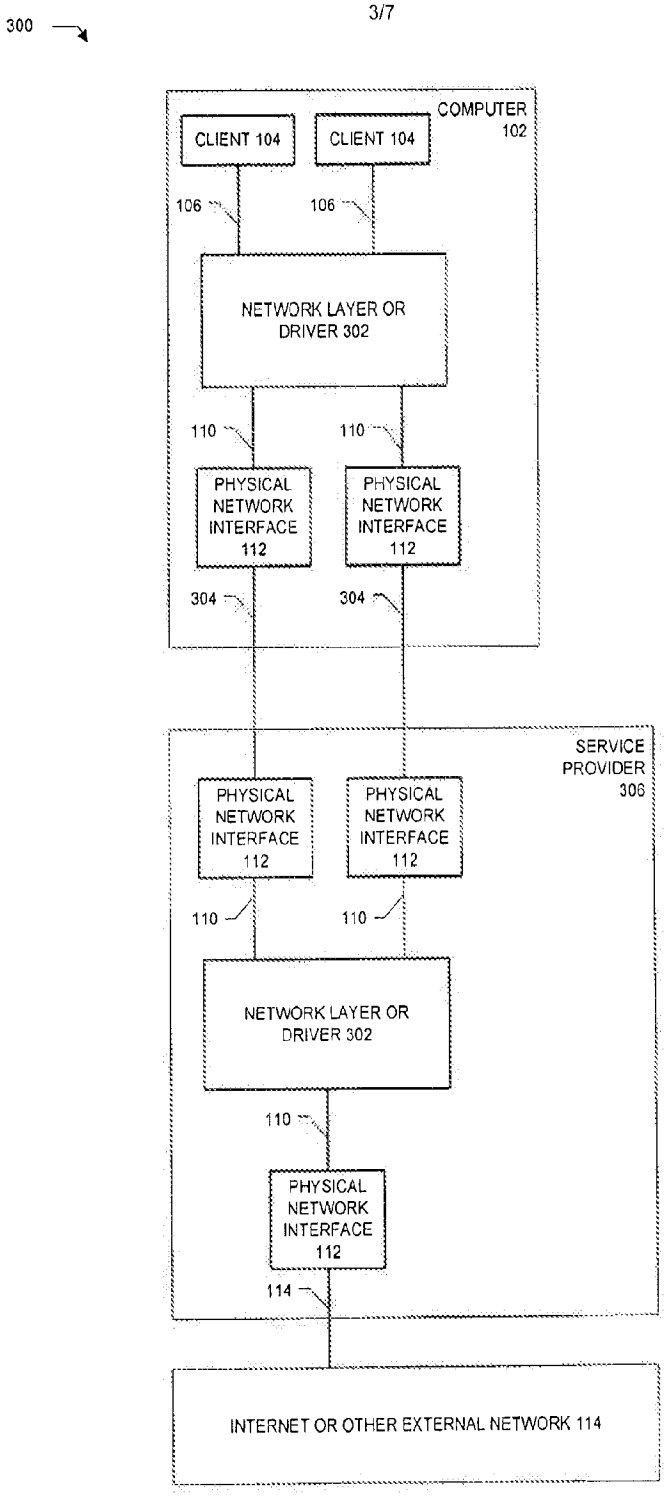


FIG 3. (PRIOR ART)

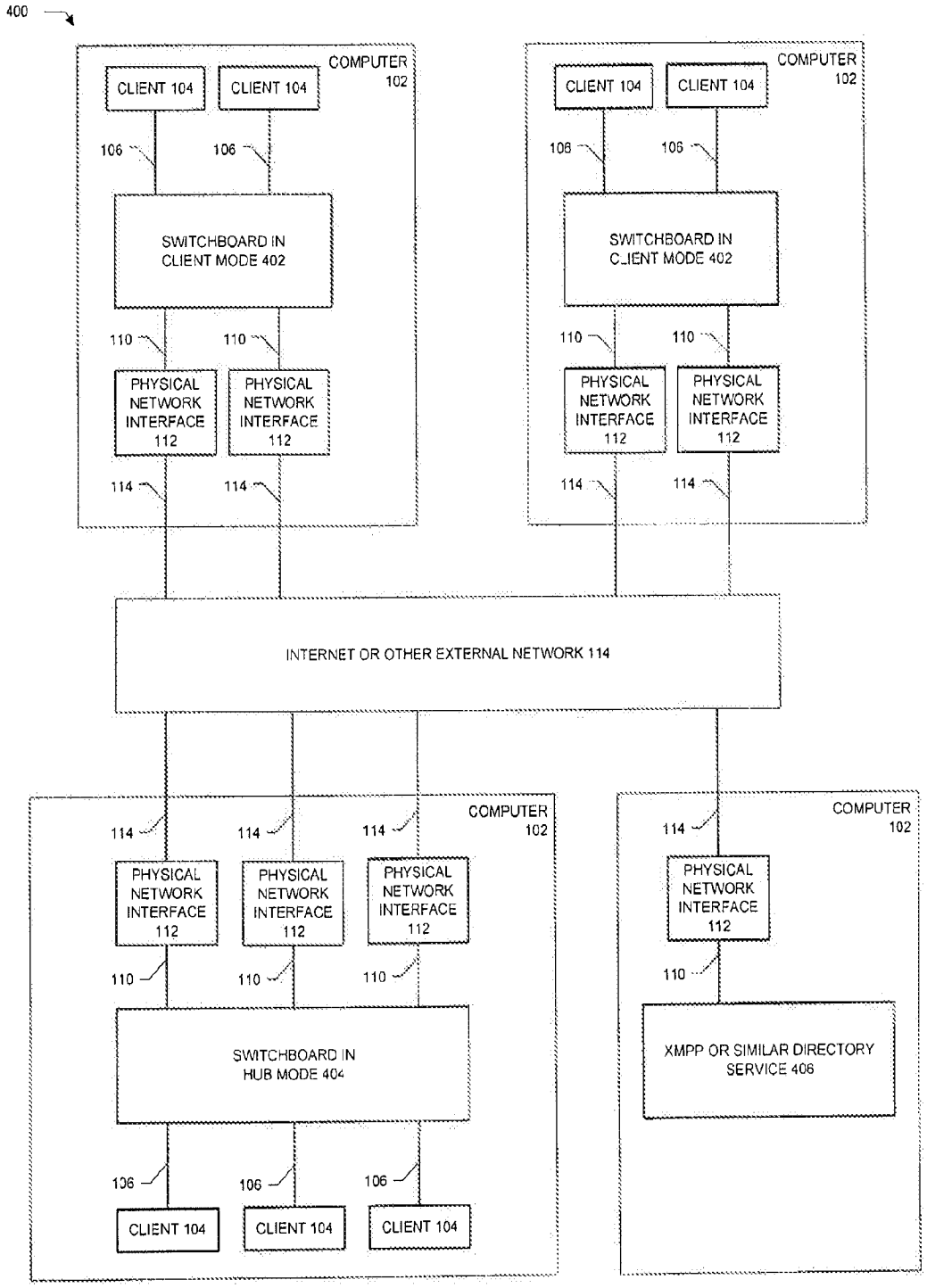

400
COMPUTER 102
CLIENT 104
CLIENT 104
106
106
SWITCHBOARD IN CLIENT MODE 402
110
110
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
114
114
COMPUTER 102
CLIENT 104
CLIENT 104
106
106
SWITCHBOARD IN CLIENT MODE 402
110
110
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
114
114
INTERNET OR OTHER EXTERNAL NETWORK 114
COMPUTER 102
114
114
114
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
110
110
110
SWITCHBOARD IN HUB MODE 404
106
106
106
CLIENT 104
CLIENT 104
CLIENT 104
COMPUTER 102
114
PHYSICAL NETWORK INTERFACE 112
110
XMPP OR SIMILAR DIRECTORY SERVICE 406

FIG 4.

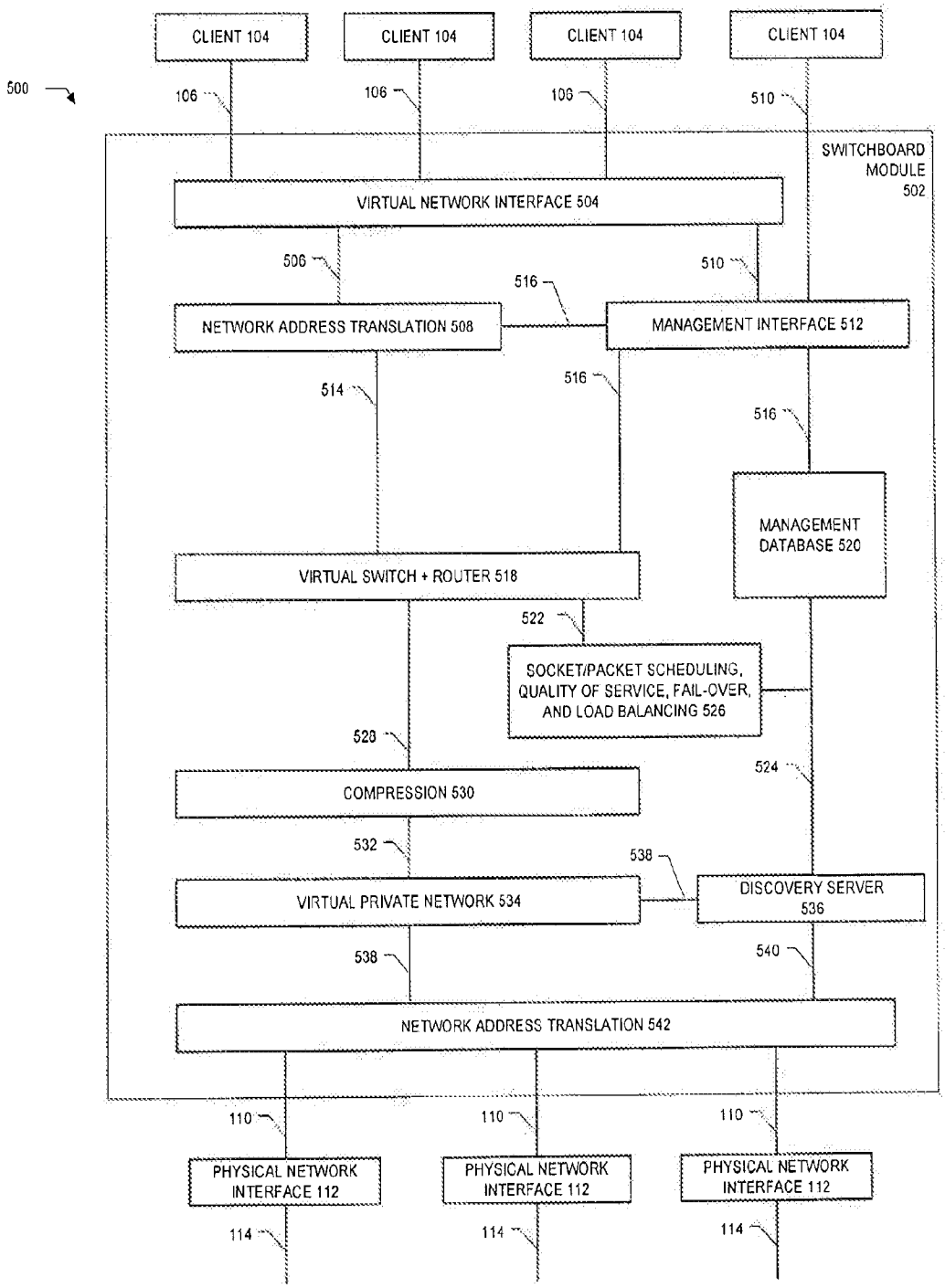

500
CLIENT 104
CLIENT 104
CLIENT 104
CLIENT 104
106
106
106
510
SWITCHBOARD MODULE 502
VIRTUAL NETWORK INTERFACE 504
506
510
516
NETWORK ADDRESS TRANSLATION 508
MANAGEMENT INTERFACE 512
514
516
516
MANAGEMENT DATABASE 520
VIRTUAL SWITCH + ROUTER 518
522
SOCKET/PACKET SCHEDULING, QUALITY OF SERVICE, FAIL-OVER, AND LOAD BALANCING 526
528
524
COMPRESSION 530
532
538
VIRTUAL PRIVATE NETWORK 534
DISCOVERY SERVER 536
538
540
NETWORK ADDRESS TRANSLATION 542
110
110
110
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
PHYSICAL NETWORK INTERFACE 112
114
114
114

FIG 5.

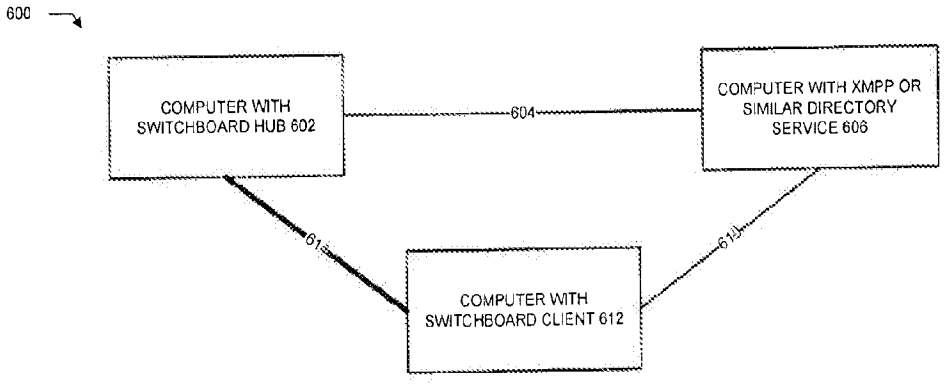

600
COMPUTER WITH SWITCHBOARD HUB 602
604
COMPUTER WITH XMPP OR SIMILAR DIRECTORY SERVICE 606
612
614
COMPUTER WITH SWITCHBOARD CLIENT 612

FIG 6a.

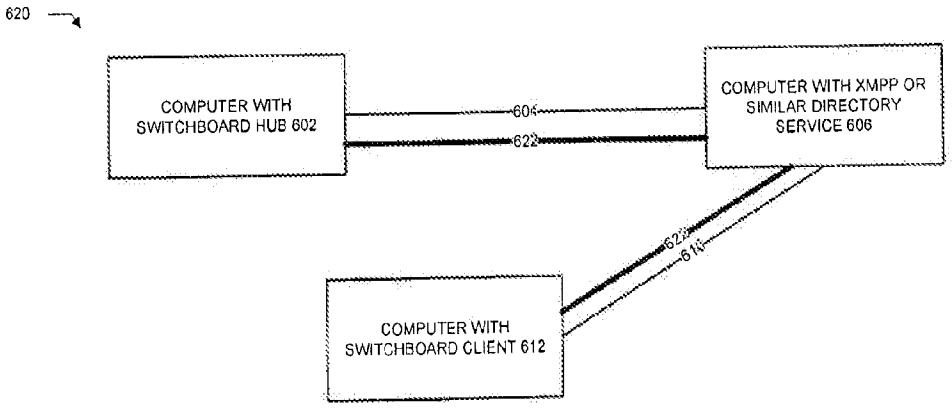

620
COMPUTER WITH SWITCHBOARD HUB 602
604
622
COMPUTER WITH XMPP OR SIMILAR DIRECTORY SERVICE 606
624
616
COMPUTER WITH SWITCHBOARD CLIENT 612

FIG 6b.

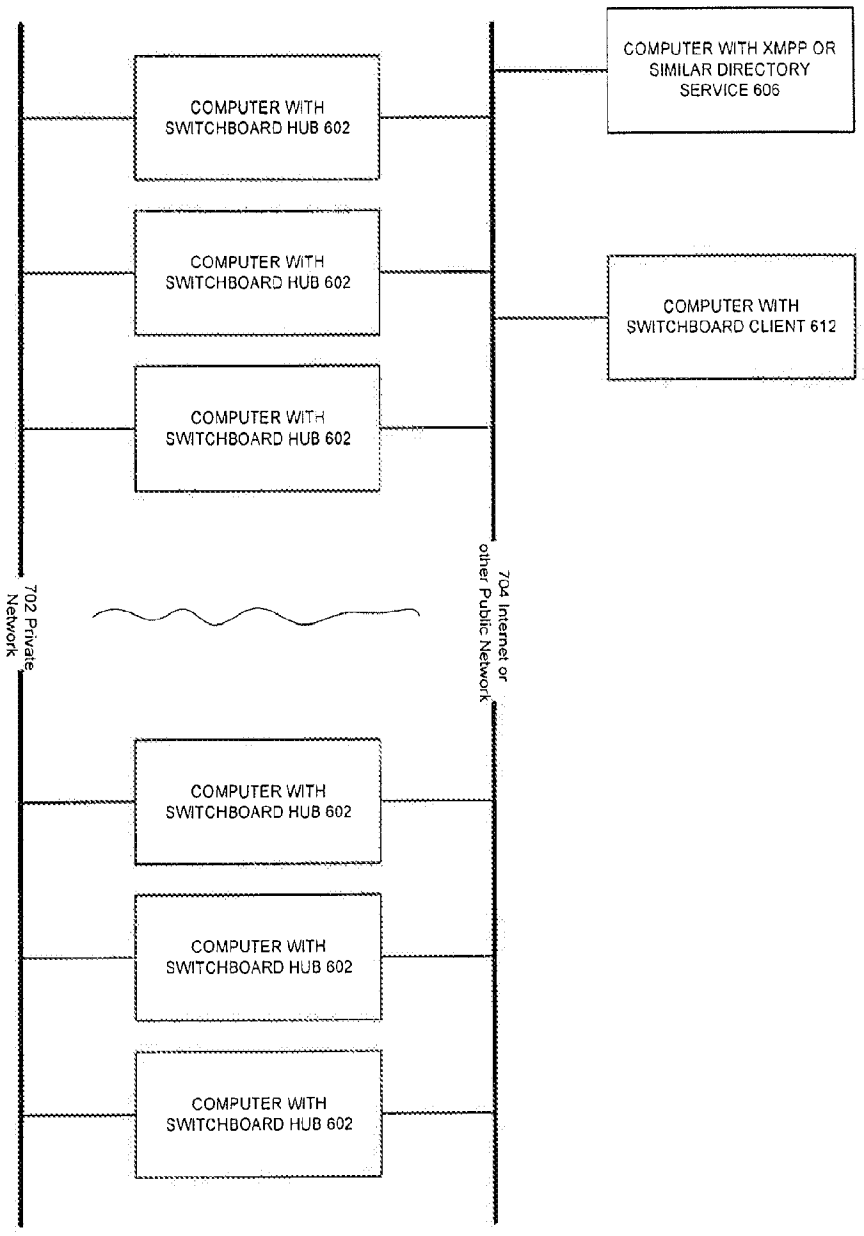

700
COMPUTER WITH XMPP OR SIMILAR DIRECTORY SERVICE 606
COMPUTER WITH SWITCHBOARD HUB 602
COMPUTER WITH SWITCHBOARD HUB 602
COMPUTER WITH SWITCHBOARD CLIENT 612
COMPUTER WITH SWITCHBOARD HUB 602
702 Private Network
704 Internet or other Public Network
COMPUTER WITH SWITCHBOARD HUB 602
COMPUTER WITH SWITCHBOARD HUB 602
COMPUTER WITH SWITCHBOARD HUB 602

FIG 7.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 13/25559

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 9/00 (2013.01)
USPC - 726/15
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 726/15; IPC(8): G06F 9/00 (2013.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/150; 713/151; 726/2; IPC(8): G06F 9/00 (2013.01)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Google Scholar; Google Web; Google Patents; PatBase; PubWEST(PGPB,USPT,USOC,EPAB,JPAB);
Search Terms: switchboard, hub, client, compute, network, communicate, connect, external, global, internet, directory, Extensible Messaging, Light Directory Access Protocol, register, switch, Jingle, exchange

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0023210 A1 (Tuomenoksa et al.) 21 February 2002 (21.02.2002), entire document, especially para [0006], [0018], [0051]-[0052], [0054], [0061], [0066], [0068]-[0069], [0091], [0102], [0110], [0123], [0167], [0190], [0212]	1-20
Y	US 2011/0258453 A1 (Mansfield) 20 October 2011 (20.10.2011), entire document, especially para [0024]-[0026], [0032]	1-20
Y	US 2009/0285175 A1 (Nix) 19 November 2009 (19.11.2009), entire document, especially para [0229], [0240]	8, 10, 14, 15
Y	US 2007/0019619 A1 (Foster et al.) 25 January 2007 (25.01.2007), entire document, especially para [0008]	13
A	US 5,969,632 A (Diamant et al.) 19 October 1999 (19.10.1999), entire document	1-20
A	US 2004/0049702 A1 (Subramaniam et al.) 11 March 2004 (11.03.2004), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2013 (20.03.2013)	23 APR 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 May 2014 (01.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/066155 A2

(51) International Patent Classification:
H04L 29/02 (2006.01)

(21) International Application Number:
PCT/US2013/065619

(22) International Filing Date:
18 October 2013 (18.10.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/716,742 22 October 2012 (22.10.2012) US
13/781,596 28 February 2013 (28.02.2013) US

(71) Applicant: **GOOGLE INC.** [US/US]; 1600 Ampitheatre Parkway, Mountain Via, CA 94043 (US).

(72) Inventors: **ARINI, Nicholas, Salvatore**; 1600 Ampitheatre Parkway, Mountain Via, CA 94043 (US). **CHARLEBOIS, Owen, Arthur**; 1600 Ampitheatre Parkway, Mountain Via, CA 94043 (US).

(74) Agents: **STEARNS, Robert, L.** et al.; Dickinson Wright PLLC, 2600 W. Big Beaver Road, Suite 300, Troy, MI 48084-3312 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: MONITORING MEDIA CONSUMPTION HABITS

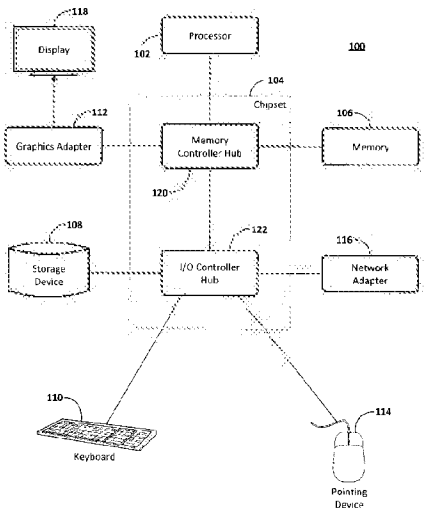


FIG. 1

(57) **Abstract**: A device to monitor media consumption, includes a data store comprising a computer readable medium storing a program of instructions for monitoring media consumption; a processor that executes the program of instructions; a user registration module to register a user associated with the device; a media detection module to detect media being consumed by the user; an interfacing module to interface with another device; and a communication module to communicate the media detection to an outside source, the interfacing module is configured to automatically detect that the other device is a fixed meter device, and if the other device is a fixed meter device, the device acknowledges the other device is detecting media.

WO 2014/066155 A2

MONITORING MEDIA CONSUMPTION HABITS

Claim of Priority

[0001] This application claims priority to U.S. Provisional Patent Application Number 61/716,742, filed October 22, 2012, entitled "Monitoring Media Consumption Habits," now pending. This patent application contains the entire Detailed Description of U.S. Provisional Application Number 61/716,742.

Background

[0002] A measurement system monitors media consumption habits by a media consumer. Thus, by being cognizant of the media consumption habits, a content provider may effectively determine prices for advertisements, or determine whether certain content displayed or presented at a specific time is effective. Media consumption may refer to a viewing a program, listening to an audio program, reading a web site, for example.

[0003] In recent times, certain media, such as television, is consumed outside of the home in greater frequencies. The advent of internet TV and other smart devices allows a media consumer to view programs over the internet, which traditionally have been distributed through cable or antenna based broadcasts.

[0004] Various techniques have been developed to monitor media consumption habits. One such technique is a fixed meter system. In a fixed meter system, a device is installed at the home. The device serves to monitor various media consumers who may reside at the home. Prior to watching, or while watching a program, each media consumer individually indicates that they are present. Further, a media consumer indicates when they leave the room as well. In this way, the fixed meter system may correlate the program being broadcast from a device with the number of media consumers indicating their presence. Thus, the device can provide

a measurement if only one, some or all the media consumers who reside in the home watch a program.

[0005] In another technique, a media consumer may be provided a portable metering system to monitor the media consumer's media consumption. Thus, if the media consumer walks into an establishment with a radio program being broadcast, the portable metering system may detect that the media consumer is exposed to the radio program. The portable metering system may be equipped with the capability of detecting the radio program by various techniques, such as detecting a digital watermark embedded in the audio or matching the detected audio with audio fingerprints stored in a database. Unlike the fixed metering system, the portable metering system allows for monitoring of consumption habits both inside and outside a home.

Summary

[0006] A device to monitor media consumption, includes a data store comprising a computer readable medium storing a program of instructions for monitoring media consumption; a processor that executes the program of instructions; a user registration module to register a user associated with the device; a media detection module to detect media being consumed by the user; an interfacing module to interface with another device; and a communication module to communicate the media detection to an outside source the interfacing module is configured to automatically detect that the other device is a fixed meter device, and if the other device is a fixed meter device, the device acknowledges the other device is detecting media.

Description of the Drawings

[0007] The detailed description refers to the following drawings, in which like numerals refer to like items, and in which:

[0008] FIG. 1 is a high-level block diagram illustrating an example computer;

[0009] FIG. 2 illustrates an example of a system for monitoring media consumption habits;

[0010] FIG. 3 illustrates an example of a method for monitoring media consumption; and

[0011] FIG. 4 illustrates an example implementation of the system of FIG. 2.

Detailed Description

[0012] With respect to known techniques for monitoring media consumption habits, several issues exist preventing or limiting an accurate data measurement. Also, various inconveniences to users exist, thereby preventing an easy and seamless experience. Further, in situations with multiple implementations existing for monitoring at-home consumption versus remote consumption, duplicate detections for a single media consumption event are likely.

[0013] For example, in a fixed metering system, every media consumer who resides in the home logs in and registers as a present viewer while consuming media (e.g. viewing a television program). Over time, some media consumers may find this process to be inconvenient. Thus, to work around the fixed metering system, only one media consumer may login as a registered viewer, while other media consumers viewing the program may avoid this process because they find it to be inconvenient. Thus, the fixed metering system, due to its perceived inconvenience, may not provide an accurate indication of media consumption for all individuals in a household.

[0014] In the portable meter system, a media consumer entering a room or location where a fixed meter system is also installed may be registered as a media consumer with both the fixed meter system and the portable metering system. The media consumer may be registered as present by an operator of a remote control that interfaces with the fixed meter system. In this case, with overlapping fixed and portable metering systems, the media consumer is detected twice (by the fixed meter system and the portable metering system), while only viewing one program, thereby confounding the accuracy of detection.

[0015] Disclosed herein are methods and systems for monitoring media consumption. The aspects disclosed herein provide a user-friendly technique for monitoring media consumption, while maintaining and improving the accuracy of detection. The aspects disclosed herein allow for the integration of a fixed meter system with a portable metering system, and may obviate a media consumer manually logging-in to a fixed meter system to denote presence while consuming media.

[0016] In situations in which the systems discussed here collect personal information about users, or may make use of personal information, the users will be provided with an opportunity to control whether programs or features collect user information (*e.g.*, information about a user's social network, social actions or activities, a user's preferences, or a user's current location), or to control whether and/or how to receive content from the content server that may be more relevant to the user. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user will have control over how information is collected about the user and used by a content server.

[0017] FIG. 1 is a high-level block diagram illustrating an example computer 100. The computer 100 includes at least one processor 102 coupled to a chipset 104. The chipset 104 includes a memory controller hub 120 and an input/output (I/O) controller hub 122. A memory 106 and a graphics adapter 112 are coupled to the memory controller hub 120, and a display 118 is coupled to the graphics adapter 112. A storage device 108, keyboard 110, pointing device 114, and network adapter 116 are coupled to the I/O controller hub 122. Other aspects of the computer 100 may have different architectures.

[0018] The storage device 108 is a non-transitory computer-readable storage medium such as a hard drive, compact disk read-only memory (CD-ROM), DVD, or a solid-state memory device. The memory 106 holds instructions and data used by the processor 102. The pointing device 114 is a mouse, track ball, or other type of pointing device, and is used in combination with the keyboard 110 to input data into the computer system 100. The graphics adapter 112 displays images and other information on the display 118. The network adapter 116 couples the computer system 100 to one or more computer networks.

[0019] The computer 100 is adapted to execute computer program modules for providing functionality described herein. As used herein, the term "module" refers to computer program logic used to provide the specified functionality. Thus, a module can be implemented in hardware, firmware, and/or software. In one aspect, program

modules are stored on the storage device 108, loaded into the memory 106, and executed by the processor 102.

[0020] The types of computers used by the entities and processes disclosed herein can vary depending upon the aspect and the processing power required by the entity. The computer 100 may be a mobile device, tablet, smartphone or any sort of computing element with the above-listed elements. For example, a video corpus, such as a hard disk, solid state memory or storage device, might be stored in a distributed database system comprising multiple blade servers working together to provide the functionality described herein. The computers can lack some of the components described above, such as keyboards 110, graphics adapters 112, and displays 118.

[0021] FIG. 2 illustrates an example of a system for monitoring media consumption habits 200. The system 200 includes a user registration module 210, a media detection module 220, an interfacing module 230, a communication module 240, and a mode selection module 250.

[0022] The system 200 may be installed on the computer 100, as shown in FIG. 1. The computer 100 may be a portable device, such as a smart phone or tablet, and thus, the media consumer may incorporate the computer 100 as an accessory that normally accompanies them.

[0023] The user registration module 210 allows the system 200 to register a specific user as the media consumer associated with system 200. The user registration module 210 may be equipped with a login screen that allows a specific user to register as the media consumer. Alternatively, the user registration module 210 may automatically detect that the owner associated with computer 100 (that the system 200 is implemented on) is the media consumer.

[0024] The media detection module 220 detects media that the media consumer identified by the user registration module 210 may come in contact with. Media may include television programs, advertisements, radio broadcasts, movies, movies, for example. The media detection module 220 may employ various techniques for detecting media. In one instance, the media detection module 220 may automatically detect the media being consumed by uploading the audio associated with the media, and comparing it with audio stored in a database. Alternatively, or in

addition to, the media detection module 220 may allow a user to manually enter an acknowledgement that a specific media item is being consumed.

[0025] The interfacing module 230 interfaces with other metering systems in a general proximity of the system 200. The interfacing module 230 may employ various communication techniques, such as short-range communication, near field communication, infrared communication, for example. The system 200 may determine that media consumption detected by the media detection module 220 occurs in a location with an established fixed meter system, such as a second system 200 set to stationary mode, for example. In this case, the interfacing module 230 may override the media detection module 220, and control the system 200 to not record media detection when in the presence of a fixed meter system. As explained above, the overriding prevents a double recordation of media detection.

[0026] The interfacing module 230 may automatically detect that a fixed meter system is in the same location where the media consumption occurs. Alternatively, or in addition to, the interfacing module 230 may allow the media consumer to manually indicate that the system 200 is in the same location as a fixed meter system.

[0027] Thus, the interfacing module 230 allows the system 200 to acknowledge that other metering systems (such as a fixed meter system) may also be recording media consumption of the media consumer associated with the system 200. The interfacing module 230 may use this acknowledgment to disable or edit the recordation of media consumption when the system 200 is in the presence of another metering system.

[0028] The communication module 240 communicates the media detection to an outside source, such as a ratings agency, that tracks media consumption. The communication module 240 may communicate data pertaining to the media consumed, the media consumer, the location of the media consumption, or other data associated with the system 200. The communication module 240 may employ various communication techniques. The communication module 240 may also delay communication based on predefined conditions, such as the availability of a WiFi connection, or at certain user-defined time periods.

[0029] The mode selection module 250 may allow the system 200 to toggle between operating in a stationary mode (i.e. a fixed meter system) or in a portable

mode (i.e. a portable metering system). Depending on the implementation, the system 200 may be set to one of the modes based on the application. In this way, both a fixed meter system and a portable metering system may be implemented on a device such as a smart phone implementing system 200. By providing the mode selection module 250, separate devices do not need to be manufactured for a fixed meter system and a portable metering system.

[0030] The user registration module 210 and the interfacing module 230 may operate differently in the stationary mode versus the portable mode. For example, if a second system 200 (in stationary mode) is located near a media producing device, the interfacing module 230 may detect that a smart phone associated with a media consumer is in a nearby location. The interfacing module 230 may detect that metering systems associated with a media consumer are nearby, by employing various communication techniques, such as short range communication, near field communication, infrared communication, for example. Thus, the interfacing module 230 may communicate to the user registration module 210 that a media consumer is in the presence of a media device associated with the system 200 (in stationary mode). Thus, based on the media consumer identified by the interfacing module 230, the system 200 (in stationary mode) may identify that the media consumer is at a nearby location.

[0031] By allowing the second system 200 (in stationary mode) to automatically perform a user registration based on a detection by the interfacing module 230 that a system 200 associated with a media consumer is nearby, a media consumer may not have to perform a manual registration to denote the media consumer's presence. Further, the second system 200 is more likely to register multiple media consumers, due to the second system 200 recognizing each media consumer's personal device.

[0032] As explained above, the second system 200 may identify the media consumer by detecting the device via the interfacing module 230. The system 200 may store a database that associates various devices with a respective media consumer. Alternatively, the system 200 may request or prompt that a media consumer manually login when it detects that a media consumer is nearby. The device associated with the media consumer may or may not implement system 200.

[0033] FIG. 3 illustrates an example of a method for monitoring media consumption 300. The method 300 may be implemented on the system 200 depicted in FIG. 2.

[0034] In operation 310, the system 200 registers a media consumer. The registration can occur through an automatic detection based on the operation of the computer 100, or through a manual process of allowing the media consumer to enter relevant information, such as the media consumer's identity or an authentication.

[0035] In operation 320, the system 200 detects media consumption. As explained in reference to FIG. 2, the media consumption detection may be either automatic or manually performed. If the media consumption is detected automatically, a user may ascertain whether the system 200 was correct in identifying and detecting the media.

[0036] Thus, if the system 200, implemented on computer 100, is worn or carried by a media consumer who enters into an establishment with a popular radio or television program being broadcast, in operation 320, the program may be identified and the system 200 may record data pertaining to the media consumption by the user.

[0037] In operation 330, the system 200 interfaces with any devices that may be at a nearby location. In performing the interfacing, the system 200 may determine if a fixed meter system, for example a second system 200 (in stationary mode), also detected the media consumption recorded in operation 320. If in operation 330 a determination is made that the second system 200 is at a nearby location, and the second system 200 also records media consumption, the system 200 may determine that the data recorded in operation 320 is redundant. Accordingly, the system 200 may delete data pertaining to the recordation of media consumption.

[0038] In operation 340, the system 200 may communicate the data recorded to a reporting or monitoring entity. As explained in operation 330, the data recorded in operation 320 is verified to be a unique recordation or a redundant recordation. The system 200 may delay the reporting of the data until the system 200 is in the range of a specific communication protocol, such as WiFi.

[0039] FIG. 4 illustrates an example implementation of the system 200. As shown in FIG. 4, a smart phone 400A (implemented with a system 200 set to stationary mode) is placed near a media device 410. A media consumer 420 carries

a smart phone 400B (implemented with a system 200 set to portable mode), and actively views and listens to media sourced from the media device 410.

[0040] In the example shown in FIG. 4, the smart phone 400A detects that smart phone 400B is at a nearby location. Thus, smart phone 400A may automatically register media consumer 420, and record media consumption by media consumer 420.

[0041] Further, the smart phone 400B detects that smart phone 400A is in a nearby position, and that smart phone 400B is capable of media detection. Smart phone 400B may not perform any recordation of media consumption while smart phone 400B is in a nearby location to smart phone 400A.

[0042] Based on the systems and methods disclosed herein, an accurate metering of media consumption is realized by ensuring that multiple metering systems work together to avoid multiple recordation of a single media consumption event. Further, because the aspects disclosed herein are implemented on a device such as a smart phone, a convenience to the user is realized due to the process of manually registering one's presence prior to media consumption recordation being obviated.

[0043] In addition to the above, various modifications to the aspects disclosed herein may be implemented. For example, if a user authorizes usage of the aspects disclosed herein with a location detection unit, the location detection unit may be incorporated with the media detection disclosed herein. Thus, an entity that monitors data may ascertain where media is being consumed along with the actual detection.

[0044] Additionally, the aspects disclosed herein may be incorporated with an automatic payment system. For example, if the media consumer pays for an item at a store using a portable device, the same portable device may be used to detect media consumption. In this way, information about media consumption and commerce may be correlated.

[0045] Certain of the devices shown in Figure 1 include a computing system. The computing system includes a processor (CPU) and a system bus that couples various system components including a system memory such as read only memory (ROM) and random access memory (RAM), to the processor. Other system memory may be available for use as well. The computing system may include more than one processor or a group or cluster of computing system networked together to provide

greater processing capability. The system bus may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. A basic input/output (BIOS) stored in the ROM or the like, may provide basic routines that help to transfer information between elements within the computing system, such as during start-up. The computing system further includes data stores, which maintain a database according to known database management systems. The data stores may be implemented in many forms, such as a hard disk drive, a magnetic disk drive, an optical disk drive, tape drive, or another type of computer readable media which can store data that are accessible by the processor, such as magnetic cassettes, flash memory cards, digital versatile disks, cartridges, random access memories (RAMs) and, read only memory (ROM). The data stores may be connected to the system bus by a drive interface. The data stores provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the computing system.

[0046] To enable human (and in some instances, machine) user interaction, the computing system may include an input device, such as a microphone for speech and audio, a touch sensitive screen for gesture or graphical input, keyboard, mouse, motion input, and so forth. An output device can include one or more of a number of output mechanisms. In some instances, multimodal systems enable a user to provide multiple types of input to communicate with the computing system. A communications interface generally enables the computing device system to communicate with one or more other computing devices using various communication and network protocols.

[0047] The preceding disclosure refers to a number of flow charts and accompanying descriptions to illustrate the aspects represented in Figure 3. The disclosed devices, components, and systems contemplate using or implementing any suitable technique for performing the steps illustrated in these figures. Thus, Figure 3 is for illustration purposes only and the described or similar steps may be performed at any appropriate time, including concurrently, individually, or in combination. In addition, many of the steps in these flow charts may take place simultaneously and/or in different orders than as shown and described. Moreover,

the disclosed systems may use processes and methods with additional, fewer, and/or different steps.

[0048] Aspects disclosed herein can be implemented in digital electronic circuitry, or in computer software, firmware, or hardware, including the herein disclosed structures and their equivalents. Some aspects can be implemented as one or more computer programs, i.e., one or more modules of computer program instructions, encoded on a tangible computer storage medium for execution by one or more processors. A computer storage medium can be, or can be included in, a computer-readable storage device, a computer-readable storage substrate, or a random or serial access memory. The computer storage medium can also be, or can be included in, one or more separate tangible components or media such as multiple CDs, disks, or other storage devices. The computer storage medium does not include a transitory signal.

[0049] As used herein, the term processor encompasses all kinds of apparatus, devices, and machines for processing data, including by way of example a programmable processor, a computer, a system on a chip, or multiple ones, or combinations, of the foregoing. The processor can include special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application-specific integrated circuit). The processor also can include, in addition to hardware, code that creates an execution environment for the computer program in question, e.g., code that constitutes processor firmware, a protocol stack, a database management system, an operating system, a cross-platform runtime environment, a virtual machine, or a combination of one or more of them.

[0050] A computer program (also known as a program, module, engine, software, software application, script, or code) can be written in any form of programming language, including compiled or interpreted languages, declarative or procedural languages, and the program can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, object, or other unit suitable for use in a computing environment. A computer program may, but need not, correspond to a file in a file system. A program can be stored in a portion of a file that holds other programs or data (e.g., one or more scripts stored in a markup language document), in a single file dedicated to the program in question, or in multiple coordinated files (e.g., files that store one or more modules, sub-programs, or portions of code). A

computer program can be deployed to be executed on one computer or on multiple computers that are located at one site or distributed across multiple sites and interconnected by a communication network.

[0051] To provide for interaction with an individual, the herein disclosed aspects can be implemented using an interactive display, such as a graphical user interface (GUI). Such GUI's may include interactive features such as pop-up or pull-down menus or lists, selection tabs, scannable features, and other features that can receive human inputs.

[0052] The computing system disclosed herein can include clients and servers. A client and server are generally remote from each other and typically interact through a communications network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other. In some aspects, a server transmits data (e.g., an HTML page) to a client device (e.g., for purposes of displaying data to and receiving user input from a user interacting with the client device). Data generated at the client device (e.g., a result of the user interaction) can be received from the client device at the server.

We claim:

1. A device to monitor media consumption, comprising:

a data store comprising a computer readable medium storing a program of instructions for monitoring media consumption;

a processor that executes the program of instructions;

a user registration module to register a user associated with the device;

a media detection module to detect media being consumed by the user;

an interfacing module to interface with another device; and

a communication module to communicate the media detection to an outside source,

the interfacing module is configured to automatically detect that the other device is a fixed meter device, and if the other device is a fixed meter device, the device acknowledges the other device is detecting media.

2. The device according to claim 1, wherein the user registration module registers the user via an authentication process.

3. The device according to claim 1, wherein the user registration module automatically registers the user based on prior information associated with the device.

4. The device according to claim 1, further comprising a mode switching module to set the device in a stationary mode or a portable mode.

5. The device according to claim 4, wherein the device is a mobile device.

6. The device according to claim 1, the interfacing module interfaces with other devices via short range communication.

7. The device according to claim 1, wherein if the other device is a fixed meter device, the device deactivates the media detection module.

8. The device according to claim 1, wherein if the other device is a fixed meter device, the device allows the user to manually deactivate the media detection module.

9. A method for monitoring media consumption via a device, comprising:

registering a user associated with the device;

detecting media being consumed by the user;

interfacing with another device to meter the media being consumed;

communicating the media detection to an outside source; and

detecting that the other device is a fixed meter device, and if the other device is a fixed meter device, acknowledging to the user via the device that the other device is detecting media,

the method being performed by a processor.

10. The method according to claim 9, wherein the registration is performed via an authentication process.

11. The method according to claim 9, wherein the registration automatically registers the user based on prior information associated with the device.

12. The method according to claim 9, further comprising allowing the user to set the device in a stationary mode or a portable mode.

13. The method according to claim 12, wherein the device is a mobile device.

14. The method according to claim 9, wherein the interfacing is performed via short range communication.

15. The method according to claim 9, wherein if the other device is a fixed meter device, the device deactivates the detection of media consumption.

16. The method according to claim 9, wherein if the other device is a fixed meter device, the device allows the user to manually deactivate the detection of media consumption.

17. A system for monitoring media consumption, comprising:

a first detection device associated with a user to detect media consumption of the user; and

a second detection device associated with a media device to detect media consumption of the user,

when the first detection device and the second detection device are proximal to each other, either the first detection device or the second detection device disables the detection of media.

18. The system according to claim 17, wherein the first detection device and the second detection device are mobile devices.

19. The system according to claim 17, wherein the first detection device and the second detection device communicate to each other via short range communication.

20. The system according to claim 17, wherein the media device is an internet television.

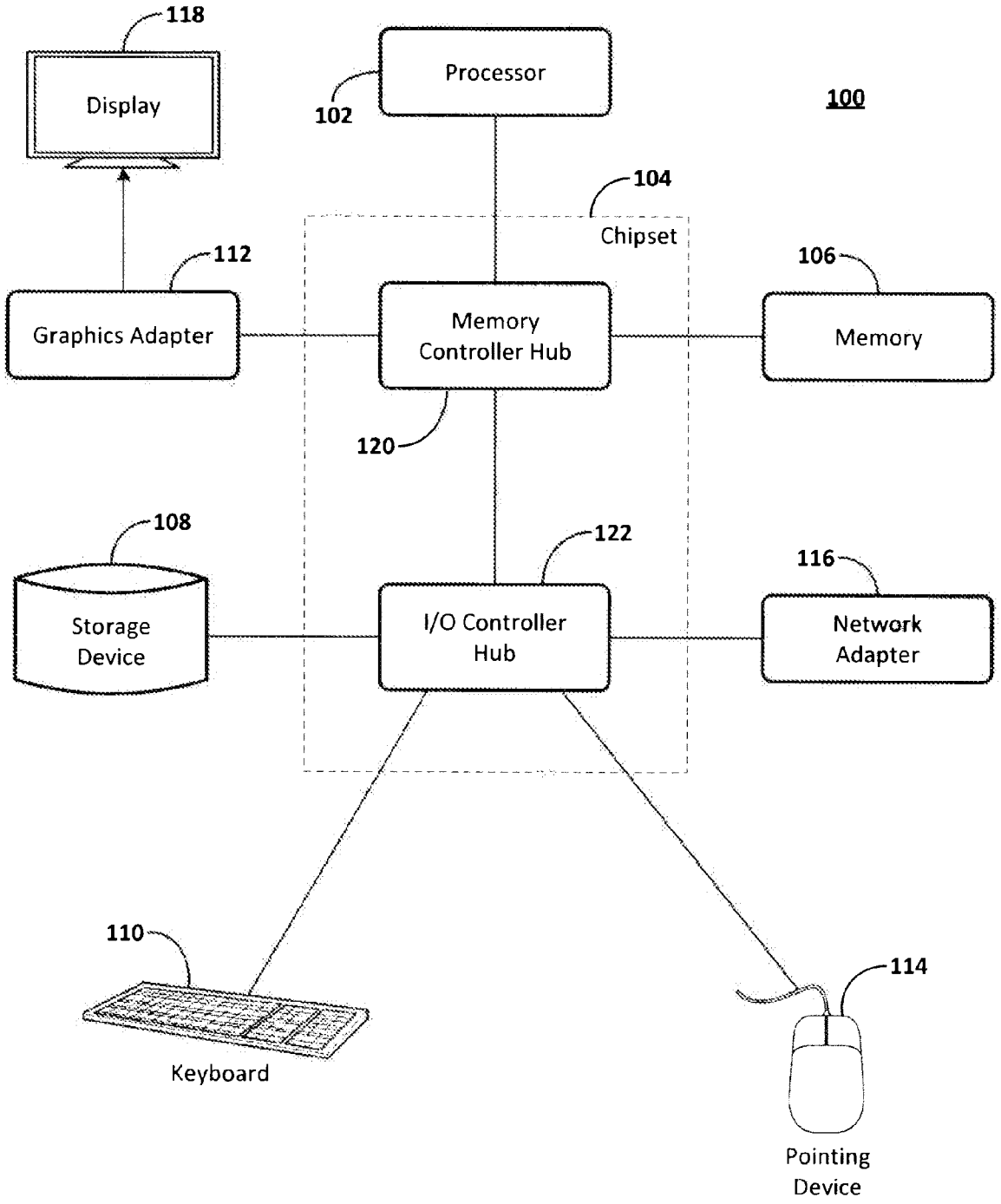

118
Display
Processor
102
100
104
Chipset
112
Graphics Adapter
Memory Controller Hub
106
Memory
120
108
Storage Device
122
I/O Controller Hub
116
Network Adapter
110
Keyboard
114
Pointing Device

FIG. 1

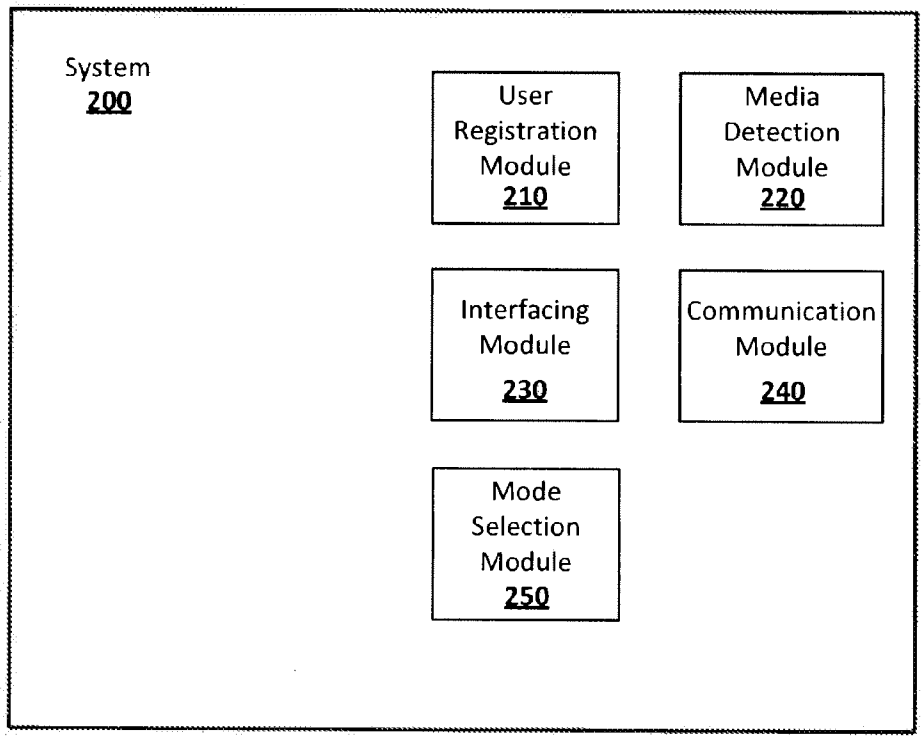

System
200
User Registration Module
210
Media Detection Module
220
Interfacing Module
230
Communication Module
240
Mode Selection Module
250

FIG. 2

300

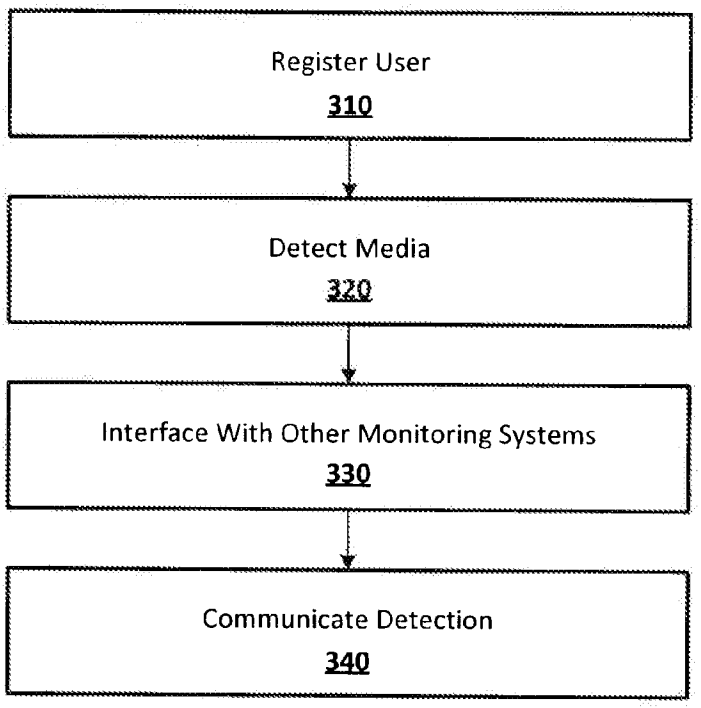

Register User
310
Detect Media
320
Interface With Other Monitoring Systems
330
Communicate Detection
340

FIG. 3

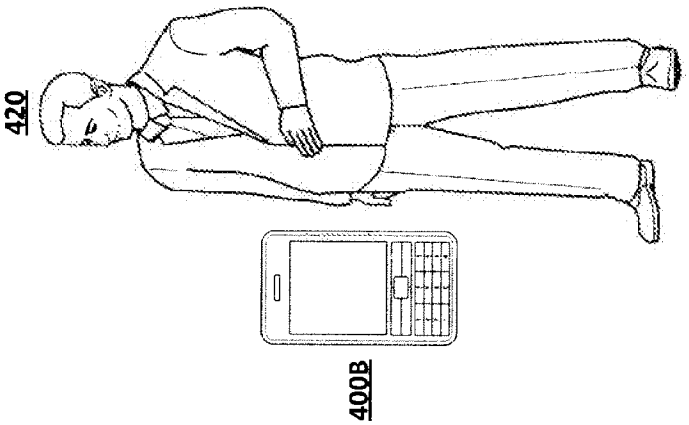
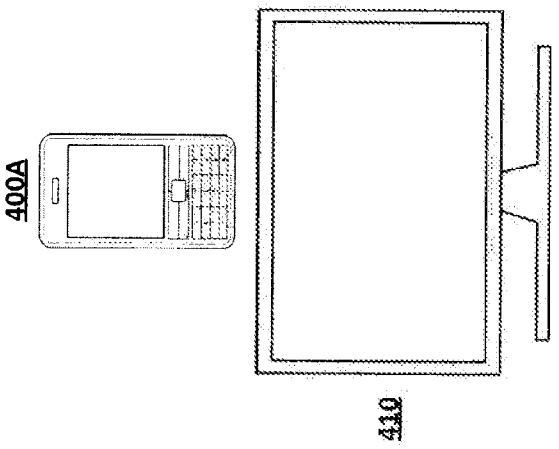


FIG. 4



Espacenet

Bibliographic data: WO2014117599 (A1) — 2014-08-07

ROUTING DOMAIN SELECTION METHOD, DEVICE AND SYSTEM

Inventor(s): LIAO HUI [CN]; ZENG BO [CN] ± (LIAO, HUI, ; ZENG, BO)

Applicant(s): HUAWEI TECH CO LTD [CN] ± (HUAWEI TECHNOLOGIES CO., LTD)

Classification: **- international:** ***H04L12/721; H04L12/733***
- cooperative:

Application number: WO2013CN89785 20131218

Priority number(s): CN2013141052 20130201

Also published as: CN103973565 (A)

Abstract of WO2014117599 (A1)

Provided in an embodiment of the present invention are a routing domain selection method, device and system, the routing domain selection method comprising: a source node transmits a first public land mobile network identity (PLMN ID) to a target node, the PLMN ID being the same PLMN ID in any one of the source nodes and the destination nodes; if the target node receives the first PLMN ID, then the source node receives a reply message transmitted by the target node; and the source node transmits a message requesting establishment of a communication interface to the target node via a routing domain corresponding to the first PLMN ID. The routing domain selection method, device and system provided in the embodiment of the present invention are used to establish a

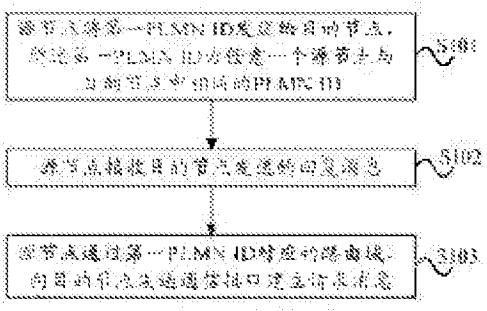


图 1 / FIG. 1

S101 A SOURCE NODE TRANSMITS A FIRST PUBLIC LAND MOBILE NETWORK IDENTITY (PLMN ID) TO A TARGET NODE, THE PLMN ID BEING THE SAME PLMN ID IN ANY ONE OF THE SOURCE NODES AND THE DESTINATION NODES

S102 THE SOURCE NODE RECEIVES A REPLY MESSAGE TRANSMITTED BY THE TARGET NODE

S103 THE SOURCE NODE TRANSMITS A MESSAGE REQUESTING ESTABLISHMENT OF A COMMUNICATION INTERFACE TO THE TARGET NODE VIA A ROUTING DOMAIN CORRESPONDING TO THE FIRST PLMN ID

network connection between communication nodes by using a proper routing domain.

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 8 月 7 日 (07.08.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/117599 A1

(51) 国际专利分类号:
H04L 12/721 (2013.01) *H04L 12/733* (2013.01)

(21) 国际申请号: PCT/CN2013/089785

(22) 国际申请日: 2013 年 12 月 18 日 (18.12.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310041052.9 2013 年 2 月 1 日 (01.02.2013) CN

(71) 申请人: **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **廖晖 (LIAO, Hui)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
曾博 (ZENG, Bo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: ROUTING DOMAIN SELECTION METHOD, DEVICE AND SYSTEM

(54) **发明名称**: 路由域选择方法、装置和系统

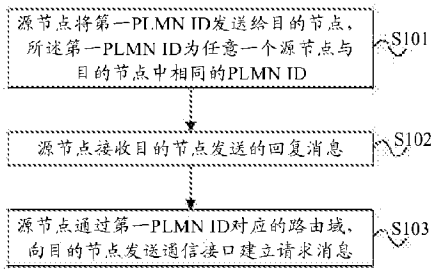


图 1 / FIG. 1

S101 A SOURCE NODE TRANSMITS A FIRST PUBLIC LAND MOBILE NETWORK IDENTITY (PLMN ID) TO A TARGET NODE, THE PLMN ID BEING THE SAME PLMN ID IN ANY ONE OF THE SOURCE NODES AND THE DESTINATION NODES

S102 THE SOURCE NODE RECEIVES A REPLY MESSAGE TRANSMITTED BY THE TARGET NODE

S103 THE SOURCE NODE TRANSMITS A MESSAGE REQUESTING ESTABLISHMENT OF A COMMUNICATION INTERFACE TO THE TARGET NODE VIA A ROUTING DOMAIN CORRESPONDING TO THE FIRST PLMN ID

(57) **Abstract**: Provided in an embodiment of the present invention are a routing domain selection method, device and system, the routing domain selection method comprising: a source node transmits a first public land mobile network identity (PLMN ID) to a target node, the PLMN ID being the same PLMN ID in any one of the source nodes and the destination nodes; if the target node receives the first PLMN ID, then the source node receives a reply message transmitted by the target node; and the source node transmits a message requesting establishment of a communication interface to the target node via a routing domain corresponding to the first PLMN ID. The routing domain selection method, device and system provided in the embodiment of the present invention are used to establish a network connection between communication nodes by using a proper routing domain.

(57) **摘要**: 本发明实施例提供一种路由域选择方法、装置和系统，一种路由域选择方法包括：源节点将第一通用陆地移动网络标识 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述源节点与所述目的节点中相同的 PLMN ID；若所述目的节点接受所述第一 PLMN ID，则所述源节点接收所述目的节点发送的回复消息；所述源节点通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送通信接口建立请求消息。本发明实施例提供的路由域选择方法、装置和系统，用于在通信节点之间使用正确的路由域建立网络连接。

WO 2014/117599 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

路由域选择方法、装置和系统

本申请要求于 2013 年 02 月 01 日提交中国专利局、申请号为201310041052.9、发明名称为"路由域选择方法、装置和系统"的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明实施例涉及通信技术，尤其涉及一种路由域选择方法、装置和系统。

背景技术

移动通信网络中，为每个运营商分配了专属的陆地通用移动网络标识（Public Land Mobile Network Identity，PLMN ID），运营商使用的网络设备中均包含该运营商的 PLMN ID，根据 PLMN ID 可以判断网络设备归属哪个运营商。

LTE 网络共享是指多个运营商共享无线接入网演进型基站（Evolved NodeB，eNodeB），或者共享基站及一部分或全部核心网设备，例如移动性管理实体（Mobility Management Entity，MME）、服务网关（Serving Gateway，S-GW）等的一种网络架构，运营商可以通过共享网络为处于其他运营商覆盖范围内的用户提供网络服务。被共享的 eNodeB 称为共享 eNodeB，共享 eNodeB 的拥有者称为主运营商，使用该共享 eNodeB 的运营商称为从运营商。从运营商除了通过共享网络提供网络服务外，还可以拥有自己的专用网络，专用网络中的 eNodeB 供该运营商专用，称为自有 eNodeB。

X2 接口是指两个 eNodeB 之间的逻辑连接，网络中的两个 eNodeB 之间通过 X2 接口连接并交换数据。当共享网络和专用网络共同部署时，共享网络中的共享 eNodeB 和专用网络中的自有 eNodeB 需要通过建立 X2 接口进行数据传输。共享网络和专用网络的 IP 地址由各自网络的运营商独立规划，因此共享网络与专用网络之间的 IP 地址可能重叠而发生冲突。为了解

决 IP 冲突的问题，共享网络一般采用多重虚拟路由转发技术来隔离不同运营商的路由域。共享 eNodeB 具有多重路由域，但共享 eNodeB 之间以及共享 eNodeB 与自有 eNodeB 之间建立 X2 接口时，共享 eNodeB 可能选择错误的路由域，从而可能导致 X2 接口建立失败或者连接到错误的 eNodeB。

发明内容

本发明实施例提供一种路由域选择方法、装置和系统，用于在通信节点之间使用正确的路由域建立网络连接。

第一方面提供一种路由域选择方法，包括:

源节点将第一 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述源节点与所述目的节点中相同的 PLMN ID;

若所述目的节点接受所述第一 PLMN ID，则

所述源节点接收所述目的节点发送的回复消息;

所述源节点通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送通信接口建立请求消息。

在第一方面第一种可能的实现方式中，还包括:

若所述目的节点不接受所述第一 PLMN ID，则

所述源节点接收所述目的节点发送的第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

所述源节点向所述目的节点发送回复消息;

所述源节点接收所述目的节点通过所述第二 PLMN ID 对应的路由域发送的通信接口建立请求消息。

在第一方面第二种可能的实现方式中，若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 相同，则所述第一 PLMN ID 为所述源节点的主运营商 PLMN ID;

若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 不同，并且所述目的节点的主运营商 PLMN ID 与所述源节点的任一

PLMN ID 相同，则所述第一 PLMN ID 为所述目的节点的主运营商 PLMN ID。。

在第一方面第三种可能的实现方式中，所述第一 PLMN ID 为所述源节点和所述目的节点之间最短的路由长度对应的 PLMN ID。

结合第一方面至第一方面第三种可能的实现方式中任一种可能的实现方式，在第四种可能的实现方式中，所述源节点将第一 PLMN ID 发送给目的节点包括:

所述源节点通过自配置透传消息将所述第一PLMN ID发送给所述目的节点。。

第二方面提供一种路由域选择方法，其特征在于，包括:

目的节点接收源节点发送的第一 PLMN ID，所述第一 PLMN ID 为任意一个所述源节点与所述目的节点中相同的 PLMN ID;

若所述目的节点接受所述第一 PLMN ID，则

所述目的节点向所述源节点发送回复消息;

所述目的节点接收所述源节点通过所述第一PLMN ID对应的路由域发送的通信接口建立请求消息。

在第二方面第一种可能的实现方式中，还包括:

若所述目的节点不接受所述第一 PLMN ID，则

所述目的节点将第二 PLMN ID 发送给所述源节点，所述第二 PLMN ID 为除所述第一PLMN ID以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

所述目的节点接收所述源节点发送的回复消息;

所述目的节点通过所述第二 PLMN ID 对应的路由域，向所述源节点发送通信接口建立请求消息。

在第二方面第二种可能的实现方式中，所述目的节点将第二 PLMN ID 发送给所述源节点，包括:

所述目的节点通过自配置透传消息将所述第二PLMN ID发送给所述源节点。

结合第二方面第二种可能的实现方式，在第三种可能的实现方式中，所述第二PLMN ID为所述源节点和所述目的节点之间最短的路由域长度对应的 PLMN ID。

第三方面提供一种通信节点，包括:

第一发送模块，用于将第一 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述通信节点与所述目的节点中相同的 PLMN ID;

第一接收模块，用于接收所述目的节点发送的回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

第二发送模块，用于当所述第一接收模块接收到所述目的节点发送的回复消息时，通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送通信接口建立请求消息；当所述第一接收模块接收到所述目的节点发送的第二 PLMN ID 时，则向所述目的节点发送回复消息;

第二接收模块，用于当所述第二发送模块向所述目的节点发送回复消息时，接收所述目的节点通过所述第二 PLMN ID 对应的路由域发送的通信接口建立请求消息。

在第三方面第一种可能的实现方式中，若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 相同，则所述第一 PLMN ID 为所述源节点的主运营商 PLMN ID;

若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 不同，并且所述目的节点的主运营商 PLMN ID 与所述源节点的任一 PLMN ID 相同，则所述第一 PLMN ID 为所述目的节点的主运营商 PLMN ID。

在第三方面第二种可能的实现方式中，所述第一 PLMN ID 为所述源节点和所述目的节点之间最短的路由长度对应的 PLMN ID。

结合第三方面至第三方面第二种可能的实现方式中的任一种可能的实现方式，在第三种可能的实现方式中，所述第一发送模块，具体用于通过自配置透传消息将所述第一 PLMN ID 发送给所述目的节点。。

第四方面提供一种通信节点，包括:

第一接收模块，用于接收源节点发送的第一 PLMN ID，所述第一 PLMN ID 为任意一个所述源节点与所述通信节点中相同的 PLMN ID;

第一发送模块，用于向所述源节点发送回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

第二接收模块，用于当所述第一发送模块向所述源节点发送回复消息时，接收所述源节点通过所述第一 PLMN ID 对应的路由域发送的通信接口建立请求消息；当所述第一发送模块向所述源节点发送第二 PLMN ID 时，接收所述源节点发送的回复消息；

第二发送模块，用于当所述第二接收模块接收到所述源节点发送的回复消息时，通过所述第二 PLMN ID 对应的路由域，向所述源节点发送通信接口建立请求消息。

在第四方面第一种可能的实现方式中，还包括：

所述第一发送模块，具体用于通过自配置透传消息将所述第二 PLMN ID 发送给所述源节点。

在第四方面第二种可能的实现方式中，所述第二 PLMN ID 为所述源节点和所述通信节点之间最短的路由域长度对应的 PLMN ID。

第五方面提供一种通信系统，包括：源节点和目的节点；

所述源节点为如第三方面任一种可能的实现方式所述的通信节点；

所述目的节点为第四方面任一种可能的实现方式所述的通信节点

本发明实施例提供的路由域选择方法、装置和系统，在通信节点间接口的建立过程中，通过选择源节点与目的节点的一个相同的 PLMN ID，并采用与该 PLMN ID 对应的路由域建立通信节点间接口，实现了在通信节点间建立网络连接时，选择正确的路由域建立接口的过程。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的路由域选择方法实施例一的流程图；

图 2 为本发明实施例提供的路由域选择方法实施例二的流程图；

图 3 为本发明实施例提供的路由域选择方法实施例三的信令流程图；

图 4 为本发明实施例提供的路由域选择方法实施例四的信令流程图；

图 5 为本发明实施例提供的路由域选择方法实施例五的信令流程图；
图 6 为本发明实施例提供的路由域选择方法实施例六的信令流程图；
图 7 为本发明实施例提供的路由域选择方法实施例七的信令流程图；
图 8 为本发明实施例提供的通信节点实施例一的结构示意图；
图 9 为本发明实施例提供的通信节点实施例二的结构示意图；
图 10 为本发明实施例提供的通信系统实施例一的结构示意图；
图 11 为本发明实施例提供的通信节点实施例五的硬件结构示意图；
图 12 为本发明实施例提供的通信节点实施例六的硬件结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

在 LTE 网络中，两个 eNodeB 之间需要建立 X2 接口时，X2 接口建立的发起 eNodeB 称为源 eNodeB，另一 eNodeB 称为目的 eNodeB。在 X2 接口建立的过程中，源 eNodeB 和目的 eNodeB 之间会交互自配置透传消息（eNB Configuration Transfer）。eNodeB 自配置透传消息中包括两个关键信元 Global eNB ID 和 Selected TAI，其中 Global eNB ID 中包含 eNodeB 的主运营商 PLMN ID，Selected TAI 中包含 eNodeB 选择使用的 PLMN ID。eNodeB 可以通过邻站配置信息得知附近其他 eNodeB 的 PLMN ID，邻站配置信息可以是预设在 eNodeB 中的，也可以是 eNodeB 通过自发现邻站方式（Auto Neighbor Relation，ANR）动态获得的，总之，eNodeB 只能与已知 PLMN ID 的其他 eNodeB 建立 X2 接口。

本发明以下各实施例所述的通信节点可以为 LTE 网络中的 eNodeB，本发明实施例的方法用于在共享 eNode 之间或者共享 eNodeB 和自有 eNodeB 之间选择正确的路由域并建立 X2 接口。但本实施例所述的通信节点和方法不以此为限，只要通信网络中的两个通信节点之间可以得知对方的 PLMN

ID，都可以使用本实施例的路由选择方法选择正确的路由并建立网络连接接口。

图 1 为本发明实施例提供的路由域选择方法实施例一的流程图，本实施例的方法用于源节点侧，如图 1 所示，本实施例的方法包括:

步骤 S101，源节点将第一 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个源节点与目的节点中相同的 PLMN ID。

具体地，通信网络中的两个通信节点之间建立接口的过程之前，源节点和目的节点可以通过邻站配置信息得知彼此的 PLMN ID，源节点或者目标节点可以在双方节点的 PLMN ID 中确定至少一个相同的 PLMN ID。通信网络中，每个运营商都有自己专属的 PLMN ID，运营商的通信节点中都包含该 PLMN ID，若运营商提供的通信节点为共享通信节点，则该通信节点中还包括其他运营商的 PLMN ID。若一个运营商 A 需要使用其他运营商的通信节点，则只能选择其他运营商提供的共享通信节点，并且该共享通信节点中需要包含运营商 A 的 PLMN ID，这样才可以在运营商 A 的通信节点和该共享通信节点之间建立网络接口，并实现网络连接。因此，在通信节点间建立接口时，首先需要判断两个通信节点之间是否存在相同的 PLMN ID，若不存在，则两个通信节点之间无法建立接口。当源节点需要建立与目的节点间的通信接口时，源节点将任意一个源节点与目的节点中相同的 PLMN ID 发送给目的节点。

步骤 S102，源节点接收目的节点发送的回复消息。

具体地，源节点将任意一个源节点与目的节点中相同的 PLMN ID 发送给目的节点后，目的节点判断是否接受使用该 PLMN ID 建立源节点与目的节点之间的通信接口，若目的节点接受使用该 PLMN ID，则源节点接收目的节点发送的回复消息，源节点可以根据该回复消息得知目的节点是否同意使用源节点选择的 PLMN ID 建立通信接口。

步骤 S103，源节点通过第一 PLMN ID 对应的路由域，向目的节点发送通信接口建立请求消息。

具体地，若源节点接收到的回复消息表示接受第一 PLMN ID，即目的节点统一使用第一 PLMN ID 建立通信接口，则源节点使用第一 PLMN ID 对应的路由域在源节点和目的节点之间建立网络接口，源节点向目的节点发送通信接口建立请求消息。通信网路中，使用基于 IP 地址的路由域连接，

每个运营商自己规划路由域中的 IP 地址，即每个 PLMN ID 对应一个路由域。网络中的每个通信节点均有自己的 IP 地址，但两个通信节点的 IP 地址处于同一个路由域中才能互相通信。共享通信节点中具有多重路由域，并且每个路由域对应一个 PLMN ID，因此，当共享通信节点之间或者共享通信节点和自有通信节点之间建立接口时，当选择了两个通信节点间相同的 PLMN ID，可以采用该 PLMN ID 对应的路由域，使用该路由域中的 IP 地址建立网络接口并实现通信。

本实施例，在通信节点间接口的建立过程中，通过选择源节点与目的节点的一个相同的 PLMN ID，并采用与该 PLMN ID 对应的路由域建立通信节点间接口，实现了在通信节点间建立网络连接时，选择正确的路由域建立接口的过程。

图 2 为本发明实施例提供的路由域选择方法实施例二的流程图，本实施例的方法用于目的节点侧，如图 2 所示，本实施例的方法包括:

步骤 S201，目的节点接收源节点发送的第一 PLMN ID，所述第一 PLMN ID 为任意一个源节点与目的节点中相同的 PLMN ID。

具体地，通信网络中的两个通信节点之间建立接口的过程之前，源节点和目的节点可以通过邻站配置信息得知彼此的 PLMN ID，源节点或者目标节点可以在双方节点的 PLMN ID 中确定至少一个相同的 PLMN ID。通信网络中，每个运营商都有自己专属的 PLMN ID，运营商的通信节点中都包含该 PLMN ID，若运营商提供的通信节点为共享通信节点，则该通信节点中还包括其他运营商的 PLMN ID。若一个运营商 A 需要使用其他运营商的通信节点，则只能选择其他运营商提供的共享通信节点，并且该共享通信节点中需要包含运营商 A 的 PLMN ID，这样才可以在运营商 A 的通信节点和该共享通信节点之间建立网络接口，并实现网络连接。因此，在通信节点间建立接口时，首先需要判断两个通信节点之间是否存在相同的 PLMN ID，若不存在，则两个通信节点之间无法建立接口。当源节点请求和目的节点建立通信接口时，目的节点接收到任意一个源节点与目的节点中相同的 PLMN ID，目的节点根据该 PLMN ID 进行进一步判断，目的节点可以使用该 PLMN ID 与源节点建立通信接口，还可以重新选择一个新的 PLMN ID 并使用新的 PLMN ID 建立通信接口。

步骤 S202，目的节点向源节点发送回复消息。

具体地，若目的节点接受源节点发送的第一 PLMN ID，则目的节点向源节点发送回复消息，将目的节点确定的结果发送给源节点，该回复消息包括是否使用源节点选择的 PLMN ID 对应的路由域建立通信接口。

步骤 S203，目的节点接收源节点通过第一 PLMN ID 对应的路由域发送的通信接口建立请求消息。

具体地，目的节点若向源节点发送的回复消息表示接受源节点选择的 PLMN ID 建立通信接口，则源节点可以使用该 PLMN ID 对应的路由域建立通信接口，则目的节点可以接收到源节点通过该 PLMN ID 对应的路由域发送的通信接口建立请求消息。通信网路中，使用基于 IP 地址的路由域连接，每个运营商自己规划路由域中的 IP 地址，即每个 PLMN ID 对应一个路由域。网络中的每个通信节点均有自己的 IP 地址，但两个通信节点的 IP 地址处于同一个路由域中才能互相通信。共享通信节点中具有多重路由域，并且每个路由域对应一个 PLMN ID，因此，当共享通信节点之间或者共享通信节点和自有通信节点之间建立接口时，当选择了两个通信节点间相同的 PLMN ID，可以采用该 PLMN ID 对应的路由域，使用该路由域中的 IP 地址建立网络接口并实现通信。

本实施例，在通信节点间接口的建立过程中，通过选择源节点与目的节点的一个相同的 PLMN ID，并采用与该 PLMN ID 对应的路由域建立通信节点间接口，实现了在通信节点间建立网络连接时，选择正确的路由域建立接口的过程。

图 3 至图 6 所示实施例示出源节点选择 PLMN ID 的具体方法。

图 3 为本发明实施例提供的路由域选择方法实施例三的信令流程图，如图 3 所示，本实施例的方法包括:

步骤 S301，源 eNodeB 确定源 eNodeB 的主运营商 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 相同，选择源 eNodeB 的主运营商 PLMN ID。

具体地，源 eNodeB 和目的 eNodeB 建立 X2 接口时，源 eNodeB 首先判断邻站配置信息中目的 eNodeB 的主运营商 PLMN ID 和源 eNodeB 的主运营商 PLMN ID 是否相同，若相同，则选择源 eNodeB 的主运营商 PLMN ID。

步骤 S302，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括自组网（Self-Organized Network，SON）请求信息，Selected TAI 中包括源

eNodeB 的主运营商 PLMN ID。

具体地，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，请求与目的 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括源 eNodeB 的主运营商 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的源 eNodeB 主运营商 PLMN ID 对应的路由域的 IP 地址。

步骤 S303，目的 eNodeB 向源 eNodeB 发送自配置透传消息，其中包括 SON 回复信息，Selected TAI 中包括源 eNodeB 的主运营商 PLMN ID。

具体地，目的 eNodeB 接收到源 eNodeB 发送的自配置透传消息后，判断源 eNodeB 发送的自配置透传消息中 Selected TAI 信元包含的 PLMN ID 是否可用，若目的 eNodeB 可以使用 Selected TAI 信元中的源 eNodeB 主运营商 PLMN ID 建立接口，则也向源 eNodeB 发送自配置透传消息，同意使用源 eNodeB 选择的源 eNodeB 主运营商 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 回复信息，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括源 eNodeB 的主运营商 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为目的 eNodeB 预设的源 eNodeB 主运营商 PLMN ID 对应的路由域的 IP 地址。

步骤 S304，目的 eNodeB 和源 eNodeB 使用源 eNodeB 的主运营商 PLMN ID 对应的路由域进行通信。

具体地，源 eNodeB 和目的 eNodeB 进行自配置透传消息的交互后，确定了各自的 IP 地址，则可以使用该 IP 地址对应的路由域进行通信，此时源 eNodeB 和目的 eNodeB 之间的 X2 接口建立成功。

图 4 为本发明实施例提供的路由域选择方法实施例四的信令流程图，如图 4 所示，本实施例的方法包括:

步骤 S401，源 eNodeB 确定源 eNodeB 的主运营商 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 不同，并且目的 eNodeB 的主运营商 PLMN ID 与源节点的任一 PLMN ID 相同，选择目的 eNodeB 的主运营商 PLMN ID。

具体地，源 eNodeB 和目的 eNodeB 建立 X2 接口时，源 eNodeB 首先判断邻站配置信息中目的 eNodeB 的主运营商 PLMN ID 和源 eNodeB 的主运营商 PLMN ID 是否相同，若不同，则继续判断目的 eNodeB 的主运营商 PLMN ID 与源 eNodeB 中的其他 PLMN ID 是否相同，若源 eNodeB 的 PLMN

ID 存在与目的 eNodeB 的主运营商 PLMN ID 相同的 PLMN ID，则选择目的 eNodeB 的主运营商 PLMN ID。

步骤 S402，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，Selected TAI 中包括目的 eNodeB 的主运营商 PLMN ID。

具体地，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，请求与目的 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括目的 eNodeB 的主运营商 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的目的 eNodeB 主运营商 PLMN ID 对应的路由域的 IP 地址。

步骤 S403，目的 eNodeB 向源 eNodeB 发送自配置透传消息，其中包括 SON 回复信息，Selected TAI 中包括目的 eNodeB 的主运营商 PLMN ID。

具体地，目的 eNodeB 接收到源 eNodeB 发送的自配置透传消息后，判断源 eNodeB 发送的自配置透传消息中 Selected TAI 信元包含的 PLMN ID 是否可用，若目的 eNodeB 可以使用 Selected TAI 信元中的目的 eNodeB 主运营商 PLMN ID 建立接口，则也向源 eNodeB 发送自配置透传消息，同意使用源 eNodeB 选择的目的 eNodeB 主运营商 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 回复信息，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括目的 eNodeB 的主运营商 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为目的 eNodeB 预设的目的 eNodeB 主运营商 PLMN ID 对应的路由域的 IP 地址。

步骤 S404，目的 eNodeB 和源 eNodeB 使用目的 eNodeB 的主运营商 PLMN ID 对应的路由域进行通信。

具体地，源 eNodeB 和目的 eNodeB 进行自配置透传消息的交互后，确定了各自的 IP 地址，则可以使用该 IP 地址对应的路由域进行通信，此时源 eNodeB 和目的 eNodeB 之间的 X2 接口建立成功。

图 5 为本发明实施例提供的路由域选择方法实施例五的信令流程图，如图 5 所示，本实施例的方法包括:

步骤 S501，源 eNodeB 确定源 eNodeB 的主运营商 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 不同，并且目的 eNodeB 的主运营商 PLMN ID

与源节点的任一 PLMN ID 均不同，选择源 eNodeB 的 PLMN ID 与目的 eNodeB 的 PLMN ID 中任一相同的 PLMN ID。

具体地，源 eNodeB 和目的 eNodeB 建立 X2 接口时，源 eNodeB 首先判断邻站配置信息中目的 eNodeB 的主运营商 PLMN ID 和源 eNodeB 的主运营商 PLMN ID 是否相同，若不同，则继续判断目的 eNodeB 的主运营商 PLMN ID 与源 eNodeB 中的其他 PLMN ID 是否相同，若源 eNodeB 的 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 均不同，则选择源 eNodeB 的 PLMN ID 与目的 eNodeB 的 PLMN ID 中任一相同的 PLMN ID 作为已选 PLMN ID。

步骤 S502，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。

具体地，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，请求与目的 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括源 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S503，目的 eNodeB 向源 eNodeB 发送自配置透传消息，其中包括 SON 回复信息，Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。

具体地，目的 eNodeB 接收到源 eNodeB 发送的自配置透传消息后，判断源 eNodeB 发送的自配置透传消息中 Selected TAI 信元包含的 PLMN ID 是否可用，若目的 eNodeB 可以使用 Selected TAI 信元中的源 eNodeB 确定的已选 PLMN ID 建立接口，则也向源 eNodeB 发送自配置透传消息，同意使用源 eNodeB 确定的已选 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 回复信息，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括源 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为目的 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S504，目的 eNodeB 和源 eNodeB 使用源 eNodeB 确定的已选 PLMN ID 对应的路由域进行通信。

具体地，源 eNodeB 和目的 eNodeB 进行自配置透传消息的交互后，确定了各自的 IP 地址，则可以使用该 IP 地址对应的路由域进行通信，此时源 eNodeB 和目的 eNodeB 之间的 X2 接口建立成功。

图 6 为本发明实施例提供的路由域选择方法实施例六的信令流程图，如图 6 所示，本实施例的方法包括:

步骤 S601，源 eNodeB 确定源 eNodeB 的主运营商 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 不同，并且目的 eNodeB 的主运营商 PLMN ID 与源节点的任一 PLMN ID 均不同，选择源 eNodeB 的 PLMN ID 与目的 eNodeB 的 PLMN ID 中相同的 PLMN ID 中对应的源 eNodeB 和目的 eNodeB 之间路由长度最短的一个 PLMN ID。

具体地，源 eNodeB 和目的 eNodeB 建立 X2 接口时，源 eNodeB 首先判断邻站配置信息中目的 eNodeB 的主运营商 PLMN ID 和源 eNodeB 的主运营商 PLMN ID 是否相同，若不同，则继续判断目的 eNodeB 的主运营商 PLMN ID 与源 eNodeB 中的其他 PLMN ID 是否相同，若源 eNodeB 的 PLMN ID 与目的 eNodeB 的主运营商 PLMN ID 均不同，则继续判断源 eNodeB 的 PLMN ID 与目的 eNodeB 的 PLMN ID 中相同的 PLMN ID 对应的源 eNodeB 和目的 eNodeB 之间路由长度，也就是说判断使用相同的 PLMN ID 中的哪个 PLMN ID 对应的路由域在源 eNodeB 和目的 eNodeB 之间建立网络连接的路由长度最短，将该对应路由长度最短的 PLMN ID 作为已选 PLMN ID。

步骤 S602，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。

具体地，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，请求与目的 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括源 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S603，目的 eNodeB 向源 eNodeB 发送自配置透传消息，其中包括 SON 回复信息，Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。

具体地，目的 eNodeB 接收到源 eNodeB 发送的自配置透传消息后，判断源 eNodeB 发送的自配置透传消息中 Selected TAI 信元包含的 PLMN ID 是否可用，若目的 eNodeB 可以使用 Selected TAI 信元中的源 eNodeB 确定的已选 PLMN ID 建立接口，则也向源 eNodeB 发送自配置透传消息，同意使用源 eNodeB 确定的已选 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 回复信息，该自配置透传消息中源 eNodeB 和目的

eNodeB 的 Selected TAI 信元中都包括源 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为目的 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S604，目的 eNodeB 和源 eNodeB 使用源 eNodeB 确定的已选 PLMN ID 对应的路由域进行通信。

具体地，源 eNodeB 和目的 eNodeB 进行自配置透传消息的交互后，确定了各自的 IP 地址，则可以使用该 IP 地址对应的路由域进行通信，此时源 eNodeB 和目的 eNodeB 之间的 X2 接口建立成功。

上述路由域选择方法实施例二至实施例五中，源 eNodeB 通过判断目的 eNodeB 和源 eNodeB 的 PLMN ID，选择适合的 PLMN ID 对应的路由域建立源 eNodeB 和目的 eNodeB 之间的 X2 接口，实现了在源 eNdoeB 和目的 eNdoeB 之间建立网络连接时，选择正确的路由域建立接口的过程。其中，上述实施例五中，源 eNodeB 在具备判断源 eNdoeB 和目的 eNdoeB 之间路由长度的前提下，选择路由长度最短的路由域建立 X2 接口，节约了网络资源，为本发明的优选实施例。

图 7 为本发明实施例提供的路由域选择方法实施例七的信令流程图，如图 7 所示，本实施例的方法包括:

步骤 S701，源 eNodeB 选择源 eNodeB 的 PLMN ID 与目的 eNodeB 的 PLMN ID 中任一相同的 PLMN ID。

具体地，源 eNodeB 和目的 eNodeB 建立 X2 接口时，源 eNodeB 首先根据邻站配置信息中目的 eNodeB 的 PLMN ID，选择一个目的 eNodeB 与源 eNodeB 相同的 PLMN ID 作为已选 PLMN ID。源 eNodeB 确定已选 PLMN ID 的方法可以根据上述方法实施例三至实施例六的任一种方法。

步骤 S702，源 eNodeB 向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。

具体地，源 eNodeB 确定已选 PLMN ID 后，向目的 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，请求与目的 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 中包括源 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S703，目的 eNdoeB 重新确定已选 PLMN ID。

具体地，目的 eNodeB 接收到源 eNodeB 发送的自配置透传消息后，根据目的 eNdoeB 中的邻站配置信息重新判断目的 eNodeB 的 PLMN ID 与源 eNodeB 的 PLMN ID 中相同的 PLMN ID 对应的目的 eNodeB 和源 eNodeB 之间路由长度，也就是说判断使用相同的 PLMN ID 中的哪个 PLMN ID 对应的路由域在目的 eNodeB 和源 eNodeB 之间建立网络连接的路由长度最短，将该对应路由长度最短的 PLMN ID 重新作为已选 PLMN ID。

步骤 S704，目的 eNodeB 向源 eNodeB 发送自配置透传消息，其中包括 SON 请求信息，Selected TAI 中包括目的 eNodeB 确定的已选 PLMN ID。

具体地，目的 eNodeB 重新确定已选 PLMN ID 后，向源 eNodeB 发送自配置透传消息，通知源 eNodeB 使用目的 eNodeB 重新确定的已选 PLMN ID，并使用该已选 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 请求信息，请求与源 eNodeB 间建立自组网连接，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括目的 eNodeB 确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为目的 eNodeB 预设的已选 PLMN ID 对应的路由域的 IP 地址。

步骤 S705，源 eNodeB 再次向目的 eNodeB 发送自配置透传消息，其中包括 SON 回复信息，Selected TAI 中包括目的 eNodeB 确定的已选 PLMN ID。

具体地，源 eNdoeB 收到目的 eNodeB 发送的自配置透传消息后，判断目的 eNodeB 发送的自配置透传消息中 Selected TAI 信元包含的 PLMN ID 是否可用，若源 eNodeB 可以使用 Selected TAI 信元中的目的 eNodeB 重新确定的已选 PLMN ID 建立接口，则再次向源 eNodeB 发送自配置透传消息，同意使用目的 eNodeB 重新确定的已选 PLMN ID 对应的路由域建立网络接口，该自配置透传消息中包括 SON 回复信息，该自配置透传消息中源 eNodeB 和目的 eNodeB 的 Selected TAI 信元中都包括目的 eNodeB 重新确定的已选 PLMN ID。该自配置透传消息中的 X2 TNL Configuration Info 信元中包括为源 eNodeB 预设的目的 eNodeB 重新确定的已选 PLMN ID 对应的路由域的 IP 地址。若源 eNodeB 无法使用 Selected TAI 信元中的目的 eNodeB 重新确定的已选 PLMN ID 建立接口，则本次通信接口建立过程失败。

步骤 S706，目的 eNodeB 和源 eNodeB 使用目的 eNodeB 确定的已选

PLMN ID 对应的路由域进行通信。

具体地，源 eNodeB 和目的 eNodeB 进行自配置透传消息的交互后，确定了各自的 IP 地址，则可以使用该 IP 地址对应的路由域进行通信，此时源 eNodeB 和目的 eNodeB 之间的 X2 接口建立成功。

进一步地，步骤 S703 中，目的 eNodeB 重新确定已选 PLMN ID 时，可以不判断目的 eNodeB 的 PLMN ID 与源 eNodeB 的 PLMN ID 中相同的 PLMN ID 对应的目的 eNodeB 和源 eNodeB 之间路由长度，而是将目的 eNoedB 的 PLMN ID 与源 eNodeB 的 PLMN ID 中任一相同的 PLMN ID 重新作为已选 PLMN ID。但这样可能不能选择目的 eNodeB 与源 eNodeB 之间路由长度最短的路由域建立 X2 接口。

本实施例，当源 eNodeB 通过判断目的 eNodeB 和源 eNodeB 的 PLMN ID，选择适合的 PLMN ID 后，目的 eNodeB 继续对该 PLMN ID 对应的源 eNdoeB 和目的 eNdoeB 之间的路由长度进行判断，在目的 eNodeB 具备判断源 eNdoeB 和目的 eNdoeB 之间路由长度的前提下，实现了在源 eNdoeB 和目的 eNdoeB 之间建立网络连接时，选择正确的路由域建立接口的过程，并进一步地节约了网络资源，为本发明的优选实施例。

需要说明的是，上述各实施例中，源节点和目的节点之间互相传送自配置透传消息可以通过 MME 等核心网设备进行，本发明不限制自配置透传消息的发送路径，只要源节点和目的节点可以交互自配置透传消息即可。

图 8 为本发明实施例提供的通信节点实施例一的结构示意图，本实施例的通信节点为源节点，如图 8 所示，本实例的通信节点包括：

第一发送模块 81，用于将第一 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述通信节点与所述目的节点中相同的 PLMN ID。

第一接收模块 82，用于接收所述目的节点发送的回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID。

第二发送模块 83，用于当第一接收模块 82 接收到所述目的节点发送的回复消息时，通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送通信接口建立请求消息；当第一接收模块 82 接收到所述目的节点发送的第二 PLMN ID 时，则向所述目的节点发送回复消息。

第二接收模块 84，用于当第二发送模块 83 向所述目的节点发送回复消

息时，接收所述目的节点通过所述第二 PLMN ID 对应的路由域发送的通信接口建立请求消息。

本实施例提供的通信节点用于实现图 1 所示路由域选择方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

进一步地，图 8 所示通信节点中，若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 相同，则所述第一 PLMN ID 为所述源节点的主运营商 PLMN ID；若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 不同，并且所述目的节点的主运营商 PLMN ID 与所述源节点的任一 PLMN ID 相同，则所述第一 PLMN ID 为所述目的节点的主运营商 PLMN ID。

进一步地，所述第一 PLMN ID 为所述源节点和所述目的节点之间最短的路由长度对应的 PLMN ID。

进一步地，第一发送模块 81，具体用于通过自配置透传消息将所述第一 PLMN ID 发送给所述目的节点。

图 9 为本发明实施例提供的通信节点实施例二的结构示意图，本实施例的通信节点为目的节点，如图 9 所示，本实例的通信节点包括：

第一接收模块 91，用于接收源节点发送的第一 PLMN ID，所述第一 PLMN ID 为任意一个所述源节点与所述通信节点中相同的 PLMN ID。

第一发送模块 92，用于向所述源节点发送回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID。

第二接收模块 93，用于当第一发送模块 91 向所述源节点发送回复消息时，接收所述源节点通过所述第一 PLMN ID 对应的路由域发送的通信接口建立请求消息；当第一发送模块 91 向所述源节点发送第二 PLMN ID 时，接收所述源节点发送的回复消息。

第二发送模块 94，用于当第二接收模块 93 接收到所述源节点发送的回复消息时，通过所述第二 PLMN ID 对应的路由域，向所述源节点发送通信接口建立请求消息。

本实施例提供的通信节点用于实现图 2 所示路由域选择方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

进一步地，第一发送模块 92，具体用于通过自配置透传消息将所述第

二 PLMN ID 发送给所述源节点。

进一步地，所述第二 PLMN ID 为所述源节点和所述通信节点之间最短的路由域长度对应的 PLMN ID。

图 10 为本发明实施例提供的通信系统实施例一的结构示意图，如图 10 所示，本实例的通信系统包括:

源节点 111，包括图 8 所示通信节点实施例的通信节点，用于实现图 1 至图 7 所示路由域选择方法源节点侧的技术方案。

目的节点 112，，包括图 9 所示通信节点实施例的通信节点，用于实现图 2 至图 7 所示路由域选择方法目的节点侧的技术方案。

图 11 为本发明实施例提供的通信节点实施例五的硬件结构示意图，如图 11 所示，本实施例的通信节点为源节点，其中包括：处理器 121、存储器 122、接收器 123 和发送器 124，其中处理器 121、存储器 122、接收器 123 和发送器 124 通过系统总线相连。

处理器 121，用于执行图 1 至图 7 所示路由域选择方法实施例中源节点侧所进行的操作。

存储器 122，用于存储处理器 121 需要处理的数据并存储处理器 121 处理后的数据。

接收器 123，用于接收目的节点发送的数据。

发送器 124，用于向目的节点发送数据。

处理器 121，具体用于选择所述源节点与目的节点中一个相同的 PLMN ID；选择所述 PLMN ID 对应的路由域，以采用所述路由域建立所述源节点和所述目的节点之间的通信接口。

图 12 为本发明实施例提供的通信节点实施例六的硬件结构示意图，如图 12 所示，本实施例的通信节点为目的节点，其中包括：处理器 131、存储器 132、接收器 133 和发送器 134，其中处理器 131、存储器 132、接收器 133 和发送器 134 通过系统总线相连。

处理器 131，用于执行图 2 至图 7 所示路由域选择方法实施例中目的节点侧所进行的操作。

存储器 132，用于存储处理器 131 需要处理的数据并存储处理器 131 处理后的数据。

接收器 133，用于接收源节点发送的数据。

发送器 134，用于向源节点发送数据。

处理器 131，具体用于选择源节点与所述目的节点中一个相同的 PLMN ID；选择与所述目的节点选择的 PLMN ID 对应的路由域，以采用所述路由域建立所述源节点和所述目的节点之间的通信接口。

本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权利要求

1、一种路由域选择方法，其特征在于，包括:

源节点将第一通用陆地移动网络标识 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述源节点与所述目的节点中相同的 PLMN ID;

若所述目的节点接受所述第一 PLMN ID，则

所述源节点接收所述目的节点发送的回复消息;

所述源节点通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送通信接口建立请求消息。

2、根据权利要求 1 所述的方法，其特征在于，还包括:

若所述目的节点不接受所述第一 PLMN ID，则

所述源节点接收所述目的节点发送的第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

所述源节点向所述目的节点发送回复消息;

所述源节点接收所述目的节点通过所述第二PLMN ID对应的路由域发送的通信接口建立请求消息。

3、根据权利要求 1 所述的方法，其特征在于，若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 相同，则所述第一 PLMN ID 为所述源节点的主运营商 PLMN ID;

若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 不同，并且所述目的节点的主运营商 PLMN ID 与所述源节点的任一 PLMN ID 相同，则所述第一 PLMN ID 为所述目的节点的主运营商 PLMN ID。

4、根据权利要求 1 所述的方法，其特征在于，所述第一 PLMN ID 为所述源节点和所述目的节点之间最短的路由长度对应的 PLMN ID。

5、根据权利要求 1~4 任一项所述的方法，其特征在于，所述源节点将第一 PLMN ID 发送给目的节点包括:

所述源节点通过自配置透传消息将所述第一PLMN ID发送给所述目的节点。

6、一种路由域选择方法，其特征在于，包括:

目的节点接收源节点发送的第一通用陆地移动网络标识 PLMN ID，所述第一 PLMN ID 为任意一个所述源节点与所述目的节点中相同的 PLMN ID;

若所述目的节点接受所述第一 PLMN ID，则

所述目的节点向所述源节点发送回复消息;

所述目的节点接收所述源节点通过所述第一PLMN ID对应的路由域发送的通信接口建立请求消息。

7、根据权利要求 6 所述的方法，其特征在于，还包括:

若所述目的节点不接受所述第一 PLMN ID，则

所述目的节点将第二 PLMN ID 发送给所述源节点，所述第二 PLMN ID 为除所述第一PLMN ID以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

所述目的节点接收所述源节点发送的回复消息;

所述目的节点通过所述第二 PLMN ID 对应的路由域，向所述源节点发送通信接口建立请求消息。

8、根据权利要求 7 所述的方法，其特征在于，所述目的节点将第二 PLMN ID 发送给所述源节点，包括:

所述目的节点通过自配置透传消息将所述第二PLMN ID发送给所述源节点。

9、根据权利要求 7 所述的方法，其特征在于，

所述第二PLMN ID为所述源节点和所述目的节点之间最短的路由域长度对应的 PLMN ID。

10、一种通信节点，其特征在于，包括:

第一发送模块，用于将第一通用陆地移动网络标识 PLMN ID 发送给目的节点，所述第一 PLMN ID 为任意一个所述通信节点与所述目的节点中相同的 PLMN ID;

第一接收模块，用于接收所述目的节点发送的回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID;

第二发送模块，用于当所述第一接收模块接收到所述目的节点发送的回复消息时，通过所述第一 PLMN ID 对应的路由域，向所述目的节点发送

通信接口建立请求消息；当所述第一接收模块接收到所述目的节点发送的第二 PLMN ID 时，则向所述目的节点发送回复消息；

第二接收模块，用于当所述第二发送模块向所述目的节点发送回复消息时，接收所述目的节点通过所述第二 PLMN ID 对应的路由域发送的通信接口建立请求消息。

11、根据权利要求 10 所述的通信节点，其特征在于，若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 相同，则所述第一 PLMN ID 为所述源节点的主运营商 PLMN ID；

若所述源节点的主运营商 PLMN ID 与所述目的节点的主运营商 PLMN ID 不同，并且所述目的节点的主运营商 PLMN ID 与所述源节点的任一 PLMN ID 相同，则所述第一 PLMN ID 为所述目的节点的主运营商 PLMN ID。

12、根据权利要求 10 所述的通信节点，其特征在于，所述第一 PLMN ID 为所述源节点和所述目的节点之间最短的路由长度对应的 PLMN ID。

13、根据权利要求 10～12 任一项所述的通信节点，其特征在于，所述第一发送模块，具体用于通过自配置透传消息将所述第一 PLMN ID 发送给所述目的节点。

14、一种通信节点，其特征在于，包括：

第一接收模块，用于接收源节点发送的第一通用陆地移动网络标识 PLMN ID，所述第一 PLMN ID 为任意一个所述源节点与所述通信节点中相同的 PLMN ID；

第一发送模块，用于向所述源节点发送回复消息或第二 PLMN ID，所述第二 PLMN ID 为除所述第一 PLMN ID 以外任意一个所述源节点与所述目的节点中相同的 PLMN ID；

第二接收模块，用于当所述第一发送模块向所述源节点发送回复消息时，接收所述源节点通过所述第一 PLMN ID 对应的路由域发送的通信接口建立请求消息；当所述第一发送模块向所述源节点发送第二 PLMN ID 时，接收所述源节点发送的回复消息；

第二发送模块，用于当所述第二接收模块接收到所述源节点发送的回复消息时，通过所述第二 PLMN ID 对应的路由域，向所述源节点发送通信接口建立请求消息。

15、根据权利要求 14 所述的通信节点，其特征在于，所述第一发送模块，具体用于通过自配置透传消息将所述第二 PLMN ID 发送给所述源节点。

16、根据权利要求 14 所述的通信节点，其特征在于，所述第二 PLMN ID 为所述源节点和所述通信节点之间最短的路由域长度对应的 PLMN ID。

17、一种通信系统，其特征在于，包括：源节点和目的节点；

所述源节点为如权利要求 10～13 任一项所述的通信节点；

所述目的节点为如权利要求 14～16 任一项所述的通信节点。

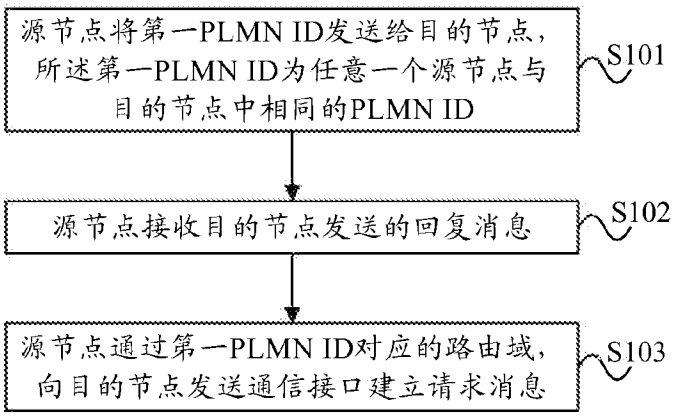

源节点将第一PLMN ID发送给目的节点，所述第一PLMN ID为任意一个源节点与目的节点中相同的PLMN ID
S101
源节点接收目的节点发送的回复消息
S102
源节点通过第一PLMN ID对应的路由域，向目的节点发送通信接口建立请求消息
S103

图 1

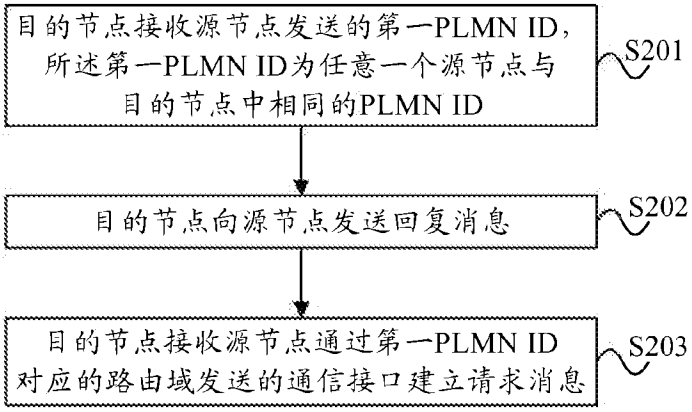

目的节点接收源节点发送的第一PLMN ID，所述第一PLMN ID为任意一个源节点与目的节点中相同的PLMN ID
S201
目的节点向源节点发送回复消息
S202
目的节点接收源节点通过第一PLMN ID对应的路由域发送的通信接口建立请求消息
S203

图2

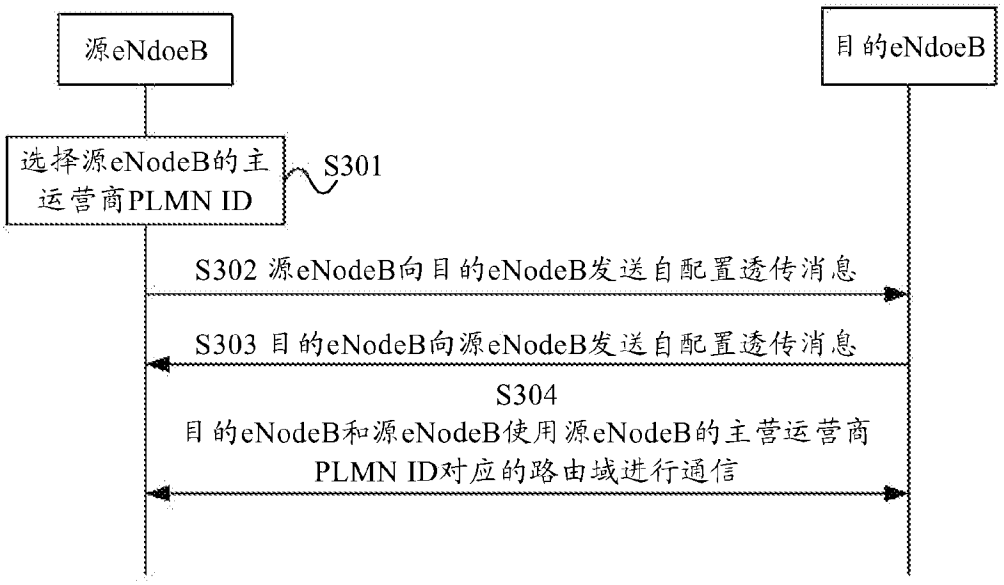

源eNdoeB
目的eNdoeB
选择源eNodeB的主运营商PLMN ID
S301
S302 源eNodeB向目的eNodeB发送自配置透传消息
S303 目的eNodeB向源eNodeB发送自配置透传消息
S304
目的eNodeB和源eNodeB使用源eNodeB的主营运营商PLMN ID对应的路由域进行通信

图3

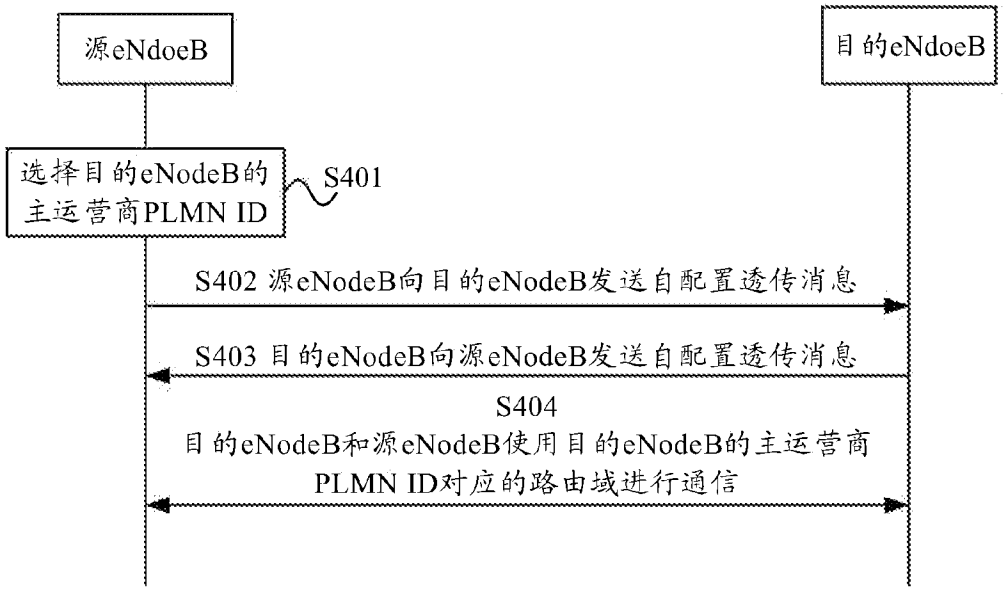

源eNdoeB
目的eNdoeB
选择目的eNodeB的主运营商PLMN ID
S401
S402 源eNodeB向目的eNodeB发送自配置透传消息
S403 目的eNodeB向源eNodeB发送自配置透传消息
S404
目的eNodeB和源eNodeB使用目的eNodeB的主运营商PLMN ID对应的路由域进行通信

图 4

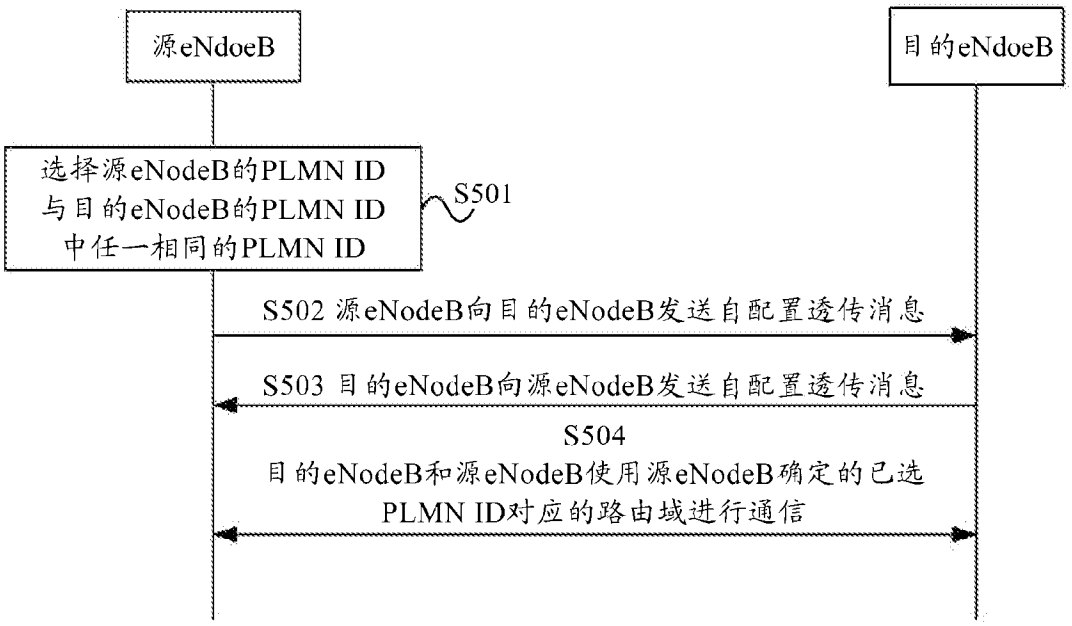

源eNdoeB
目的eNdoeB
选择源eNodeB的PLMN ID
与目的eNodeB的PLMN ID
中任一相同的PLMN ID
S501
S502 源eNodeB向目的eNodeB发送自配置透传消息
S503 目的eNodeB向源eNodeB发送自配置透传消息
S504
目的eNodeB和源eNodeB使用源eNodeB确定的已选
PLMN ID对应的路由域进行通信

图5

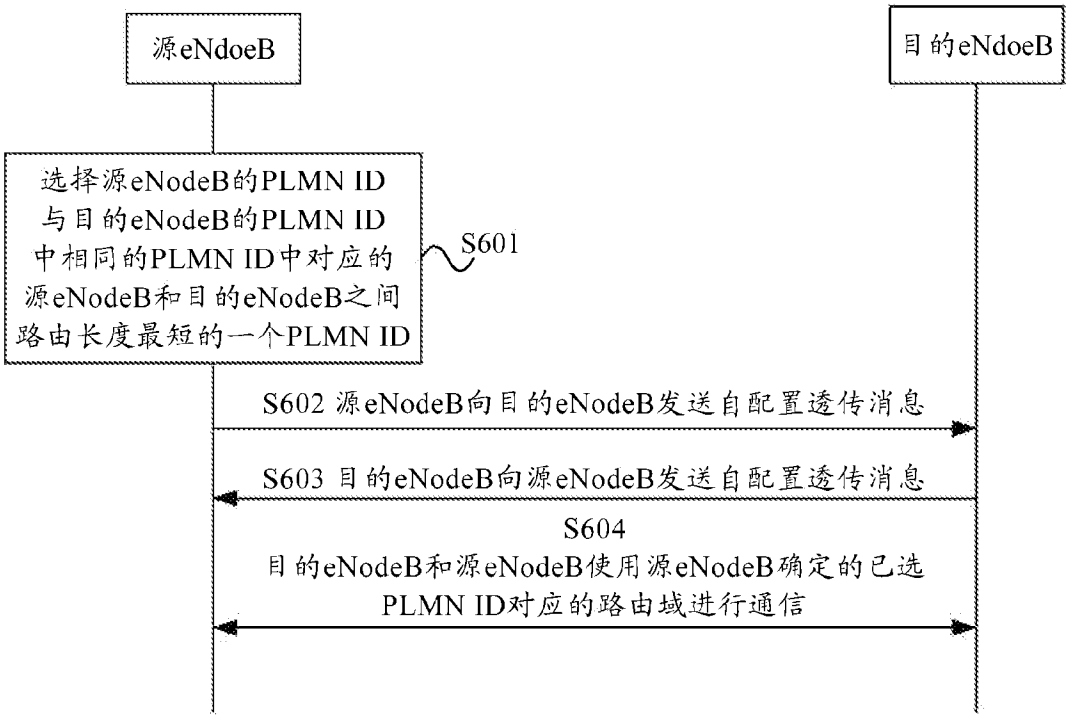

源eNdoeB
目的eNdoeB
选择源eNodeB的PLMN ID
与目的eNodeB的PLMN ID
中相同的PLMN ID中对应的
源eNodeB和目的eNodeB之间
路由长度最短的一个PLMN ID
S601
S602 源eNodeB向目的eNodeB发送自配置透传消息
S603 目的eNodeB向源eNodeB发送自配置透传消息
S604
目的eNodeB和源eNodeB使用源eNodeB确定的已选
PLMN ID对应的路由域进行通信

图 6

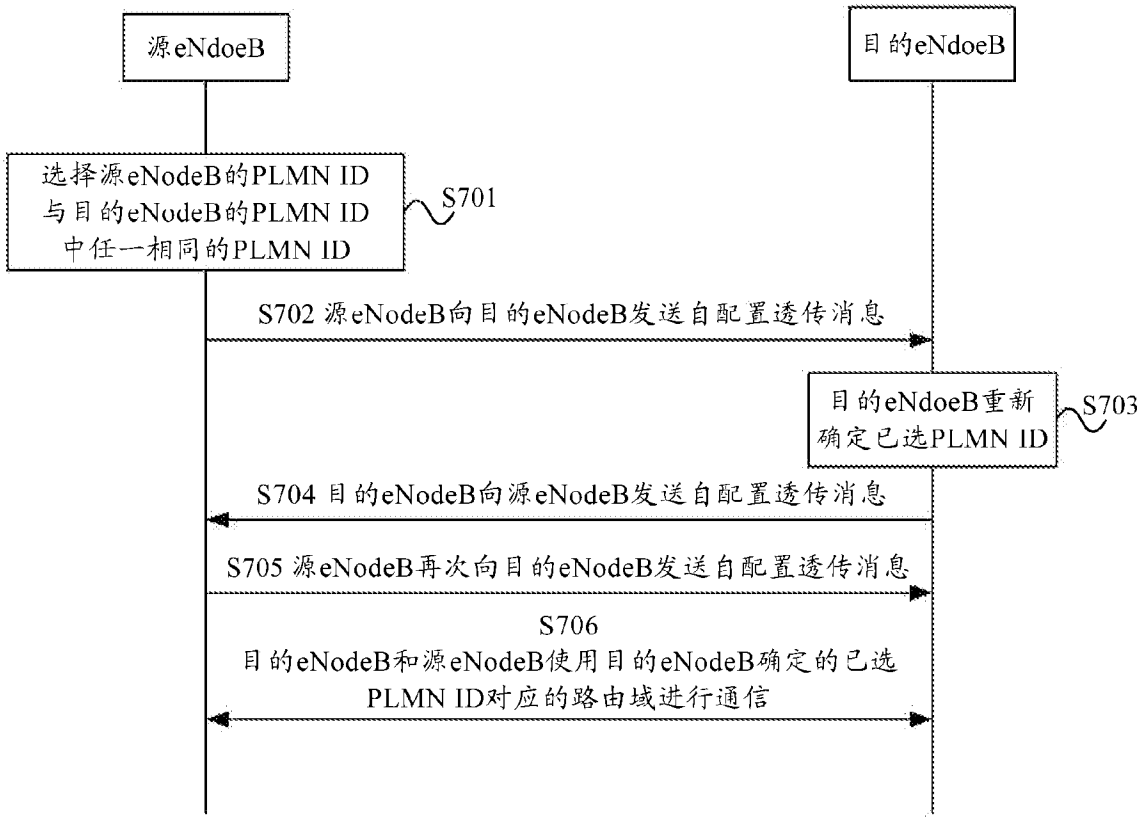

源eNdoeB
目的eNdoeB
选择源eNodeB的PLMN ID
与目的eNodeB的PLMN ID
中任一相同的PLMN ID
S701
S702 源eNodeB向目的eNodeB发送自配置透传消息
目的eNdoeB重新
确定已选PLMN ID
S703
S704 目的eNodeB向源eNodeB发送自配置透传消息
S705 源eNodeB再次向目的eNodeB发送自配置透传消息
S706
目的eNodeB和源eNodeB使用目的eNodeB确定的已选
PLMN ID对应的路由域进行通信

图7

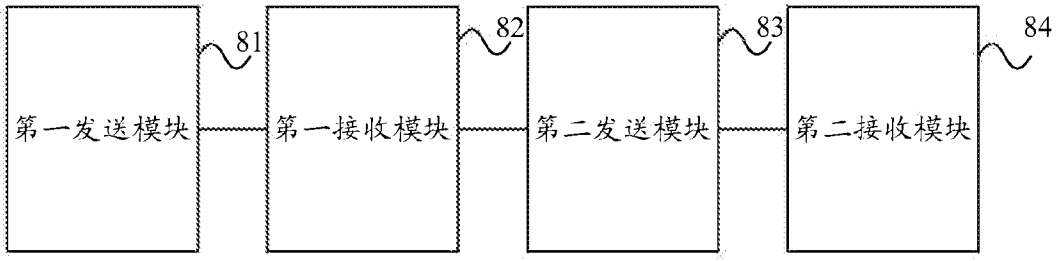

81
82
83
84
第一发送模块
第一接收模块
第二发送模块
第二接收模块

图 8

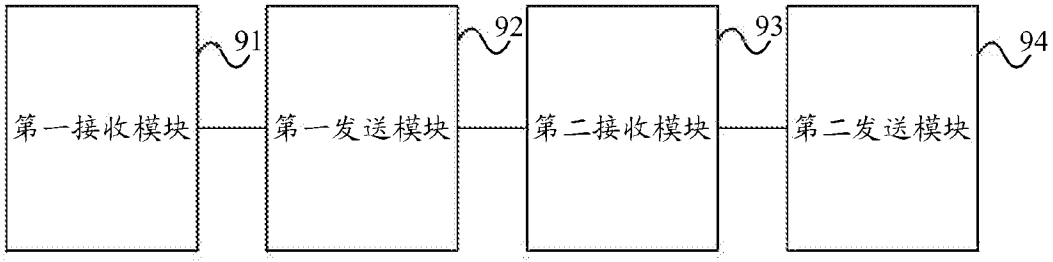


图 9

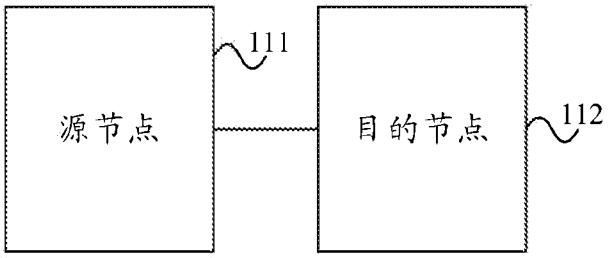


图 10

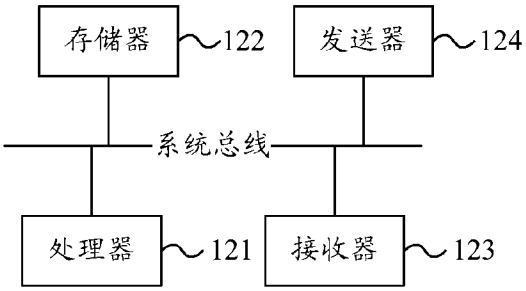


图 11

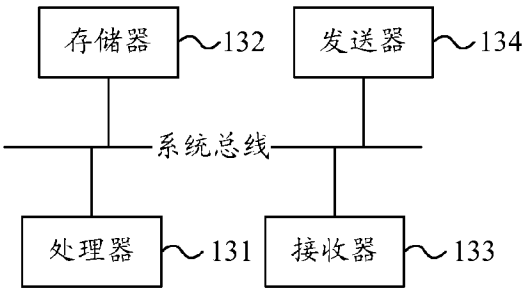


图12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/089785

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04Q; H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, USTXT, WOTXT, EPTXT, DWPI, VEN, 3GPP: plmn; son; ad hoc network; self-organi+; self; organi+; selforgani+; sharing; share?; share; ????NB?; ??node???; enb; enodeb; operator?; operater?; source; target; destination; "plmn-id"; "plmn_id"; id?; ident+; "plmn id"; identifier; send+; sent; transmit+; deliver+; transfer+; same; common; equal+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2010078676 A1 (ZTE CORP.), 15 July 2010 (15.07.2010), description, page 4, line 25 to page 5, line 20, and figures 1 and 2	1, 3-6
A		2, 7-17
Y	3GPP TSG SA, 3GPP TS 23.251 V11.4.0, Network Sharing, Architecture and functional description (Release 11) [online], 18 December 2012 (18.12.2012), section 5.2a, Retrieved from the Internet: <http://www.3 gpp.org/ftp/Specs/archive/23_series/23.251/>	1, 3-6
A		2, 7-17
A	HUAWEI TECHNOLOGIES CO., LTD.; 3GPP TSG RAN WG3 Meeting #62, R3-083132, Addition of Selected PLMN Identity in Relocation Procedure [online], 05 November 2008 (05.11.2008), the whole document, Retrieved from the Internet: <http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_62/docs/>	1-17
A	ZTE CORP.; 3GPP TSG-RAN WG3 #73bis, R3-112540, Consideration on RAN sharing for HeNB [online], 19 October 2011 (19.10.2011), the whole document, Retrieved from the Internet: <http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_73bis/Docs/>	1-17

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 March 2014 (10.03.2014)	**27 March 2014 (27.03.2014)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **YANG, Haiyang** Telephone No.: (86-10) **62411342**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/089785

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102098742 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 15 June 2011 (15.06.2011), the whole document	1-17
A	WO 2008051458 A1 (INTERDIGITAL PATENT HOLDINGS, INC.), 02 May 2008 (02.05.2008), the whole document	1-17
A	WO 2010026438 A1 (TELEFON AB L.M. ERICSSON), 11 March 2010 (11.03.2010), the whole document	1-17

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/089785

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2010078676 A1	15.07.2010	CN 102172057 A	31.08.2011
		RU 2495540 C2	10.10.2013
		US 2011269471 A1	03.11.2011
		EP 2384033 A1	02.11.2011
		IN 201105384 P1	28.09.2012
		US 8374612 B2	12.02.2013
		RU 2011130221 A	10.02.2013
CN 102098742 A	15.06.2011	CN 102098742 B	10.07.2013
WO 2008051458 A2	02.05.2008	TW 200829044 A	01.07.2008
		WO 2008051458 A3	07.08.2008
		US 2008098467 A1	24.04.2008
WO 2010026438 A1	11.03.2010	US 2011263282 A1	27.10.2011
		US 8630648 B2	14.01.2014
		EP 2345277 A1	20.07.2011
		CN 102239719 A	09.11.2011

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/089785

CONTINUATION: A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/721 (2013.01) i

H04L 12/733 (2013.01) i

国际检索报告

国际申请号
PCT/CN2013/089785

A. 主题的分类

见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)
IPC：H04Q；H04W；H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)
CNABS，CNTXT，USTXT，WOTXT，EPTXT，DWPI，VEN，3GPP：plmn；son；自组网；self-organi+；self；organi+；selforgani+；sharing；share?；share；????NB?；??node???；enb；enodeb；operator?；operater?；原；源；目标；目的；"plmn-id"；"plmn_id"；id?；ident+；"plmn id"；标识；相同；同样；同 ；相等； 样；共同；send+；sent；transmit+；deliver+；transfer+；same；common；equal+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	WO2010078676 A1 (中兴通讯股份有限公司) 15. 7 月 2010(15.07.2010) 说明书第 4 页第 25 行至第 5 页第 20 行，说明书附图 1，2	1,3-6
A		2, 7-17
Y	3GPP TSG SA；3GPP TS 23.251 V11.4.0，Network Sharing; Architecture and functional description(Release 11) [online]，18. 12 月 2012(18.12.2012) 第 5.2a 节，；Retrieved from the Internet： < http://www.3gpp.org/ftp/Specs/archive/23_series/23.251/ >	1,3-6
A		2, 7-17
A	华为技术有限公司；3GPP TSG RAN WG3 Meeting #62，R3-083132，Addition of Selected PLMN Identity in Relocation Procedure [online]，05. 11 月 2008(05.11.2008)，全文， Retrieved from the Internet： < http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_62/docs/ >	1-17
A	中兴通讯股份有限公司；3GPP TSG-RAN WG3 #73bis，R3-112540，Consideration on RAN sharing for HeNB [online]，19. 10 月 2011(19.10.2011)，全文， Retrieved from the Internet： < http://www.3gpp.org/ftp/tsg_ran/WG3_Iu/TSGR3_73bis/Docs/ >	1-17

☒ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：
"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
10. 3 月 2014(10.03.2014)	**27.3 月 2014 (27.03.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 杨海洋 电话号码：(86-10) **62411342**

C(续). 相关文件

类 型	引用文件，必要时，指明相关段落	相关的权利要求
A	CN102098742A(大唐移动通信设备有限公司) 15. 6 月 2011(15.06.2011) 全文	1-17
A	WO2008051458 A2(交互数字专利控股公司) 02. 5 月 2008(02.05.2008) 全文	1-17
A	WO2010026438 A1(爱立信电话股份有限公司) 11. 03 月 2010(11.03.2010) 全文	1-17

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/089785

检索报告中引用的专利文件	公布日期	同族专利	公布日期
WO2010078676 A1	15.07.2010	CN102172057 A	31.08.2011
		RU2495540 C2	10.10.2013
		US2011269471 A1	03.11.2011
		EP2384033 A1	02.11.2011
		IN201105384P1	28.09.2012
		US8374612 B2	12.02.2013
		RU2011130221 A	10.02.2013
CN102098742A	15.06.2011	CN102098742B	10.07.2013
WO2008051458 A2	02.05.2008	TW200829044 A	01.07.2008
		WO2008051458 A3	07.08.2008
		US2008098467 A1	24.04.2008
WO2010026438 A1	11.03.2010	US2011263282 A1	27.10.2011
		US8630648 B2	14.01.2014
		EP2345277 A1	20.07.2011
		CN102239719 A	09.11.2011

续：A.主题的分类
H04L 12/721(2013.01) i
H04L 12/733(2013.01) i

Espacenet

Bibliographic data: WO2014166258 (A1) — 2014-10-16

METHOD AND DEVICE FOR DISPLAYING SUBSCRIBER IDENTITY MODULE CARD CONTACTS

Inventor(s): ZHOU YONG [CN] + (ZHOU, YONG)

Applicant(s): ZTE CORP [CN] + (ZTE CORPORATION)

Classification: **- international:** ***H04M1/275;*** *H04M1/725*
- cooperative: **H04M1/274533**

Application number: WO2013CN87426 20131119

Priority number(s): CN20131120657 20130409

Also published as: CN104104781 (A)

Abstract of WO2014166258 (A1)

Disclosed are a method and device for displaying subscriber identity module card contacts, comprising: subscriber identity module card contact information is read; the names of all of the contacts in the subscriber identity module card contact information are compared; for contacts of identical names, a scheme in which multiple numbers correspond to the name of one contact is employed for display; and, for contacts of different names, a scheme in which one number corresponds to the name of one contact is employed for display. With the present invention, telephone numbers of contacts of identical names are set to correspond to one name, a user only needs to operate once to lookup all of the telephone numbers, thus enhancing user experience.

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 10 月 16 日 (16.10.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/166258 A1

(51) 国际专利分类号:
H04M 1/275 (2006.01) *H04M 1/725* (2006.01)

(21) 国际申请号: PCT/CN2013/087426

(22) 国际申请日: 2013 年 11 月 19 日 (19.11.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310120657.7 2013 年 4 月 9 日 (09.04.2013) CN

(71) 申请人: **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: **周涌 (ZHOU, Yong)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: **北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P.C.)**; 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: METHOD AND DEVICE FOR DISPLAYING SUBSCRIBER IDENTITY MODULE CARD CONTACTS

(54) **发明名称**: 一种显示用户身份识别卡联系人的方法及装置

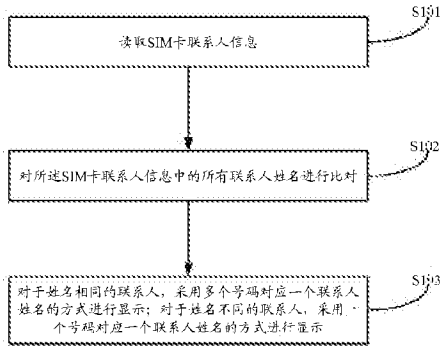


图 2 / Fig. 2

S101 READING OF THE SIM CARD CONTACT INFORMATION
S102 COMPARISON OF ALL OF THE NAMES OF THE CONTACTS IN THE SIM CARD CONTACT INFORMATION
S103 FOR THE CONTACTS OF IDENTICAL NAMES, EMPLOYMENT OF THE SCHEME IN WHICH MULTIPLE NUMBERS CORRESPOND TO THE NAME OF ONE CONTACT FOR DISPLAY; AND, FOR THE CONTACTS OF DIFFERENT NAMES, EMPLOYMENT OF THE SCHEME IN WHICH ONE NUMBER CORRESPONDS TO THE NAME OF ONE CONTACT FOR DISPLAY

(57) **Abstract**: Disclosed are a method and device for displaying subscriber identity module card contacts, comprising: subscriber identity module card contact information is read; the names of all of the contacts in the subscriber identity module card contact information are compared; for contacts of identical names, a scheme in which multiple numbers correspond to the name of one contact is employed for display; and, for contacts of different names, a scheme in which one number corresponds to the name of one contact is employed for display. With the present invention, telephone numbers of contacts of identical names are set to correspond to one name, a user only needs to operate once to lookup all of the telephone numbers, thus enhancing user experience.

(57) **摘要**: 本发明公开了一种显示用户身份识别卡联系人的方法及装置，包括：读取用户身份识别卡联系人信息；对所述用户身份识别卡联系人信息中的所有联系人姓名进行比对；对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。本发明通过将同名联系人的电话号码与一个姓名进行对应，用户只需要操作一次就可以查阅所有电话号码，提高了用户体验。

WO 2014/166258 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种显示用户身份识别卡联系人的方法及装置

技术领域

本发明涉及移动通讯技术领域，特别是涉及一种显示用户身份识别卡联系人的方法及装置。

背景技术

移动终端，例如手机上的联系人记录包括用户身份识别卡内存储和手机内存储的两部分。随着通信技术的发展，手机中的用户身份识别卡能够存储的电话号码越来越多，但是为了保持兼容，用户身份识别卡的国际规范一直限定其只能存储联系人的“姓名”和“号码”两个信息，无法像手机内存储的联系人，可以一个姓名对应多个电话号码。由于用户身份识别卡存储规范的这种限制，目前手机在读取用户身份识别卡中的联系人后，都是采用一一映射的直接显示方式。如图 1 所示（假设 SIM 卡中存储了 N 个联系人信息，N>2），从图 1 可知，如果 SIM 卡上存在多个同名的联系人，以张三（号码 1）、张三（号码 2）为例，那么在手机界面上将显示两条单独的菜单项——张三，用户需要点击不同的菜单项才能看到具体对应的号码 1、号码 2，更多号码以此类推。可见，如果用户身份识别卡上某个联系人有多条记录，那么用户将点击多次才能完全查看所有的信息。

发明内容

本发明要解决的技术问题是提供一种显示用户身份识别卡联系人的方法及装置，用以解决现有技术中用户需要点击多次才能查看同名联系人的多个号码的问题。

为解决上述技术问题，一方面，本发明实施例提供一种显示用户身份识别卡联系人的方法，包括：

读取用户身份识别卡联系人信息；

对所述用户身份识别卡联系人信息中的所有联系人姓名进行比对；

对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

优选地，在对所有联系人姓名进行比对之前，还包括：

判断是否进行同名合并显示操作；如果是，则对所有联系人姓名进行比对；如果否，则采用一个号码对应一个联系人姓名的方式进行显示。

优选地，采用多个号码对应一个联系人姓名的方式进行显示，具体包括：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示。

优选地，在采用多个号码对应一个联系人姓名的方式进行显示之后，还包括：

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

优选地，对号码添加区别辅助信息，以区别对应同一姓名的不同号码。

另一方面，本发明实施例还提供一种显示用户身份识别卡联系人的装置，包括：

读取单元，设置为读取用户身份识别卡联系人信息；

比对单元，设置为对所述用户身份识别卡联系人信息中的所有联系人姓名进行比对；

显示单元，设置为对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

优选地，所述装置还包括：

同名合并显示单元，设置为判断是否进行同名合并显示操作；如果是，则由所述比对单元对所有联系人姓名进行比对；如果否，则由显示单元采用一个号码对应一个联系人姓名的方式进行显示。

优选地，所述显示单元具体设置为：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示。

优选地，所述显示单元具体设置为：

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

优选地，所述装置还包括：

区别辅助信息添加单元，设置为对号码添加区别辅助信息，以区别对应同一姓名的不同号码。

本发明实施例通过将同名联系人的电话号码与一个姓名进行对应，用户只需要操作一次就可以查阅所有电话号码，提高了用户体验。

附图说明

图 1 是现有技术中手机 SIM 卡通讯录的显示原理图；

图 2 是本发明实施例中一种显示手机 SIM 卡联系人的方法的流程图；

图 3 是本发明实施例中手机 SIM 卡通讯录的显示原理图；

图 4 是本发明实施例中一种显示手机 SIM 卡联系人的装置的结构示意图。

具体实施方式

以下结合附图以及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不限定本发明。

本发明实施例的目的是提供一种不改变 SIM 卡联系人存储内容，仅改变存储内容和手机显示界面之间映射关系进行显示的方法和装置；即将原来一一对应的映射关系，通过对比联系人姓名，当发现多条号码对应的联系人姓名相同时，自动将原来的一一映射关系改为一个姓名对应多个号码的映射关系，使得用户只需要一次操作就可以查看 SIM 卡上同名记录下的多个电话号码。

如图 2、3 所示，本发明实施例涉及一种显示手机 SIM 卡联系人的方法，包括：

步骤 S101，读取 SIM 卡联系人信息；

步骤 S102，对所述 SIM 卡联系人信息中的所有联系人姓名进行比对；

本步骤中，进行比对，主要判断是否存在同名的联系人。

步骤 S103，对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

本步骤中，同名的联系人在界面上只显示一条姓名记录，并将其所有对应的电话号码显示在对应的号码页面下。如果有多个同名联系人的情况，都同理进行处理。

另外，由于有些用户习惯多人重名情况下，将多条记录单独分开显示，为了解决以上问题，本发明实施例的方法还包括如下步骤：

优选地，在步骤 S102 之前，还包括：

判断是否进行同名合并显示操作；如果是，则对所有联系人姓名进行比对；如果否，则采用一个号码对应一个联系人姓名的方式进行显示。

在一个优选实施例中，步骤 S103 中，采用多个号码对应一个联系人姓名的方式进行显示，可以包括：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示。

优选地，步骤 S103 中，在采用多个号码对应一个联系人姓名的方式进行显示之后，还包括：

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

另外，对于同名联系人对应的号码，在界面上添加区别辅助信息，例如标示出手机号码归属地等信息，供用户区别时参考；用户也可以号码旁添加其它相关的辅助信息，以帮助区分。

如果手机 SIM 卡上有多个姓名和号码都相同的记录，那么这种情况下，可以只显示一条记录，也可以显示多条记录，提示用户存在完全相同的号码记录，用户可以手动删除，以节省 SIM 卡存储空间。

本方法可以仅限于 SIM 卡联系人的显示，也可以扩展到将 SIM 卡、手机内存的联系人显示完全统一，给用户更好的体验。

如图 4 所示，本发明实施例还涉及一种实现上述方法的显示手机 SIM 卡联系人的装置，包括：

读取单元 201，设置为读取 SIM 卡联系人信息；

比对单元 202，设置为对所述 SIM 卡联系人信息中的所有联系人姓名进行比对；

显示单元 203，设置为对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

另外，为达更加技术效果，本发明实施例装置还包括：

同名合并显示单元，设置为判断是否进行同名合并显示操作；如果是，则由所述比对单元 202 对所有联系人姓名进行比对；如果否，则由显示单元 203 采用一个号码对应一个联系人姓名的方式进行显示。

区别辅助信息添加单元，设置为对号码添加区别辅助信息，以区别对应同一姓名的不同号码。

显示单元 203 具体设置为：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示；

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

由上述实施例可以看出，本发明实施例通过将同名联系人的电话号码与一个姓名进行对应，用户只需要操作一次就可以查阅所有电话号码，提高了用户体验。

尽管为示例目的，已经公开了本发明的优选实施例，本领域的技术人员将意识到各种改进、增加和取代也是可能的，因此，本发明的范围应当不限于上述实施例。

工业实用性：

本发明涉及移动通讯技术领域，提供一种显示手机 SIM 卡联系人的方法及装置，解决了现有技术中用户需要点击多次才能查看同名联系人的多个号码的问题，通过将同名联系人的电话号码与一个姓名进行对应，用户只需要操作一次就可以查阅所有电话号码，提高了用户体验。

权 利 要 求 书

1、 一种显示用户身份识别卡联系人的方法，包括：

读取用户身份识别卡联系人信息；

对所述用户身份识别卡联系人信息中的所有联系人姓名进行比对；

对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

2、 根据权利要求 1 所述的方法，其中，在对所有联系人姓名进行比对之前，还包括：

判断是否进行同名合并显示操作；如果是，则对所有联系人姓名进行比对；如果否，则采用一个号码对应一个联系人姓名的方式进行显示。

3、 根据权利要求 1 或 2 所述的方法，其中，采用多个号码对应一个联系人姓名的方式进行显示，具体包括：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示。

4、 根据权利要求 1 或 3 所述的方法，其中，在采用多个号码对应一个联系人姓名的方式进行显示之后，还包括：

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

5、 根据权利要求 4 所述的方法，其中，

对号码添加区别辅助信息，以区别对应同一姓名的不同号码。

6、 根据权利要求 1 至 5 任一项所述的方法，其中，所述用户身份识别卡包括：SIM 卡或 USIM 卡。

7、 一种显示用户身份识别卡联系人的装置，包括：

读取单元，设置为读取用户身份识别卡联系人信息；

比对单元，设置为对所述用户身份识别卡联系人信息中的所有联系人姓名进行比对；

显示单元，设置为对于姓名相同的联系人，采用多个号码对应一个联系人姓名的方式进行显示；对于姓名不同的联系人，采用一个号码对应一个联系人姓名的方式进行显示。

8、 根据权利要求 7 所述的装置，其中，所述装置还包括：

同名合并显示单元，设置为判断是否进行同名合并显示操作；如果是，则由所述比对单元对所有联系人姓名进行比对；如果否，则由显示单元采用一个号码对应一个联系人姓名的方式进行显示。

9、 根据权利要求 7 或 8 所述的装置，其中，所述显示单元具体设置为：

当进行全部同名合并显示时，则将该姓名对应的所有号码显示在该姓名对应的号码页面内；

当进行部分同名合并显示时，则将用户选定的一个或多个号码显示在该姓名对应的号码页面内，与该姓名相同的剩余联系人，按照一个号码对应一个联系人姓名的方式进行显示。

10、 根据权利要求 7 或 9 所述的装置，其中，所述显示单元具体设置为：

当进行全部同名分离显示操作时，则采用一个号码对应一个联系人姓名的方式进行显示；

如果是部分同名分离显示，则针对多个号码对应同一姓名联系人的情况，将用户选定的一个或多个号码采用一个号码对应一个联系人姓名的方式进行显示，剩余的同名联系人采用多个号码对应一个联系人姓名的方式进行显示。

11、 根据权利要求 10 所述的装置，其中，所述装置还包括：

区别辅助信息添加单元，设置为对号码添加区别辅助信息，以区别对应同姓名的不同号码。

12、 根据权利要求 7 至 11 任一项所述的装置，其中，所述用户身份识别卡包括：SIM 卡或 USIM 卡。

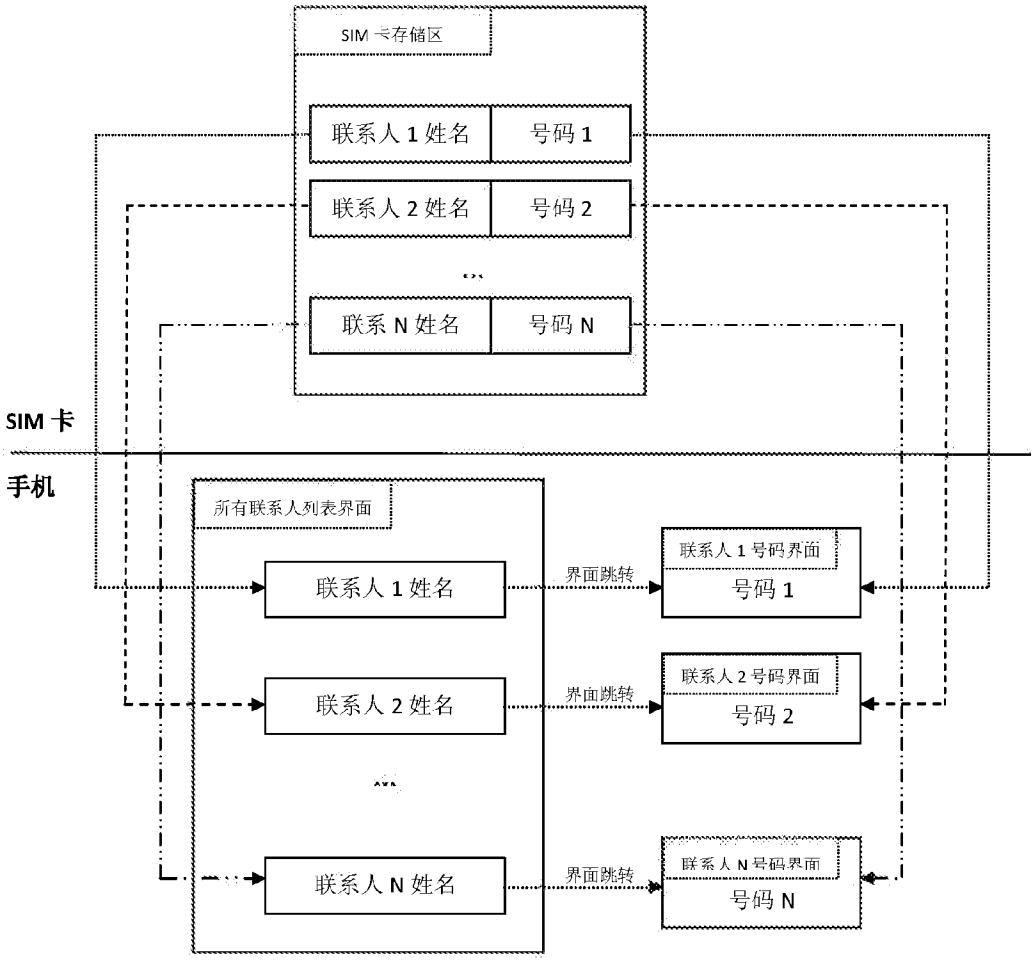


图 1

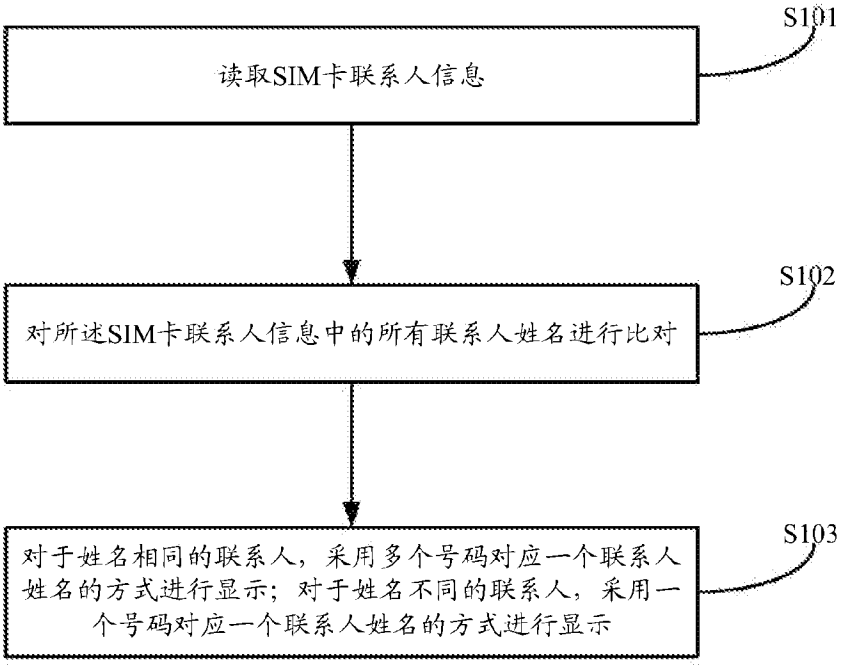


图 2

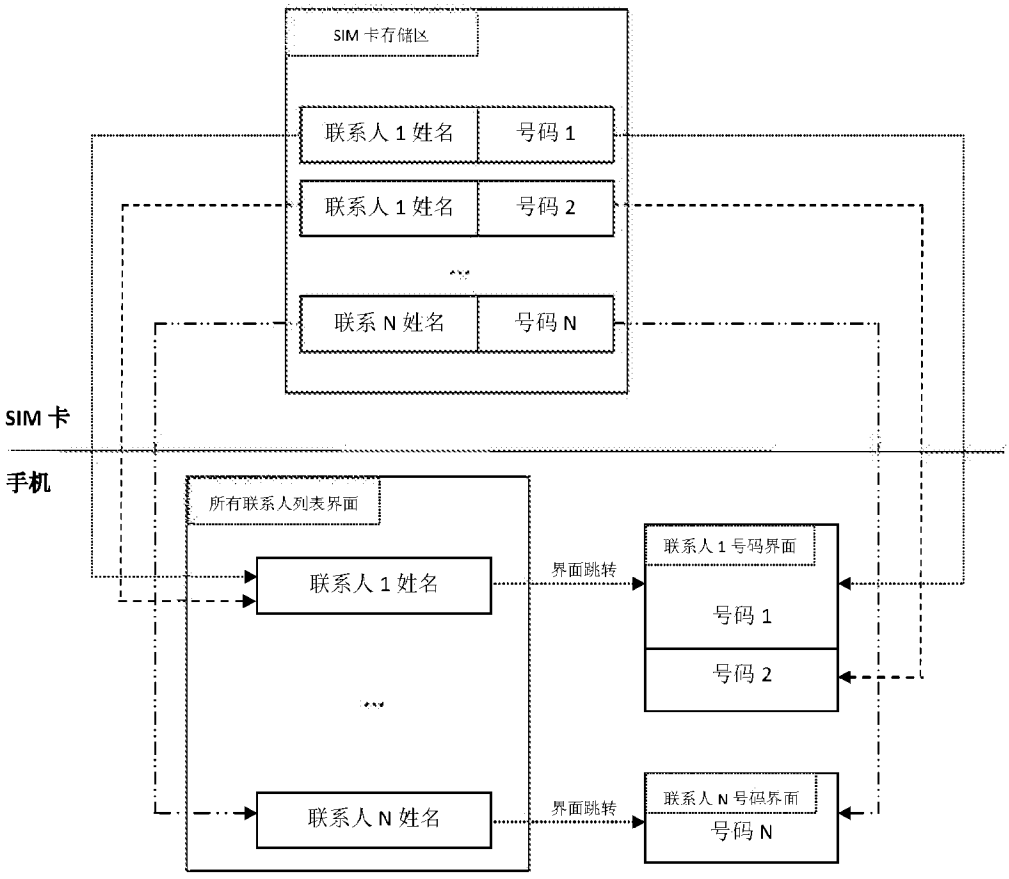


图 3

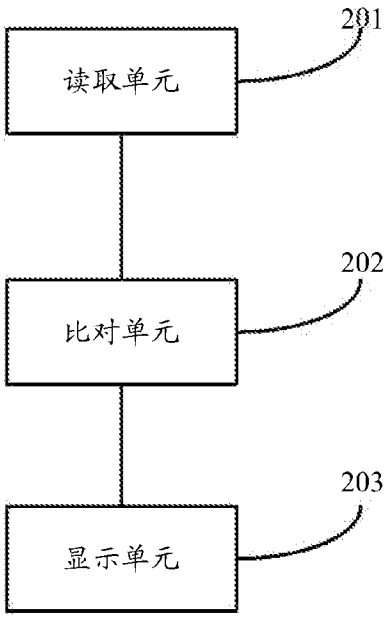


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/087426

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04M1/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNKI, CNTXT, VEN: telephone list, telephone directory, address list, contacts, numbers, name?, same name, SIM, USIM, card, display, compare+, combinat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	TW I287381 B (ASUSTEK COMPUTER INC.) 21 September 2007 (21.09.2007)	
X	claims 1, 2, 10, 11, and description, page 9 line 21 to page 10 line 3	1-4, 6-10, 12
Y	See above	5, 11
	CN 102104684 A (HUAWEI DEVICE CO., LTD.) 22 June 2011 (22.06.2011)	
Y	description, paragraphs [0031]-[0048], and table 1	5, 11
A	The whole document	1-4, 6-10, 12
	CN 102905002 A (GUANGDONG OPPO MOBILE COMMUNICATION CO., LTD.)	
A	30 January 2013 (30.01.2013) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 2014 (17.02.2014)	27 February 2014 (27.02.2014)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer GAO, Xia Telephone No. (86-10) 62089547

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/087426

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
TWI 287381 B	21.09.2007	TW 200713994 A	01.04.2007
		US 2007060199 A1	15.03.2007
		US 8170613 B2	01.05.2012
CN 102104684 A	22.06.2011	CN 102104684 B	09.10.2013
CN 102905002 A	30.01.2013	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/087426

Continuation of: second sheet A. CLASSIFICATION OF SUBJECT MATTER

H04M 1/275 (2006.01) i

H04M 1/725 (2006.01) n

国际检索报告

国际申请号
PCT/CN2013/087426

A. 主题的分类

见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04M1/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS, CNKI, CNTXT, VEN: 通讯录，通讯簿，通信录，通信簿，电话本，联系人，号码，姓名，名字，重名，同名，多个，卡，显示，比对，对比，合并；contacts, telephone list, telephone directory, address list, numbers, name?, same, SIM, USIM, card, display, compare+, combinat+

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
	TW I287381 B (华硕电脑股份有限公司) 21.9 月 2007 (21.09.2007)	
X	权利要求 1、2、10、11，以及说明书第 9 页第 21 行-第 10 页第 3 行	1-4, 6-10, 12
Y	同上	5, 11
	CN 102104684 A (华为终端有限公司) 22.6 月 2011 (22.06.2011)	
Y	说明书第[0031]-[0048]段，以及表 1	5, 11
A	全文	1-4, 6-10, 12
	CN 102905002 A (广东欧珀移动通信有限公司) 30.1 月 2013 (30.01.2013)	
A	全文	1-12

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
17.2 月 2014（17.02.2014）	**27.2 月 2014 (27.02.2014)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西上城路 6 号 100088 传真号：　(86-10)62019451	受权官员 **高霞** 电话号码：(86-10) **62411499**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/087426

检索报告中引用的专利文件	公布日期	同族专利	公布日期
TW I287381 B	21.09.2007	TW 200713994 A	01.04.2007
		US 2007060199 A1	15.03.2007
		US 8170613 B2	01.05.2012
CN 102104684 A	22.06.2011	CN 102104684 B	09.10.2013
CN 102905002 A	30.01.2013	无	

续： 第 2 页 **A.** 主题的分类

H04M 1/275 (2006.01) i

H04M 1/725 (2006.01) n

Electronic Acknowledgement Receipt

EFS ID:	21149007
Application Number:	13966096
International Application Number:	
Confirmation Number:	8712
Title of Invention:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
First Named Inventor/Applicant Name:	CLAY PERREAULT
Customer Number:	20995
Filer:	John M Carson/Norman Green
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.001C1
Receipt Date:	07-JAN-2015
Filing Date:	13-AUG-2013
Time Stamp:	18:27:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_SMARB19_001C1_01_07_2015.pdf	220905 9b828e8743d3fa0a5117104bd5f1dad6d623e82a	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	5	
Warnings:					
Information:					
2	Foreign Reference	Ref42_CA2659007.pdf	4712669 b8ffbd7ea248ee05a2ef93c71c60676e2e6def4b	no	62
Warnings:					
Information:					
3	Foreign Reference	Ref43_CA2778905.pdf	7009768 b8f04de5e7d508ab8261631df13fd3f7fa20a564	no	82
Warnings:					
Information:					
4	Foreign Reference	Ref44_CN102137024A.pdf	1808580 4c531eb36dcb3065d8bb1903b2f67665b453d65b	no	18
Warnings:					
Information:					
5	Foreign Reference	Ref45_JP2011199384.pdf	1171823 300397098b0e1107a3b04e309dcb11191ade6184	no	13
Warnings:					
Information:					
6	Foreign Reference	Ref46_WO01050693A1.pdf	9161416 27e9e469d8be5d592552b89122af00384eb2231f	no	126
Warnings:					
Information:					
7	Foreign Reference	Ref47_WO03027801A2.pdf	1589172 35be5edf47019053d41eef2b46cb43d61c0ca754	no	20
Warnings:					
Information:					
8	Foreign Reference	Ref48_WO2013120069A1.pdf	2034106 9705f71c44c96dbd8fea783951cd4fe571a3844c	no	26
Warnings:					
Information:					

9	Foreign Reference	Ref49_WO2014066155A2.pdf	1656227 9edd609c44ff99c765f8f4c8b77d8dea81d70727	no	21
Warnings:					
Information:					
10	Foreign Reference	Ref50_WO2014117599A1.pdf	3367344 dbf3e55e175a40313dac74f70d297103fc7ef74f	no	40
Warnings:					
Information:					
11	Foreign Reference	Ref51_WO2014166258A1.pdf	1536864 76474f066e67258940cb8ef7502c820178cb4c19	no	22
Warnings:					
Information:					
12	Non Patent Literature	Ref52_ETSI_TS_122_173_V12_7_0_2014-10.pdf	1188696 6cf93c7e9b550351efec483bbf9b8b8536fe9d45	no	14
Warnings:					
Information:					
13	Non Patent Literature	Ref53_Huitema_et_al_Bellcore_1999.pdf	1361023 7efed91bc1685bbfb103874f69d7bfa6dff08f0f	no	14
Warnings:					
Information:					
14	Non Patent Literature	Ref54_Stallings_2003.pdf	1058786 3b18d11f32ef6c0efa3501eb9ab07965ec7e7ba4	no	12
Warnings:					
Information:					
			Total Files Size (in bytes):	37877379	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Inventor	:	Clay Perreault, et al.
App. No.	:	13/966,096
Filed	:	August 13, 2013
For	:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
Examiner	:	Sing, Simon P.
Art Unit	:	2653
Conf. No.	:	8712

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Pursuant to 37 CFR 1.56, an Information Disclosure Statement listing references is provided herewith. Copies of any listed foreign and non-patent literature references are being submitted. Any foreign references may also include English abstract(s) and/or machine translation(s), but no representation is made as to their accuracy.

If the Examiner would like additional information regarding these references or if anything is unclear, the Examiner is invited to contact the undersigned for assistance.

No Disclaimers

To the extent that anything in the Information Disclosure Statement or the listed references could be construed as a disclaimer of any subject matter supported by the present application, Applicant hereby rescinds and retracts such disclaimer.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits, and presumably no fee is required. If a First Office Action on the merits

was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 1/7/15

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

IDS
19660493
010615

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	Sing, Simon P.
SHEET 1 OF 1	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	6,445,694 B1	09-03-2002	Swartz, Robert	
	2	6,574,328 B1	06-03-2003	Wood et al.	
	3	6,785,266 B2	08-31-2004	Swartz, Robert	
	4	7,486,664 B2	02-03-2009	Swartz, Robert	
	5	7,512,117 B2	03-31-2009	Swartz, Robert	
	6	7,587,036 B2	09-08-2009	Wood et al.	
	7	7,764,777 B2	07-27-2010	Wood et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T^1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T^1

19561108
121614

Examiner Signature	Date Considered

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T^1 - Place a check mark in this area when an English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	21002018
Application Number:	13966096
International Application Number:	
Confirmation Number:	8712
Title of Invention:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
First Named Inventor/Applicant Name:	CLAY PERREAULT
Customer Number:	20995
Filer:	John M Carson/Norman Green
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.001C1
Receipt Date:	18-DEC-2014
Filing Date:	13-AUG-2013
Time Stamp:	12:57:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_SMARB19_001C1_12_18_2014.pdf	91252 ca5acb691f4373027c439d41c352c15cd78e9e59	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	91252	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT

Inventor	:	Clay Perreault, et al.
App. No.	:	13/966,096
Filed	:	August 13, 2013
For	:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
Examiner	:	Sing, Simon P
Art Unit	:	2653
Conf. No.	:	8712

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Pursuant to 37 CFR 1.56, an Information Disclosure Statement listing references is provided herewith. Copies of any listed foreign and non-patent literature references are being submitted.

No Disclaimers

To the extent that anything in the Information Disclosure Statement or the listed references could be construed as a disclaimer of any subject matter supported by the present application, Applicant hereby rescinds and retracts such disclaimer.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits, and presumably no fee is required. If a First Office Action on the merits

was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 12/18/14

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

IDS
19561154
121614

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 1 OF 11	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	1	5,325,421	06-28-1994	Hou et al.	
	2	6,553,025 B1	04-22-2003	Kung et al.	
	3	6,560,224 B1	05-06-2003	Kung et al.	
	4	6,650,641 B1	11-18-2003	Albert et al.	
	5	6,775,534 B2	08-10-2004	Lindgren et al.	
	6	6,934,279 B1	08-23-2005	Sollee et al.	
	7	6,963,739 B2	11-08-2005	Dorenbosch et al.	
	8	6,985,440 B1	01-10-2006	Albert et al.	
	9	6,993,015 B2	01-31-2006	Kobayashi, Toshihiko	
	10	7,006,508 B2	02-28-2006	Bondy et al.	
	11	7,027,564 B2	04-11-2006	James, Anthony W.	
	12	7,068,668 B2	06-27-2006	Feuer, Donald S.	
	13	7,151,772 B1	12-19-2006	Kalmanek, Jr. et al.	
	14	7,177,399 B2	02-13-2007	Dawson et al.	
	15	7,277,528 B2	10-02-2007	Rao et al.	
	16	7,400,881 B2	07-15-2008	Kallio, Juha	
	17	7,436,835 B2	10-14-2008	Castleberry et al.	
	18	7,440,442 B2	10-21-2008	Grabelsky et al.	
	19	7,486,667 B2	02-03-2009	Feuer, Donald S.	
	20	7,567,131 B2	07-21-2009	Rollender et al.	
	21	7,573,982 B2	08-11-2009	Breen et al.	
	22	7,593,390 B2	09-22-2009	Lebizay, Gerald	
	23	7,639,792 B2	12-29-2009	Qiu et al.	
	24	7,657,011 B1	02-02-2010	Zielinski et al.	
	25	7,664,495 B1	02-16-2010	Bonner et al.	
	26	7,676,215 B2	03-09-2010	Chin et al.	
	27	7,680,114 B2	03-16-2010	Yazaki et al.	
	28	7,702,308 B2	04-20-2010	Rollender, Douglas Harold	

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 2 OF 11	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	29	7,715,821 B2	05-11-2010	Rollender, Douglas Harold	
	30	7,738,384 B2	06-15-2010	Pelletier, Jeffrey P.	
	31	7,764,944 B2	07-27-2010	Rollender, Douglas Harold	
	32	7,797,459 B1	09-14-2010	Roy et al.	
	33	7,894,441 B2	02-22-2011	Yazaki et al.	
	34	7,907,551 B2	03-15-2011	Croy et al.	
	35	7,929,955 B1	04-19-2011	Bonner, Thomas W.	
	36	7,944,909 B2	05-17-2011	James, Anthony W.	
	37	7,965,645 B2	06-21-2011	Pelletier, Jeffrey P.	
	38	7,979,529 B2	07-12-2011	Kreusch et al.	
	39	7,995,589 B2	08-09-2011	Sollee et al.	
	40	8,024,785 B2	09-20-2011	Andress et al.	
	41	8,027,333 B2	09-27-2011	Grabelsky et al.	
	42	8,041,022 B1	10-18-2011	Andreasen et al.	
	43	8,050,273 B2	11-01-2011	Gass, Raymond	
	44	8,125,982 B2	02-28-2012	Feuer, Donald S.	
	45	8,145,182 B2	03-27-2012	Rudolf et al.	
	46	8,166,533 B2	04-24-2012	Yuan, Wei	
	47	8,189,568 B2	05-29-2012	Qiu et al.	
	48	8,204,044 B2	06-19-2012	Lebizay, Gerald	
	49	8,228,897 B2	07-24-2012	Mitchell, Don	
	50	8,244,204 B1	08-14-2012	Chen et al.	
	51	8,306,063 B2	11-06-2012	Erdal et al.	
	52	8,363,647 B2	01-29-2013	Fangman et al.	
	53	8,427,981 B2	04-23-2013	Wyss et al.	
	54	8,437,340 B2	05-07-2013	James, Anthony W.	
	55	8,462,915 B2	06-11-2013	Breen et al.	
	56	8,509,225 B2	08-13-2013	Grabelsky et al.	
	57	8,605,714 B2	12-10-2013	Lebizay, Gerald	

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 3 OF 11	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	58	8,605,869 B1	12-10-2013	Mobarak et al.	
	59	8,607,323 B2	12-10-2013	Yuan, Wei	
	60	8,611,354 B2	12-17-2013	Keränen et al.	
	61	8,625,578 B2	01-07-2014	Roy et al.	
	62	8,724,643 B2	05-13-2014	Feuer, Donald S.	
	63	8,750,290 B2	06-10-2014	Vance et al.	
	64	8,763,081 B2	06-24-2014	Bogdanovic et al.	
	65	8,768,951 B2	07-01-2014	Crago, William Barry	
	66	8,774,171 B2	07-08-2014	Mitchell, Don	
	67	8,804,705 B2	08-12-2014	Voxpath Networks, Inc.	
	68	2001/0052081 A1	12-13-2001	McKibben et al.	
	69	2002/0002041 A1	01-03-2002	Lindgren et al.	
	70	2002/0018445 A1	02-14-2002	Kobayashi, Toshihiko	
	71	2002/0141352 A1	10-03-2002	Fangman et al.	
	72	2003/0012196 A1	01-16-2003	Ramakrishnan, Kadangode K.	
	73	2003/0095539 A1	05-22-2003	Feuer, Donald S.	
	74	2003/0179747 A1	09-25-2003	Pyke et al.	
	75	2003/0219103 A1	11-27-2003	Rao et al.	
	76	2004/0034793 A1	02-19-2004	Yuan, Wei	
	77	2004/0203582 A1	10-14-2004	Dorenbosch et al.	
	78	2004/0203565 A1	10-14-2004	Chin et al.	
	79	2005/0063519 A1	03-24-2005	James, Anthony W.	
	80	2005/0188081 A1	08-25-2005	Gibson et al.	
	81	2005/0190892 A1	09-01-2005	Dawson et al.	
	82	2005/0202799 A1	09-15-2005	Rollender, Douglas Harold	
	83	2005/0287979 A1	12-29-2005	Rollender, Douglas Harold	
	84	2006/0007940 A1	01-12-2006	Sollee et al.	
	85	2006/0013266 A1	01-19-2006	Vega-Garcia et al.	
	86	2006/0030290 A1	02-09-2006	Rudolf et al.	

Examiner Signature	Date Considered

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 4 OF 11	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	87	2006/0078094 A1	04-13-2006	Breen et al.	
	88	2006/0142011 A1	06-29-2006	Kallio, Juha	
	89	2006/0146797 A1	07-06-2006	Lebizay, Gerald	
	90	2006/0189303 A1	08-24-2006	Rollender, Douglas Harold	
	91	2006/0205383 A1	09-14-2006	Rollender et al.	
	92	2006/0248186 A1	11-02-2006	Smith, Richard James	
	93	2006/0251056 A1	11-09-2006	Feuer, Donald S.	
	94	2006/0268921 A1	11-30-2006	Ekstrom et al.	
	95	2006/0281437 A1	12-14-2006	Cook, Charles I.	
	96	2007/0047548 A1	03-01-2007	Yazaki et al.	
	97	2007/0092070 A1	04-26-2007	Croy et al.	
	98	2007/0115935 A1	05-24-2007	Qiu et al.	
	99	2007/0121593 A1	05-31-2007	Vance et al.	
	100	2007/0174469 A1	07-26-2007	Andress et al.	
	101	2007/0220038 A1	09-20-2007	Crago, William Barry	
	102	2007/0253429 A1	11-01-2007	James, Anthony W.	
	103	2007/0263609 A1	11-15-2007	Mitchell, Don	
	104	2007/0297376 A1	12-27-2007	Gass, Raymond	
	105	2008/0013523 A1	01-17-2008	Nambakkam, Sampath	
	106	2008/0056243 A1	03-06-2008	Roy et al.	
	107	2008/0167039 A1	07-10-2008	Guedalia et al.	
	108	2008/0167020 A1	07-10-2008	Guedalia et al.	
	109	2008/0167019 A1	07-10-2008	Guedalia et al.	
	110	2008/0166999 A1	07-10-2008	Guedalia et al.	
	111	2008/0188227 A1	08-07-2008	Guedalia et al.	
	112	2008/0188198 A1	08-07-2008	Patel et al.	
	113	2008/0187122 A1	08-07-2008	Baker, Colin Lawrence Melvin	
	114	2008/0205378 A1	08-28-2008	Wyss et al.	
	115	2008/0310599 A1	12-18-2008	Purnadi et al.	

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 5 OF 11	Attorney Docket No.	SMARB19.001C1

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number *Number - Kind Code (if known)* Example: 1,234,567 B1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear
	116	2009/0003535 A1	01-01-2009	Grabelsky et al.	
	117	2009/0129566 A1	05-21-2009	Feuer, Donald S.	
	118	2009/0135724 A1	05-28-2009	Zhang et al.	
	119	2009/0135735 A1	05-28-2009	Zhang et al.	
	120	2009/0214000 A1	08-27-2009	Patel et al.	
	121	2009/0268615 A1	10-29-2009	Pelletier, Jeffrey P.	
	122	2009/0296900 A1	12-03-2009	Breen et al.	
	123	2010/0008345 A1	01-14-2010	Lebizay, Gerald	
	124	2010/0039946 A1	02-18-2010	Imbimbo et al.	
	125	2010/0105379 A1	04-29-2010	Bonner et al.	
	126	2010/0177671 A1	07-15-2010	Qiu et al.	
	127	2010/0246589 A1	09-30-2010	Pelletier, Jeffrey P.	
	128	2010/0272242 A1	10-28-2010	Croy et al.	
	129	2011/0013541 A1	01-20-2011	Croy et al.	
	130	2011/0153809 A1	06-23-2011	Ghanem et al.	
	131	2011/0176541 A1	07-21-2011	James, Anthony W.	
	132	2011/0201321 A1	08-18-2011	Bonner, Thomas W.	
	133	2011/0267986 A1	11-03-2011	Grabelsky et al.	
	134	2012/0014383 A1	01-19-2012	Geromel et al.	
	135	2012/0113981 A1	05-10-2012	Feuer, Donald S.	
	136	2012/0195415 A1	08-02-2012	Wyss et al.	
	137	2012/0250624 A1	10-04-2012	Lebizay, Gerald	
	138	2012/0282881 A1	11-08-2012	Mitchell, Don	
	139	2012/0314699 A1	12-13-2012	Qiu et al.	
	140	2013/0272297 A1	10-17-2013	AT&T Intellectual Property I, L.P.	
	141	2014/0101749 A1	04-10-2014	Rockstar Consortium US LP	
	142	2014/0211789 A1	07-31-2014	Centre One	

Examiner Signature	Date Considered

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 6 OF 11	Attorney Docket No.	SMARB19.001C1

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	143	CA 2 218 218 A1	10-14-1997	AT&T Corp.		
	144	CA 2 299 037 A1	08-22-2000	Selex Communications, LLC		Abstract
	145	CA 2 437 275 A1	10-17-2002	Nortel Networks Limited		Abstract
	146	CA 2 690 236 A1	12-18-2008	Research In Motion Ltd		Abstract
	147	CN 1498029 A	05-19-2004	Lucent Technologies Inc		Abstract
	148	CN 1498482 A	05-19-2004	Siemens AG		Abstract
	149	CN 1668137 A	09-14-2005	Lucent Technologies Inc		Abstract
	150	CN 1274114 C	09-06-2006	Siemens AG		Abstract
	151	CN 101005503 A	07-25-2007	IBM		Abstract
	152	CN 101069390 A	11-07-2007	Nokia Corp		Abstract
	153	CN 101095329 A	12-26-2007	Intel Corp		Abstract
	154	CN 1498029 B	05-12-2010	Lucent Technologies Inc		Abstract
	155	CN 101772929 A	07-07-2010	Research In Motion Ltd		Abstract
	156	CN 101069390 B	12-22-2010	Nokia Corp		Abstract
	157	CN 102484656 A	05-30-2012	Telefonaktiebolaget LM Ericsson		Abstract
	158	CN 101095329 B	10-10-2012	Intel Corp		Abstract
	159	CN 102833232 A	12-19-2012	Intel Corp		Abstract
	160	CN 101005503 B	01-16-2013	IBM		Abstract
	161	CN 101772929 B	07-02-2014	Research In Motion Ltd		Abstract
	162	DE 602 01 827 T2	11-10-2005	Alcatel SA		Abstract
	163	DE 11 2005 003 306 T5	01-24-2008	Intel Corp	*Corresponding Abstract: International Publication No. WO 2006/072099 A1 published 07-06-2006; is supplied with this document*	Abstract
	164	DE 601 33 316 T2	07-10-2008	Nortel Networks Ltd.		Abstract
	165	DE 603 17 751 T2	11-06-2008	Lucent Technologies Inc		Abstract
	166	EP 0 841 832 A2	05-13-1998	AT&T Corp.		
	167	EP 0 841 832 A3	05-19-1999	AT&T Corp.		

Examiner Signature	Date Considered

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 7 OF 11	Attorney Docket No.	SMARB19.001C1

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	168	EP 1 032 224 A2	08-30-2000	Selex Communications, LLC		
	169	EP 1 032 224 A3	08-30-2000	Selex Communications, LLC		
	170	EP 1 244 250 A1	09-25-2002	Siemens AG		Abstract
	171	EP 1 266 516 A2	12-18-2002	Nortel Networks Ltd	*Published by WIPO under: International Publication No. WO 01/069899 A2 published 12-18-2002; Abstract of which is supplied with this document*	Abstract
	172	EP 1 362 456 A2	11-19-2003	Nortel Networks Ltd	*Published by WIPO under: International Publication No. WO 02/082782 A2 published 10-17-2002; Abstract of which is supplied with this document*	Abstract
	173	EP 1 371 173 A1	12-17-2003	Siemens AG	*Published by WIPO under: International Publication No. WO 02/082728 A1 published 10-17-2002; Abstract of which is supplied with this document*	Abstract
	174	EP 1 411 743 A1	04-21-2004	Lucent Technologies Inc.		
	175	EP 1 526 697 A2	04-27-2005	3COM Corporation		
	176	EP 1 362 456 A4	05-25-2005	Nortel Networks Ltd		Abstract
	177	EP 1 575 327 A1	09-14-2005	Lucent Technologies Inc.		
	178	EP 1 610 583 A1	12-28-2005	Lucent Technologies Inc.		
	179	EP 1 526 697 A3	03-22-2006	3COM Corporation		
	180	EP 1 721 446 A1	11-15-2006	Nortel Networks Ltd	*Published by WIPO under: International Publication No. WO 2005/084002 A1 published 10-09-2005; Abstract of which is supplied with this document*	Abstract

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.*	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT		
	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 8 OF 11	Attorney Docket No.	SMARB19.001C1

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	181	EP 1 829 300 A1	09-05-2007	Nokia Corp	Published by WIPO under: International Publication No. WO 2006/067269 A1 published 06-29-2006; Abstract of which is supplied with this document	Abstract
	182	EP 1 371 173 B1	11-28-2007	Siemens AG		Abstract
	183	EP 1 411 743 B1	11-28-2007	Lucent Technologies Inc.		
	184	EP 1 362 456 B1	03-19-2008	Nortel Networks Ltd		
	185	EP 1 974 304 A2	10-01-2008	Medical Envelope LLC	*Published by WIPO under: International Publication No. WO 2007/087077 A2 published 08-02-2007; Abstract of which is supplied with this document*	Abstract
	186	EP 1 974 304 A4	10-01-2008	Medical Envelope LLC		Abstract
	187	EP 1 610 583 B1	08-26-2009	Lucent Technologies Inc.		
	188	EP 2 127 232 A1	12-02-2009	Interactive Intelligence Inc	*Published by WIPO under: International Publication No. WO 2008/103652 A1 published 08-28-2008; Abstract of which is supplied with this document*	Abstract
	189	EP 2 165 489 A1	03-24-2010	Research In Motion Ltd	*Published by WIPO under: International Publication No. WO 2008/103652 A1 published 08-28-2008; Abstract of which is supplied with this document*	Abstract
	190	EP 2 215 755 A1	08-11-2010	Broadsoft Inc	*Published by WIPO under: International Publication No. WO 2009/070278 A1 published 06-04-2009; Abstract of which is supplied with this document*	Abstract
	191	EP 2 165 489 A4	03-02-2011	Research In Motion Ltd		Abstract
	192	EP 2 127 232 A4	03-16-2011	Interactive Intelligence Inc		Abstract

Examiner Signature	Date Considered

***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 9 OF 11	Attorney Docket No.	SMARB19.001C1

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	193	EP 1 829 300 A4	05-02-2012	Nokia Corp	Corresponding Abstract: International Publication No. WO 2006/067269 A1 published 06-29-2006; is supplied with this document	Abstract
	194	EP 2 449 749 A1	05-09-2012	Telefonaktiebolaget LM Ericsson	*Published by WIPO under: International Publication No. WO 2011/000405 A1 published 01-06-2011; Abstract of which is supplied with this document*	Abstract
	195	EP 2 215 755 A4	10-24-2012	Broadsoft Inc		Abstract
	196	EP 1 829 300 B1	11-21-2012	Nokia Corp	*Corresponding Abstract: International Publication No. WO 2006/067269 A1 published 06-29-2006; is supplied with this document*	Abstract
	197	EP 2 449 749 B1	03-12-2014	Telefonaktiebolaget LM Ericsson		
	198	EP 1 266 516 B1	05-07-2014	Genband US LLC		
	199	WO 01/69899 A2	09-20-2001	Nortel Networks Ltd.		
	200	WO 01/69899 A3	09-20-2001	Nortel Networks Ltd.		
	201	WO 01/80587 A1	10-25-2001	Telefonaktiebolaget LM Ericsson		
	202	WO 02/082728 A1	10-17-2002	Siemens AG		Abstract
	203	WO 02/082782 A2	10-17-2002	Nortel Networks Limited		
	204	WO 02/082782 A3	10-17-2002	Nortel Networks Limited		
	205	WO 2005/084002 A1	09-09-2005	Nortel Networks Limited		
	206	WO 2006/067269 A1	06-29-2006	Nokia Corporation		
	207	WO 2006/072099 A1	07-06-2006	Intel Corporation		
	208	WO 2006/078175 A2	07-27-2006	Baker, Colin et al.		
	209	WO 2006/078175 A3	07-27-2006	Baker, Colin et al.		
	210	WO 2007/044454 A2	04-19-2007	Telecommunication Systems, Inc.		
	211	WO 2007/087077 A2	08-02-2007	Medical Envelope LLC		

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 10 OF 11	Attorney Docket No.	SMARB19.001C1

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document *Country Code-Number-Kind Code* Example: JP 1234567 A1	Publication Date MM-DD-YYYY	Name	Pages, Columns, Lines Where Relevant Passages or Relevant Figures Appear	T[1]
	212	WO 2007/087077 A3	08-02-2007	Medical Envelope LLC		
	213	WO 2008/085614 A2	07-17-2008	ISKOOT, Inc.		
	214	WO 2008/085614 A3	07-17-2008	ISKOOT, Inc.		
	215	WO 2008/086350 A2	07-17-2008	ISKOOT, Inc.		
	216	WO 2008/086350 A3	07-17-2008	ISKOOT, Inc.		
	217	WO 2008/103652 A1	08-28-2008	Interactive Intelligence, Inc.		
	218	WO 2008/085614 A8	12-11-2008	ISKOOT, Inc.		
	219	WO 2008/151406 A1	12-18-2008	Research In Motion Ltd		
	220	WO 2008/151406 A8	12-18-2008	Research In Motion Ltd		
	221	WO 2009/070202 A1	06-04-2009	Tellabs Operations, Inc.		
	222	WO 2009/070278 A1	06-04-2009	Broadsoft, Inc.		
	223	WO 2011/000405 A1	01-06-2011	Telefonaktiebolaget LM Ericsson		

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	224	Baker *et al.*, "Cisco Support for Lawful Intercept In IP Networks," Internet Draft - working document of the Internet Engineering Task Force (IETF), accessible at http://www.ietf.org/ietf/lid-abstracts.txt, April 2003, expires September 30, 2003, pages 1-15.	
	225	Bhushan *et al.*, "Federated Accounting: Service Charging and Billing in a Business-to-Business Environment," 0-7803-6719-7/01, © 2001 IEEE, pages 107-121.	
	226	Jajszczyk *et al.*, "Emergency Calls in Flow-Aware Networks," *IEEE Communications Letters*, Vol. 11, No. 9, September 2007, pages 753-755.	
	227	Kim *et al.*, "An Enhanced VoIP Emergency Services Prototype," *Proceedings of the 3rd International ISCRAM Conference (B. Van de Walle and M. Turoff, eds.), Newark, NJ (USA)*, May 2006, pages 1-8.	
	228	Kornfeld *et al.*, "DVB-H and IP Datacast—Broadcast to Handheld Devices," *IEEE Transactions On Broadcasting*, Vol. 53, No. 1, March 2007, pages 161-170.	
	229	Kortebi *et al.*, "SINR-Based Routing in Multi-Hop Wireless Networks to Improve VoIP Applications Support," 1-4244-0667-6/07, © 2007 IEEE, pages 491-496.	
	230	Lee *et al.*, "VoIP Interoperation with KT-NGN," in *The 6th International Conference on Advanced Communication Technology*, Technical Proceedings, 2004, pages 126-128, accompanied by Title and Contents - 4 pages.	

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application No.	13/966,096
	Filing Date	August 13, 2013
	First Named Inventor	Perreault, Clay
	Art Unit	2653
(Multiple sheets used when necessary)	Examiner	8712
SHEET 11 OF 11	Attorney Docket No.	SMARB19.001C1

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
	231	Lin *et al.*, "Effective VoIP Call Routing in WLAN and Cellular Integration," *IEEE Communications Letters*, Vol. 9, No. 10, October 2005, pages 874-876.	
	232	Ma *et al.*, "Realizing MPEG4 Video Transmission Based on Mobile Station over GPRS," *0-7803-9335-X/05,* © 2005 IEEE, pages 1241-1244.	
	233	Mintz-Habib *et al.*, "A VoIP Emergency Services Architecture and Prototype," *{mm2571,asr,hgs,xiaotaow}@cs.columbia.edu, 0-7803-9428-3/05,* © 2005 IEEE, pages 523-528.	
	234	Munir, Muhammad Farukh, "Study of an Adaptive Scheme for Voice Transmission on IP in a Wireless Networking Environment 802.11e," *Dept. of Networks and Distributed Computing, Ecole Supérieure En Sciences Informatiques (ESSI), Université De Nice*, June 2005, (pages 1-35), BEST AVAILABLE COPY - pages 1-11.	
	235	Sripanidkulchai *et al.*, "Call Routing Management in Enterprise VoIP Networks," *Copyright 2007 ACM* 978-1-59593-788-9/07/0008, 6 pages.	
	236	Thernelius, Fredrik, "SIP, NAT, and Firewalls," Master's Thesis, *ERICSSON, Department of Teleinformatics*, May 2000, pages 1-69.	
	237	Trad *et al.*, "Adaptive VoIP Transmission over Heterogeneous Wired/Wireless Networks," *V. Roca and F. Rousscau (Eds.): MIPS 2004, LNCS 3311*, pp. 25-36, 2004, © Springer-Verlag Berlin Heidelberg 2004.	
	238	Yu et al., "Service-Oriented Issues: Mobility, Security, Charging and Billing Management in Mobile Next Generation Networks," *IEEE BcN2006, 1-4244-0146-1/06,* © 2006 IEEE, pages 1-10.	

19420768
112614

Examiner Signature	Date Considered
***Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

T[1] - Place a check mark in this area when an English language Translation is attached.

Electronic Acknowledgement Receipt

EFS ID:	20803282
Application Number:	13966096
International Application Number:	
Confirmation Number:	8712
Title of Invention:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
First Named Inventor/Applicant Name:	CLAY PERREAULT
Customer Number:	20995
Filer:	John M Carson/Norman Green
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.001C1
Receipt Date:	26-NOV-2014
Filing Date:	13-AUG-2013
Time Stamp:	18:44:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	FRef1_CA2218218A1.pdf	1303485 8736889d78c5bf43bf8f57298ce30628fb0d007c	no	19

Warnings:	
Information:	

2	Foreign Reference	FRef2_CA2299037A1.pdf	2459515 9204e3cdb1b58140db00988366a0f36fc16dd4a7	no	30
Warnings:					
Information:					
3	Foreign Reference	FRef3_CA2437275A1.pdf	3218137 659abad897a7d73180ff704a58b5907c2c23c72c	no	48
Warnings:					
Information:					
4	Foreign Reference	FRef4_CA2690236A1.pdf	2261223 c7229f41c59c93ce1862877d0fe339098e81ade0	no	28
Warnings:					
Information:					
5	Foreign Reference	FRef5_CN1498029A.pdf	1083455 d05ac1a88ebe6c0316a78a157cbcda428bc6b09a	no	13
Warnings:					
Information:					
6	Foreign Reference	FRef6_CN1498482A.pdf	1650102 ffa6dc51f75f3fa22a12712bbfbfeb6864f79396	no	18
Warnings:					
Information:					
7	Foreign Reference	FRef7_CN1668137A.pdf	1807688 cca62540137fe451056660dd218429fa05bfbb1a	no	21
Warnings:					
Information:					
8	Foreign Reference	FRef8_CN1274114C.pdf	1732150 f51ca2146d1c92841272b80a9d412fe7f6d8667b	no	19
Warnings:					
Information:					
9	Foreign Reference	FRef9_CN101005503A.pdf	2237498 f35007d260013445bfee706d2b6e9ee5d32eda85	no	26
Warnings:					
Information:					
10	Foreign Reference	FRef10_CN101069390A.pdf	2768939 8194859e193c669f747f67f33ba9386370dfbf4e	no	30
Warnings:					
Information:					

11	Foreign Reference	FRef11_CN101095329A.pdf	1902050 6c7ebb38c8723d53710267bf54bf44be6921e2d3	no	23
Warnings:					
Information:					
12	Foreign Reference	FRef12_CN1498029B.pdf	833982 a75f29202e36f404eb0634ff889ff4d38f41586f	no	9
Warnings:					
Information:					
13	Foreign Reference	FRef13_CN101772929A.pdf	1629030 08c526bd92a9cf2b1b50964b69b1a2134d1aadc0	no	17
Warnings:					
Information:					
14	Foreign Reference	FRef14_CN101069390B.pdf	2209004 f8f44c75aba5224c84d0b9adbd9fef15f35c544d	no	22
Warnings:					
Information:					
15	Foreign Reference	FRef15_CN102484656A.pdf	1705748 f307d672b2d5a27e6a0b525f6e994823c8651fea	no	19
Warnings:					
Information:					
16	Foreign Reference	FRef16_CN101095329B.pdf	1361015 51e0d6311708aa7d42f82d3d60b6446a3a811661	no	15
Warnings:					
Information:					
17	Foreign Reference	FRef17_CN102833232A.pdf	1652929 77419d14a25a03114612d4a255d723e7966cd4c4	no	17
Warnings:					
Information:					
18	Foreign Reference	FRef18_CN101005503B.pdf	1847539 aac46ec05928d6c74fc32767f9ef3699681e4479	no	20
Warnings:					
Information:					
19	Foreign Reference	FRef19_CN101772929B.pdf	1551207 80c03d8efc95bfb8b627efd3e192342a2efd8d77	no	16
Warnings:					
Information:					

20	Foreign Reference	FRef20_DE60201827T2.pdf	1119159 9f9d8053d06921fd7454c6f4950161d285d9e123	no	12
Warnings:					
Information:					
21	Foreign Reference	FRef21_DE112005003306T5.pdf	1512167 6eace51bedcefe71dc8ea6f0a658421a8c681e17	no	15
Warnings:					
Information:					
22	Foreign Reference	FRef22_DE60133316T2.pdf	2073005 0b7d9cb1fe49ab2cfbf09ba4a79bba61c579fead	no	22
Warnings:					
Information:					
23	Foreign Reference	FRef23_DE60317751T2.pdf	826323 483daaec48a2ae1ea36632e06273ad6e14c39926	no	9
Warnings:					
Information:					
24	Foreign Reference	FRef24_EP0841832A2.pdf	758379 4d5156c5c3db4d33e8f390e708b23c898eefac1e	no	9
Warnings:					
Information:					
25	Foreign Reference	FRef25_EP0841832A3.pdf	235091 a6d030529f93eba0307027ca64fa6351eff52f30	no	3
Warnings:					
Information:					
26	Foreign Reference	FRef26_EP1032224A2.pdf	1507492 b66fdda86c09b5cb6355ff4d794ebe1c29c2ab22	no	15
Warnings:					
Information:					
27	Foreign Reference	FRef27_EP1032224A3.pdf	227098 fab9d807b0fcbe48e55f6bb0965f2a86aa21a2e2	no	3
Warnings:					
Information:					
28	Foreign Reference	FRef28_EP1244250A1.pdf	1375810 491c74c40bc6870da6ebba229ee1bcfb74f3a49e	no	15
Warnings:					
Information:					

29	Foreign Reference	FRef29_EP1266516A2.pdf	232303 32c6c3e74bcab714f623d0b7164c0865703d70cb	no	3
Warnings:					
Information:					
30	Foreign Reference	FRef30_EP1362456A2.pdf	201764 d414145f3edbae068ab741133e25a8547bab204c	no	3
Warnings:					
Information:					
31	Foreign Reference	FRef31_EP1371173A1.pdf	192586 27004385fcd7f33d6eaa4cc950db18e1da222da8	no	3
Warnings:					
Information:					
32	Foreign Reference	FRef32_EP1411743A1.pdf	758578 07e12820c2ddf8741baf850d8b18bf16010f1761	no	9
Warnings:					
Information:					
33	Foreign Reference	FRef33_EP1526697A2.pdf	2485309 836e62ccbf6d63dc4a8844c19d299de31b2cdf35	no	24
Warnings:					
Information:					
34	Foreign Reference	FRef34_EP1362456A4.pdf	448171 1ccbee57f439c649369b71939e4787981fd6c2fb	no	6
Warnings:					
Information:					
35	Foreign Reference	FRef35_EP1575327A1.pdf	1278549 c5ff8e8c1636b7ef99aa10efa8e3542fe08a0822	no	14
Warnings:					
Information:					
36	Foreign Reference	FRef36_EP1610583A1.pdf	1280817 6f886a1fe38cc7944e2affb538f6de4c7c3fb9d4	no	14
Warnings:					
Information:					
37	Foreign Reference	FRef37_EP1526697A3.pdf	230778 bdb80ac61450132c8f6c8b1f497bf7bbc087debf	no	3
Warnings:					
Information:					

38	Foreign Reference	FRef38_EP1721446A1.pdf	149760 c12dc86950622c5a9e01fc16ee3a682c06f31477	no	2
Warnings:					
Information:					
39	Foreign Reference	FRef39_EP1829300A1.pdf	195921 8a3ed67caaa669f3183ff35c05ae3a647423fb25	no	3
Warnings:					
Information:					
40	Foreign Reference	FRef40_EP1371173B1.pdf	1738177 069f2f942db1a537019c200d9b0530c55e6966b2	no	18
Warnings:					
Information:					
41	Foreign Reference	FRef41_EP1411743B1.pdf	762770 ebf3851c31f7662d9c1eda59c96efaab992660bb	no	9
Warnings:					
Information:					
42	Foreign Reference	FRef42_EP1362456B1.pdf	1883717 9b750b843d6f5b3bd04545d2ff7ffbcbf621578f	no	21
Warnings:					
Information:					
43	Foreign Reference	FRef43_EP1974304A2.pdf	196381 29d2f3d1725d7837fed4e5a7004fc85719df047b	no	3
Warnings:					
Information:					
44	Foreign Reference	FRef44_EP1974304A4.pdf	293312 66f9f1c13f96df8c3f50066776d3a467b53f111d	no	4
Warnings:					
Information:					
45	Foreign Reference	FRef45_EP1610583B1.pdf	1470579 0681150b1e402dbf0998e175d07302dabf0b7c25	no	15
Warnings:					
Information:					
46	Foreign Reference	FRef46_EP2127232A1.pdf	136823 a9b65fe4007f7068dd4365d3f2095d37c5eecf36	no	2
Warnings:					
Information:					

47	Foreign Reference	FRef47_EP2165489A1.pdf	135448 f2d181122dfddc9eeec51199f46eaa5b385a8de1	no	2
Warnings:					
Information:					
48	Foreign Reference	FRef48_EP2215755A1.pdf	187623 3ab8f469911de18093cbee37b4a4b5db5e72c05c	no	3
Warnings:					
Information:					
49	Foreign Reference	FRef49_EP2165489A4.pdf	226305 00c9292cd9e75dded893480f1ba1b308dc19f114	no	3
Warnings:					
Information:					
50	Foreign Reference	FRef50_EP2127232A4.pdf	315613 1d188490c5ca6d1e13dc000eb4b54d2fa8b7afb8	no	4
Warnings:					
Information:					
51	Foreign Reference	FRef51_EP1829300A4.pdf	276173 8977d6f4a2ab5bc505f6c35919da14078dc02afa	no	4
Warnings:					
Information:					
52	Foreign Reference	FRef52_EP2449749A1.pdf	144780 c4d5646435417ab1b6d0627af130c3fe97982e29	no	2
Warnings:					
Information:					
53	Foreign Reference	FRef53_EP2215755A4.pdf	269752 f7fb64ae232ffc99f8066abbace5058d05cd1abd	no	4
Warnings:					
Information:					
54	Foreign Reference	FRef54_EP1829300B1.pdf	220531 d3100d5fbd37a0343df1755b3197f1c87a796507	no	3
Warnings:					
Information:					
55		IDS_SMARB19_001C1_11_26_2014.pdf	761098 e7e70df3b0c5345f8ffc8cc836067f85f26136f7	yes	13

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	2
	Information Disclosure Statement (IDS) Form (SB08)	3	13
Warnings:			
Information:			
	Total Files Size (in bytes):	61322838	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

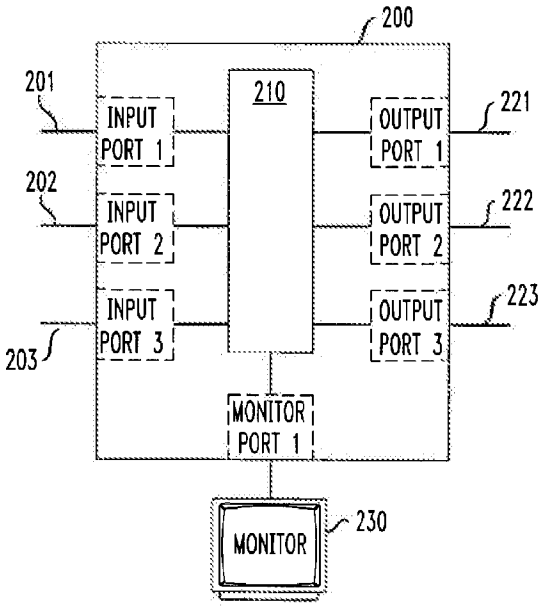
(21) (A1) **2,218,218**
(22) 1997/10/14
(43) 1998/05/08

(72) RAMAKRISHNAN, Kadangode K., US
(71) AT&T CORP., US

(51) Int.Cl.[6] H04L 12/26
(30) 1996/11/08 (746,364) US

(54) **SURVEILLANCE DE RESEAU HETEROGENE FAISANT APPEL A LA MULTI-DIFFUSION DANS UN COMMUTATEUR**

(54) **PROMISCUOUS NETWORK MONITORING UTILIZING MULTICASTING WITHIN A SWITCH**



(57) Utilisation de la multi-diffusion dans un commutateur pour établir une surveillance banalisée de réseaux de communication par commutation. Le commutateur achemine des paquets de données entre des ports d'entrée et des ports de sortie de données, et il achemine des copies de paquets de données vers un port de sortie du dispositif de surveillance. Un processeur de surveillance est relié à ce commutateur pour recevoir des copies de tous les paquets de données qu'a reçus le commutateur, ce qui lui permet de surveiller ainsi le réseau de communication.

(57) Multicasting within a switch is utilized to promiscuously monitor switched communication networks. The switch routes data packets from input ports to data output ports and routes copies of the data packets to a monitor output port. A monitor processor is connected to the switch to receive copies of all data packets received at the switch, and thereby monitor the communication network.

Promiscuous Network Monitoring Utilizing Multicasting Within a Switch

ABSTRACT OF THE DISCLOSURE

Multicasting within a switch is utilized to promiscuously monitor switched communication networks. The switch routes data packets from input ports to data output ports and routes copies of the data packets to a monitor output port. A monitor processor is connected to the switch to receive copies of all data packets received at the switch, and thereby monitor the communication network.

Promiscuous Network Monitoring Utilizing Multicasting Within a Switch

FIELD OF THE INVENTION

The present invention relates to promiscuous monitoring of communication networks. Specifically, this invention relates to a method and apparatus for providing promiscuous monitoring of a communication network through the use of multicasting within an ATM switch.

BACKGROUND

A communication network needs to be monitored to evaluate its performance and to diagnosis any potential problems. Typically, an end-station communication device(s) is connected to the network in such a manner that the end-station(s) receive all the data transmitted within the network: this is known as promiscuous monitoring. The configurations by which promiscuous monitoring can be performed will vary depending upon the type of network.

Multi-access networks, such as an FDDI (fiber distributed data interface) and Ethernet local-area network (LAN), allow multiple points of access. In these multi-access networks, a monitoring point can be easily established through which all of the network communication traffic passes. In such a case, an end-station can be connected to the network to easily perform promiscuous monitoring of the network. By disabling the end-station's filtering functions, it can receive and

promiscuously monitor all communication traffic transmitted over the network.

With asynchronous transfer mode (ATM) and other switched networks, however, such as switched Fast Ethernet or switched FDDI, promiscuous monitoring cannot be as easily performed because the links are point to point. Thus, in such networks, no one place exists within the network where a promiscuous monitor can be located to receive all the data packets/frames. A typical prior art approach is to promiscuously monitor each link going out of a switch output port by inserting a T-connector, such as an optical splitter, into the link.

Fig. 1 illustrates a prior art approach for promiscuous monitoring of a communication network. Sender communication devices 100a and 100b are connected to switch 110 which is connected to receiver communication devices 120a and 120b on links 130a and 130b, respectively. The communication network shown in Fig. 1 is simplified for illustrative purposes; thus, a typical communication network has a vast number of nodes with switches, sender and receiver communication devices, and links interconnecting the switches. Unlike the simple case shown in Fig. 1 having a single switch 110, communication data sent by a sender communication device will typically pass through multiple switches 110 before reaching a receiver communication device.

Using T-connector 140a and 140b, a copy of the packets transmitted on links 130a and 130b, respectively, will be received by not only the intended receiver, 120a and 120b, respectively, but also can be received by an end-station performing promiscuous monitoring. Within a communication network, the point of access for promiscuous monitoring is usually selected at the switch through which most of the communication traffic passes. Promiscuous monitors 150a and 150b are connected to each T-connector 140a and 140b, respectively, thereby monitoring links 130a and 130b, respectively. Alternatively, a single promiscuous monitor can be

connected to multiple T-connectors through multiple input ports in the promiscuous monitor thereby monitoring several individual links at the same monitor.

The prior art configurations present several shortcomings. As the number of switch output ports increases, the necessary number of T-connectors increases, and correspondingly the required number of monitoring end-stations or input ports at the monitoring end-station also increases. Of course, with such a monitoring configuration, monitoring costs will increase as the number of switch output ports increase. Additionally, such hardware-based monitoring techniques lack the flexibility to change as the network characteristics change. For example, although the amount of traffic over certain links may change over time, the configuration of the monitoring systems can be modified only inconveniently by changing the hardware connections or by having a large number of T-connectors and selectively enabling the reception of the ports in the promiscuous monitor.

SUMMARY OF THE INVENTION

The present invention utilizes multicasting within a switch to promiscuously monitor a switched communication network at a single point in the network. At least one port per switch is established as a monitor port, where the switch has sufficient capacity to allow the port to be used for monitoring. The switch comprises input ports, data output ports, and monitor output ports. An interconnection network within the switch is connected to the input ports, the data output ports, and the monitor output port. The interconnection network routes data packets from input ports to data output ports and routes copies of the data packets to the monitor output port. A monitor processor is connected to the switch at the monitor output port to receive copies of data packets received at the switch, and thereby monitor the communication network. The promiscuous monitor can receive copies of all data packets received at the switch

or receive copies of just a selective set of data packets received at the switch.

In another embodiment of the present invention, the switch routes copies of the data packets from some of the input ports or output ports to one monitor output port and routes copies of the data packets arriving at the remaining input ports or output ports, respectively, to another monitor output port. The present invention can also allow modification of which input ports' or output ports' data packet copies are routed to which monitor output ports. Of course, the present invention can be configured with more than two monitor output ports.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a prior art approach for promiscuous monitoring of a communication network.

Fig. 2 shows a wide area network illustrative of the configuration and operation of a contemporary communications network.

Fig. 3 illustrates a switch and promiscuous monitor according to an embodiment of the present invention.

Fig. 4 illustrates a multicasting routing methodology to perform promiscuous monitoring within the switch shown in Fig. 3.

Figs. 5A and 5B shows a switch with multiple monitor output ports according to a second embodiment of the present invention.

Fig. 6 shows a switch with multiple monitor output ports and output port-based monitoring according to a third embodiment of the present invention.

DETAILED DESCRIPTION

Networks are a principal means of exchanging or transferring information (e.g., data, voice, text, video, etc.) among communications devices (i.e., devices for inputting and/or outputting information such as computer terminals, multimedia workstations, fax machines, printers, servers, telephones, videophones, etc.) connected to the network(s). A network typically

comprises switching nodes connected to each other, and to communication devices, by links.

Fig. 2 shows a wide area network illustrative of the configuration and operation of a contemporary communications network. Network 10 comprises a plurality of switching nodes 20 and links 30. Each of the switching nodes 20 may also have associated therewith a buffer of predetermined size and each of the links 30 will have associated therewith a predetermined traffic handling capacity. Note that the depiction of a network comprising only five switching nodes is for convenience of illustration, and that an operating network may have a much larger number of switching nodes and associated connecting links.

Various switching nodes are shown illustratively connected to communications devices 40. It should be understood that the single communications devices shown connected to the switching nodes in the figure are used for simplicity of illustration, and that an actual implementation of such a network would ordinarily have a number of communications devices connected at such switching nodes. Note, as well, that the illustrated communications devices may also represent another network, such as a LAN, which is connected to network 10.

Each communications device 40 generates information for use by, or receives information from, other communications devices in the network. The term "information" as used herein is intended to include data, text, voice, video, etc. Information from communications device 40 is characterized by a set of transmission and/or rate parameters related to network link and buffer requirements needed to accommodate transmission of such information. Control information can be communicated from communication device 40 to a switch at switching node 20 to specify the rate/buffer requirements.

Communications networks will often use a networking protocol called Asynchronous Transfer Mode (ATM). In these networks, all communication at the ATM layer is in terms of fixed-size information segments, called "cells"

in ATM terminology. An ATM cell consists of 48 bytes of payload and 5 bytes for the ATM-layer header. Routing of cells is accomplished through cell switches. Packets of information may be broken up (or segmented) into multiple cells, each cell carrying the 48 bytes of information sequentially. The destination reassembles the cells received into the original packet.

ATM cells can be carried on a virtual circuit (VC) that must be set up such that received cells can be routed to multiple ports at a switch. Permanent VC connections can be easily set up through switch management; switched VC connections, however, need to be set up on a more dynamic basis.

Fig. 3 illustrates a switch and promiscuous monitor according to an embodiment of the present invention. As shown in Fig. 3, switch 200 has three input ports, three data output ports, and a monitor output port. Although switch 200 shown in Fig. 3 has a certain number of ports for illustrative purposes, the present invention is equally applicable for any switch having any number of ports.

Input links 201, 202 and 203 are connected to switch 200 at input ports 1, 2 and 3, respectively, which are connected to interconnection network 210. Interconnection network 210 is connected to data output ports 1, 2 and 3. Output links 221, 222 and 223 are connected to data output ports 1, 2 and 3, respectively. Interconnection network 210 is also connected to monitor port 1 which is connected to promiscuous monitor processor 230.

Interconnection network 210 routes data packets received at an input port to the appropriate destination data output port(s). The number of input ports and/or output ports for switch 200 can exceed the number of links of the network connected to switch 200. Additional output ports therefore are available for connecting one or more promiscuous monitors. In addition to switching communication data packets between the input ports and the data output ports, interconnection network 210 also

routes a copy of data packets received at each input port or output port to the monitor output port 1 through the use of known point-to-multipoint multicasting techniques within a single switch. Point-to-multipoint multicasting is the routing of a single message to multiple recipients. Typically, multicasting is utilized to allow a single sender to transmit a message, through the various switches of a network, to multiple senders connected to the network at various locations. To support such multicasting, switches incorporate internal mechanisms to multicast incoming data to more than one output port; at least one of these additional output ports can then act as a monitor port. The present invention takes advantage of this multicasting capability of the network by treating traffic on each input port of the switch as being from a sender which has receivers downstream on more than one output port. Thus, by multicasting within the switch, the network data traffic that passes through this switch can be promiscuously monitored.

Fig. 4 illustrates a multicasting routing methodology to perform promiscuous monitoring within the switch shown in Fig. 3. As a data packet is received at input port 2, interconnection network 210 routes the data packet to the destination data output port, for example, data output port 1; this is represented in Fig. 4 as a dotted line. Interconnection network 210 also routes a copy of the data packet to monitor output port 1; this is represented in Fig. 4 as a solid line. Similarly, as a data packet is received at input port 1, interconnection network 210 routes the data packet to the destination data output port, for example, data output port 3; this is represent in Fig. 4 as a dotted line. Interconnection network 210 also routes a copy of the data packet to monitor output port 1; this is represented in Fig. 4 as a solid line. Although not shown in Fig. 4, interconnection network 210 routes each data packet received at each input port to the appropriate destination data output port(s), while also routing a

copy of all data packets or routing a selective set of data packets to monitor output port 1.

In a second embodiment of the present invention, multiple monitor output ports are connected to the switch. By configuring the switch with multiple monitor output ports, the present invention can perform load balancing to better distribute the data packets copied for promiscuous monitoring among multiple monitor output ports. Thus, if certain input ports receive more communication data traffic than other input ports, the task of promiscuously monitoring these input ports having heavy communication traffic can be divided among the various monitor processors connected to the various monitor output ports of the switch. A similar function can be used to balance the load among output ports as well. Therefore, no one monitor processor is disproportionally monitoring more communication data than the other monitor processors.

Figs. 5A and 5B shows a switch with multiple monitor output ports according to the second embodiment of the present invention. Switch 300, as shown in Figs. 5A and 5B, has three input ports, three data output ports and two monitor output ports. Fig. 5A illustrates a configuration where as a data packet is received at input port 1 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor output port 2. Also shown in Fig. 5A, as a data packet is received at either input port 2 or input port 3 and forwarded to the proper destination output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor output port 1. The routing of the data packet copies to the monitor output ports are shown in Fig. 5A as solid lines.

Fig. 5B illustrates an alternative configuration where as a data packet is received at either input port 1 or input port 2 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor

output port 2. Also shown in Fig. 5B, as a data is received at input port 3 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the packet to monitor output port 1.

In a third embodiment of the present invention, the multicasting can be based on the data packets having been forwarded to output ports, rather than the data packets received at input ports as was the case with Figs. 4, 5A and 5B. Fig. 6 shows a switch with multiple monitor output ports and output port-based monitoring according to the third embodiment of the present invention. Switch 400, as shown in Fig. 6, has three input ports, three data output ports and two monitor output ports. As a data packet is received at input ports 1 and 2, interconnection network 410 routes a copy of the data packet to destination data output port 1; this is represented in Fig. 6 as dotted lines. Interconnection network 410 also routes a copy of the data packet to monitor output port 2; this is represented as solid lines. Similarly, as a data packet is received at input ports 1 and 3, interconnection network 410 routes a copy of the data packet to destination data output port 3; this is represented as dotted lines. Interconnection network 410 also routes a copy of the data packet to monitor output port 2; this is represented in Fig. 6 as solid lines.

In embodiments of the present invention having multiple monitor output ports, the characteristics of the interconnection network controlling the routing of data between input ports and monitor output ports can be modified as the traffic patterns of the connected links change over time. Modifications to the interconnection network can be performed easily because the routing of data is controlled through software rather than through the hardware configurations of the prior art, such as optical splitters, which are comparatively inflexible.

It should, of course, be understood that while the present invention has been described in reference to

switches having particular characteristics, switches of other characteristics should be apparent to those of ordinary skill in the art. For example, the switch can have any number of input ports, data output ports and monitor output ports. Similarly, any number of promiscuous monitor processors can be connected to the switch on monitor output ports, or in other words, output ports not being utilized. The present invention is equally applicable for any type of switch, such as an input-buffered switch, output-buffered switch and shared-memory switch.

What is claimed is:

1. A switch, within a switched communication network, for enabling promiscuous monitoring, comprising:

a plurality of input ports including a first input port, said plurality of input ports receiving a plurality of data packets including a first data packet and a second data packet;

a plurality of data output ports including a first data output port and a second data output port;

a first monitor output port; and

an interconnection network connected to i) said plurality of input ports, ii) said plurality of output ports, and iii) said first monitor output port, said interconnection network routing the first data packet from the first input port to the first data output port, said interconnection network routing a copy of the first data packet to said first monitor output port.

2. The switch of claim 1, wherein a copy of each data packet of the plurality of data packets is routed to said first monitor output port.

3. The switch of claim 1, wherein a copy of a subset of the plurality of data packets is routed to said first monitor output port.

4. The switch of claim 1, wherein said interconnection network routes a copy of each data packet received at the first input port to said first monitor output port.

5. The switch of claim 1, wherein said interconnection network selects a subset of the plurality of data packets received at the first input port and routes a copy of the subset to said first monitor output port.

6. The switch of claim 5, wherein said interconnection network selects the subset on a dynamic basis.

7. The switch of claim 5, wherein said interconnection network selects the subset on a virtual circuit basis.

8. The switch of claim 1, wherein said interconnection network routes to said first monitor output port a copy of each data packet forwarded to the first data output port.

9. The switch of claim 1, wherein said interconnection network selects a subset of the plurality of data packets forwarded to the first data output port and routes a copy of the subset to said first monitor output port.

10. The switch of claim 9, wherein said interconnection network selects the subset on a dynamic basis.

11. The switch of claim 9, wherein said interconnection network selects the subset on a virtual circuit basis.

12. The switch of claim 1, further comprising:

a second monitor output port connected to said interconnection network;

said interconnection network routes the second data packet from the second input port to the second data output port and routes a copy of the second data packet to said second monitor output port.

13. The switch of claim 12, wherein said interconnection network selects a first subset of the plurality of data packets and routes a copy of the first subset to said first monitor output port, said interconnection network selects a second subset of the plurality of data packets and routes a copy of the second subset to said second monitor output port.

14. The switch of claim 13, wherein said interconnection network balances the load between data packets routed to said first monitor output port and data packets routed to said second monitor output port.

15. The switch of claim 13, wherein said interconnection network selects the first subset or second subset on a dynamic basis.

16. The switch of claim 13, wherein said interconnection network selects the first subset or second subset on a virtual circuit basis.

FIG. 1

PRIOR ART

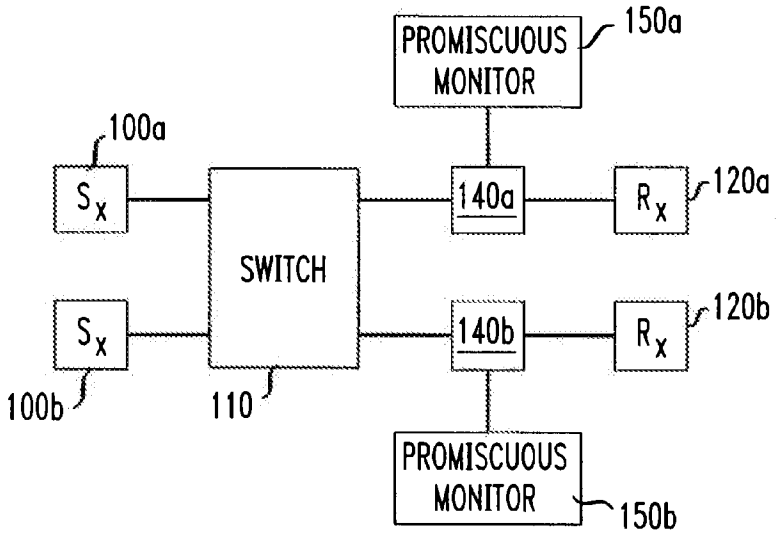


FIG. 2

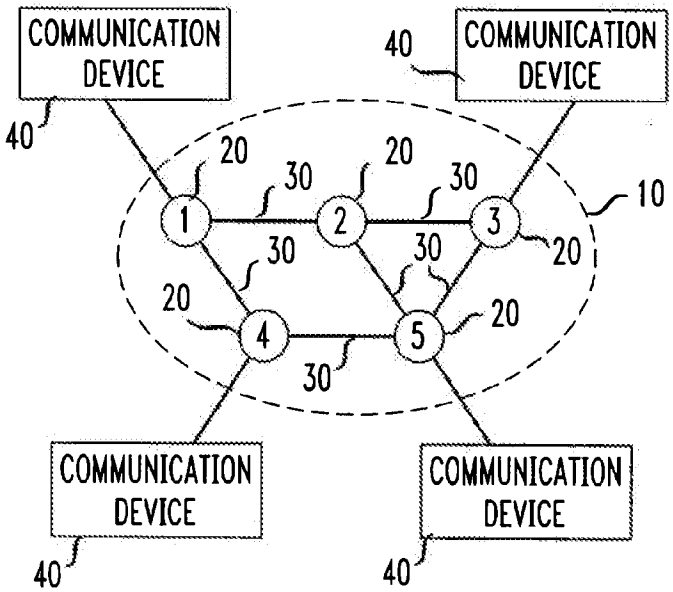


FIG. 3

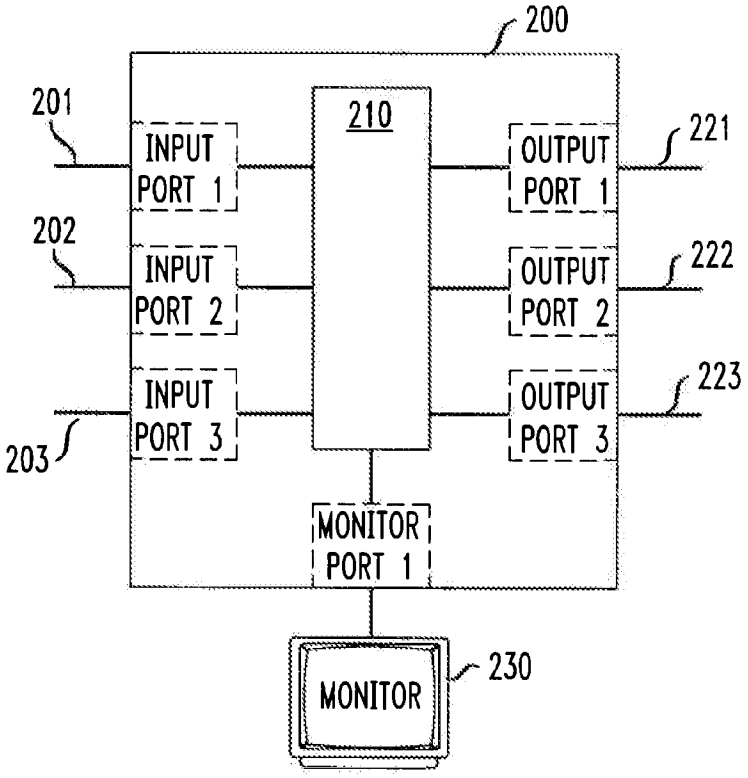

200
201
210
INPUT PORT 1
OUTPUT PORT 1
221
202
INPUT PORT 2
OUTPUT PORT 2
222
INPUT PORT 3
OUTPUT PORT 3
223
203
MONITOR PORT 1
MONITOR
230

FIG. 4

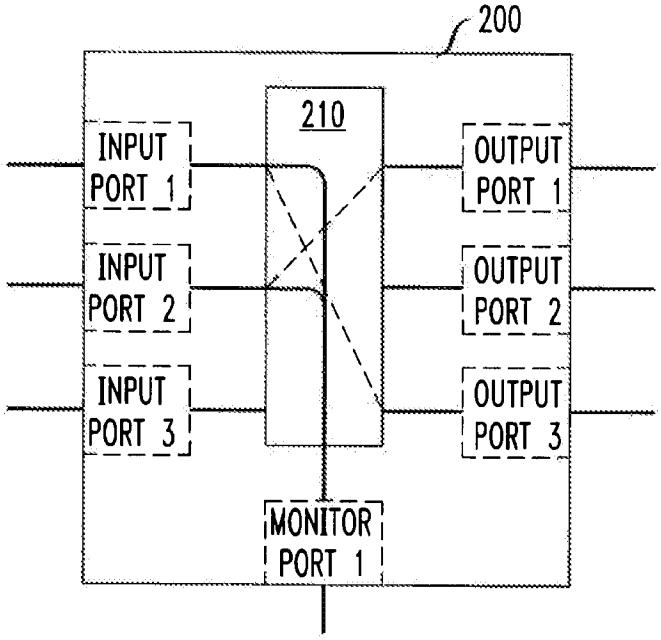

200
210
INPUT PORT 1
OUTPUT PORT 1
INPUT PORT 2
OUTPUT PORT 2
INPUT PORT 3
OUTPUT PORT 3
MONITOR PORT 1

FIG. 5A

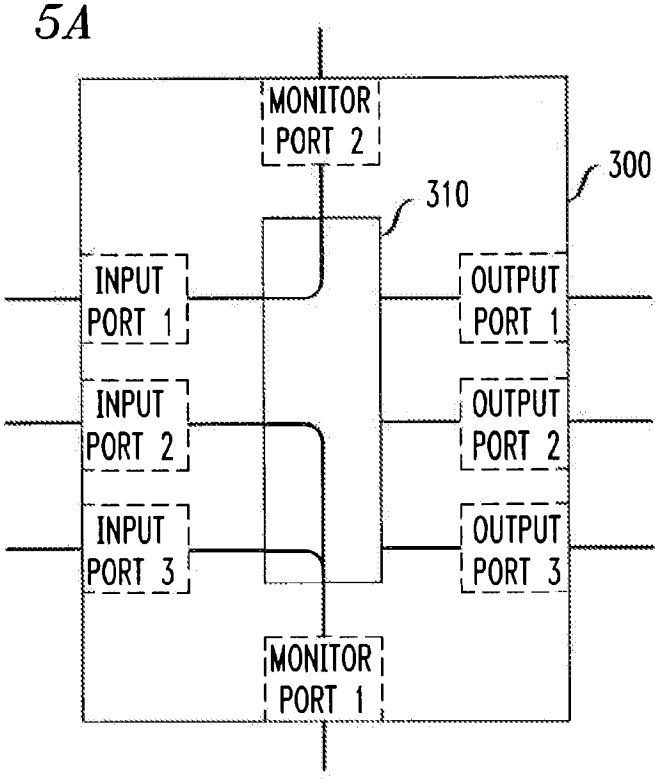

MONITOR PORT 2
300
310
INPUT PORT 1
OUTPUT PORT 1
INPUT PORT 2
OUTPUT PORT 2
INPUT PORT 3
OUTPUT PORT 3
MONITOR PORT 1

FIG. 5B

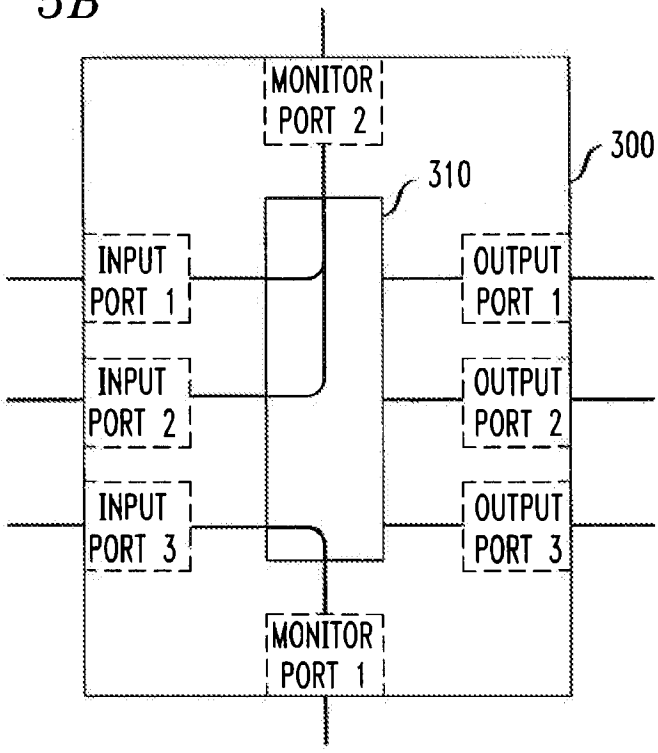
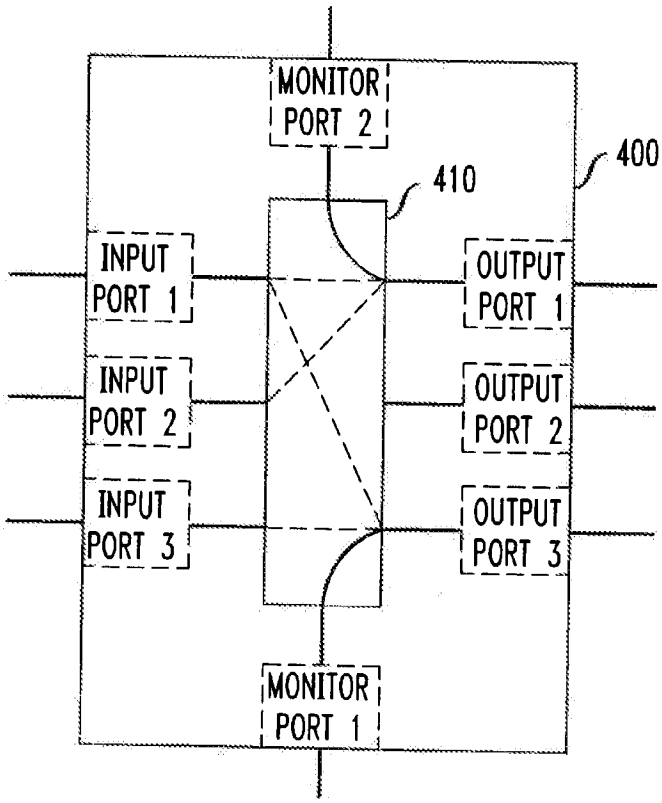

MONITOR PORT 2
300
310
INPUT PORT 1
OUTPUT PORT 1
INPUT PORT 2
OUTPUT PORT 2
INPUT PORT 3
OUTPUT PORT 3
MONITOR PORT 1

FIG. 6


MONITOR PORT 2
400
410
INPUT PORT 1
INPUT PORT 2
INPUT PORT 3
OUTPUT PORT 1
OUTPUT PORT 2
OUTPUT PORT 3
MONITOR PORT 1

(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 299 037 (13) A1

(40) 22.08.2000
(43) 22.08.2000

(12)

(21) 2 299 037

(22) 21.02.2000

(51) Int. Cl.[7]: H04M 003/42, H04M 011/06, H04Q 007/24

(30) 60/120,925 US 22.02.1999

(71) SELEX COMMUNICATIONS, LLC,
3291 Roxboro Road, ATLANTA, XX (US).

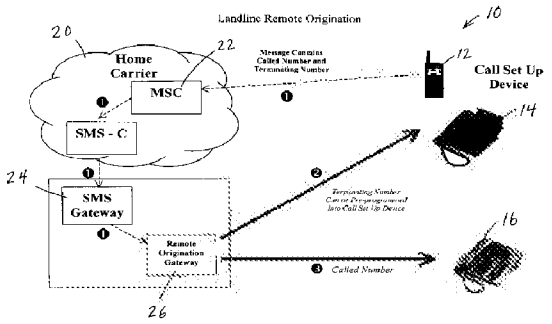
(72) ROACH, PETER O. (US).

(74) GOWLING LAFLEUR HENDERSON LLP

(54) METHODE ET APPAREIL SERVANT A LA PRESTATION D'UN SERVICE TELEPHONIQUE QUASI MOBILE
(54) METHOD AND APPARATUS FOR PROVIDING QUASI-MOBILE TELEPHONE SERVICE

(57)

A telephone system and method allowing a user to set up landline calls using a mobile telephone. A user initiates outgoing calls by inputting into the mobile phone the phone numbers of a remote phone of a called party and a local landline phone convenient for use by the user. A message containing these phone numbers is sent by the mobile telephone to a remote telephone call origination platform, which establishes a bridging connection between the remote phone and the local phone. An incoming call is received by signaling the user of an incoming call on the mobile phone. The user inputs the number of a convenient landline phone into the mobile phone, which in turn signals the remote telephone call origination platform to forward the incoming call to the designated landline phone. The system and method are adaptable to PBX systems. Advantages of both mobile and landline phones are combined, and calling card- like billing/charging can be provided without the inconvenience of inputting calling card numbers and identification codes.



OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

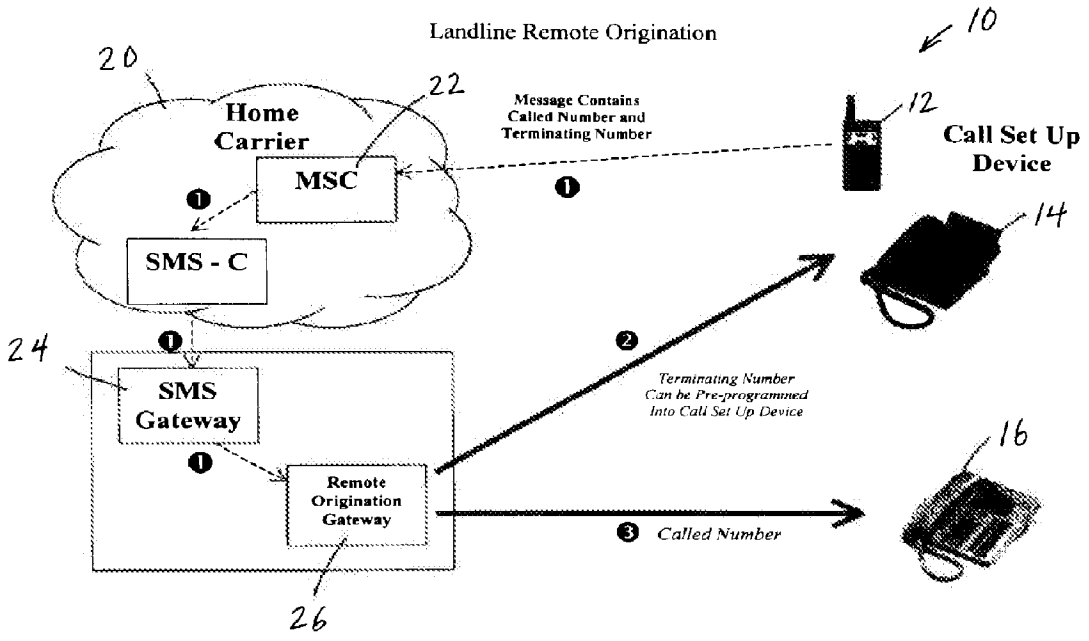
(21) (A1) **2,299,037**
(22) 2000/02/21
(43) 2000/08/22

(72) ROACH, PETER O., US
(71) SELEX COMMUNICATIONS, LLC, US

(51) Int.Cl.[7] H04M 3/42, H04Q 7/24, H04M 11/06
(30) 1999/02/22 (60/120,925) US

(54) **METHODE ET APPAREIL SERVANT A LA PRESTATION D'UN SERVICE TELEPHONIQUE QUASI MOBILE**

(54) **METHOD AND APPARATUS FOR PROVIDING QUASI-MOBILE TELEPHONE SERVICE**



(57) A telephone system and method allowing a user to set up landline calls using a mobile telephone. A user initiates outgoing calls by inputting into the mobile phone the phone numbers of a remote phone of a called party and a local landline phone convenient for use by the user. A message containing these phone numbers is sent by the mobile telephone to a remote telephone call origination platform, which establishes a bridging connection between the remote phone and the local phone. An incoming call is received by signaling the user of an incoming call on the mobile phone. The user inputs the number of a convenient landline phone into the mobile phone, which in turn signals the remote telephone call origination platform to forward the incoming call to the designated landline phone. The system and method are adaptable to PBX systems. Advantages of both mobile and landline phones are combined, and calling card-like billing/charging can be provided without the inconvenience of inputting calling card numbers and identification codes.

ABSTRACT

A telephone system and method allowing a user to set up landline calls using a mobile telephone. A user initiates outgoing calls by inputting into the mobile phone the phone numbers of a remote phone of a called party and a local landline phone convenient for use by the user. A message containing these phone numbers is sent by the mobile telephone to a remote telephone call origination platform, which establishes a bridging connection between the remote phone and the local phone. An incoming call is received by signaling the user of an incoming call on the mobile phone. The user inputs the number of a convenient landline phone into the mobile phone, which in turn signals the remote telephone call origination platform to forward the incoming call to the designated landline phone. The system and method are adaptable to PBX systems. Advantages of both mobile and landline phones are combined, and calling card-like billing/charging can be provided without the inconvenience of inputting calling card numbers and identification codes.

METHOD AND APPARATUS FOR PROVIDING QUASI-MOBILE TELEPHONE SERVICE

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of U.S. Provisional Patent Application Serial No. 60/120,925, filed February 22, 1999, the entire scope and content of which is hereby incorporated herein by reference.

TECHNICAL FIELD

The present invention relates generally to telephone systems and related telephone service methods and apparatus, and in particular relates to a system and method combining features and advantages of mobile telephone, landline telephone, and calling card telephone systems and methods.

BACKGROUND OF THE INVENTION

Currently, in many areas of the world there is limited competition in local, long distance, and international long distance telephone service. This limited competition may be due to several causes, such as regulatory constraints, exclusive concessions of the public switched telephone networks, the high cost of service a widely disbursed population in some locations, etc. In most instances, limited competition causes the local, long distance, and/or international long distance rates to the subscriber to be substantially higher than exist in competitive markets.

In a number of these areas around the world, there exists a local cellular carrier that competes with the local (landline) service provider. Oftentimes, these cellular carriers compete for a higher tier service (customers who can pay a higher cost) by providing mobility to the customer. Many of these cellular carriers desire to offer service to lower tier customers (customers with rather limited financial means). However, the higher cost of the infrastructure for cellular carriers and/or the restricted capacity of voice channels on cellular networks limit the ability of the cellular carriers to effectively reach these lower tier customers.

In the past, cellular carriers have attempted several methods to reach this lower tier customer group. Cellular carriers have used, for example, pricing packages that offer free air time during off-peak hours, pre-paid services, or restricted use packages (e.g. no roaming, inbound calling only, etc.) Most of these promotional techniques have met with limited success in attracting the lower tier customer groups. This is mainly due to the limited functionality of these cellular service packages as well as the continued high cost of the infrastructure required to offer such services. Thus, it has been found that a need exists for improved systems and methods of providing telephone service combining the lower rates typical of landline service with the mobility of cellular service.

In addition, it has been found that many mobile cellular telephone users prefer to use a standard landline telephone when available, rather than a mobile phone. This preference can be due to actual or perceived differences in connection quality or service reliability, lower cost, or certain additional features provided by landline service as compared to mobile service. Also, many users prefer to use landline service provided through a private branch exchange ("PBX") system or switchboard, when available. Because many users store frequently called telephone numbers in the memory of their mobile phones, however, it would be desirable to permit a user to utilize the automatic dialing features and stored number menus of their mobile phone when placing a call over a landline phone.

Many users also find it desirable to place calls utilizing a calling card, which may be a prepaid calling card or a periodically billed calling card. These calling cards permit users to take advantage of more favorable rates and/or consolidated billing for calls originated from different mobile and/or landline telephones. The use of a calling card, however, is often inconvenient as the user typically must input a calling card number and personal identification number ("PIN") when placing a call for billing, identification and fraud-prevention purposes. Many times, a calling card user must also dial a service provider access number to originate a calling card call. It would be desirable to provide a system and method enabling users to obtain the benefits of calling card calling without suffering the disadvantages and inconveniences typically related thereto.

Accordingly, it can be seen that a need yet remains for a method and apparatus for providing telephone service that is similar or in some ways comparable to mobile telephone service, but which can be provided at substantially lower cost. There is also a need for a system and method permitting a user to utilize memory and other features of a mobile phone to set up a landline call. In addition, a need remains for a system and method for providing calling card-like features without a number of the inconveniences typically found to result from the use of a calling card. It is to the provision of a method, system and associated apparatus meeting these and other needs that the present invention is primarily directed.

SUMMARY OF THE INVENTION

Briefly described, in a first preferred form the present invention comprises a method for providing quasi-mobile telephone service using a mobile telephone, a data network, and a Remote Telephone Call Origination ("RTCO") platform. The mobile telephone is of the type which is capable of communicating with the data network. The method includes the steps of using the mobile telephone to dial a first telephone number and a second telephone number. The first and second telephone numbers are captured by the mobile telephone and are transmitted in a data message to a data network. The data message is relayed from the data network to the RTCO platform. The RTCO platform places a first call from the RTCO platform to the first telephone number. RTCO platform also places a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

Preferably, the mobile telephone uses short messaging for communicating with the data network.

Stated another way, preferably a cellular telephone is modified and is specially programmed to allow the user to specify not only the call (destination) telephone number (the first telephone number), but also the calling (origination) telephone number of a convenient, nearby landline phone. The mobile telephone is programmed to originate a short message containing the calling number and the called number. This short message is transmitted to a platform that is programmed to originate a call to the

calling telephone number (such as a nearby landline phone) that was specified by the user. The platform is programmed to originate another call to the called telephone number specified by the subscriber. The platform is programmed to connect (bridge) the two calls together in order to allow the call to be completed. This allows the user to use the cellular telephone to setup and initiate a call, and then to use a standard (lower cost) landline telephone to actually complete the voice path of the call.

In another aspect, the present invention comprises a system for providing communication between a local device and a remote device. The system preferably includes an initiating device for receiving an input identifier of the remote device, and communicating a message containing the identifier of the remote device to a telecommunications network. The system preferably also includes remote telephone call origination means for receiving the message containing the identifier of the remote device from a telecommunications network, and for effecting a bridging connection between the local device and the remote device.

In still another aspect, the present invention comprises a system for providing communication between a remote device and a local device. The system preferably includes remote telephone call origination means for receiving an incoming call from the remote device over a telecommunications network and for communicating a message to announce the incoming call to an initiating device. The initiating device preferably includes means for inputting an identifier of the local device and communicating a message containing the identifier of the local device to the remote telephone call origination means. The remote telephone call origination means preferably receives the message containing the identifier of the local device and effects a bridging connection between the local device and the remote device.

In another aspect, the present invention comprises a method of establishing communication between a local device and a remote device. The method preferably includes inputting an identifier of the remote device into an initiating device, communicating a message containing the identifier of the remote device via a telecommunications network to a remote telephone call origination means, and effecting a bridging connection between the local device and the remote device.

In yet another aspect, the present invention comprises a method for providing communication between a remote device and a local device. The method preferably includes receiving an incoming call from the remote device, via a telecommunications network, into a remote telephone call origination means. The method preferably also includes communicating a message to announce the incoming call to an initiating device, inputting into the initiating device an identifier of the local device, and communicating a message containing the identifier of the local device to the remote telephone call origination means, whereby a bridging connection can be effected between the local device and the remote device.

In another aspect, the present invention comprises a method of charging for the cost of a telephone call. The method preferably includes initiating a telephone call between a local device and a remote device using an initiating device, communicating a message containing information identifying the initiating device to a communications network, effecting a bridging connection between the local device and the remote device, and collecting billing information regarding the telephone call and charging at least a portion of the cost of the communication to an account associated with the initiating device.

By allowing the user to setup and initiate the call using a cellular network and to actually complete the call using standard Public Switch Telephone Network ("PSTN"), the user can have the benefits of both technologies. It provides the user with substantial mobility similar to a cellular service, while allowing the user to enjoy the lower cost and dependable voice transmission over the public switch telephone network.

The system and method of the present invention also advantageously enables a user to utilize the automatic calling menus, memory-stored telephone number registers and other features of their cellular mobile phones when placing (and/or receiving) calls over a landline phone, including a PBX or switchboard connected landline phone. For example, the user can remotely originate a landline telephone connection using their mobile phone, taking advantage of any automatic calling menus, memory-stored telephone number registers or other features available through the mobile phone.

The system and method of the present invention can also function as a "Virtual Calling Card," whereby the user obtains many benefits typically associated with a standard calling card without suffering many of the typical disadvantages and inconveniences of a calling card. Because the landline connection is remotely originated though a cellular mobile phone, the caller's identity can be automatically validated through the carrier's home location register ("HLR") prior to completing the landline connection. This eliminates the need for the caller to input a calling card number and PIN with every call. The user can establish service with one or more carriers of their choice to obtain the rate structure and service plan best suited to their needs. The user's calls can be billed to the customer in a single statement, regardless of the point of connection.

The system and method of the present invention eliminate the need for the carrier to maintain a dedicated toll-free access network to offer "calling card" type services. The carrier can also select the most cost-effective location worldwide to originate telephone calls. As a result, carriers can pass along their savings to users in the form of lower rates, and/or can increase profit margins. In addition, the present invention allows cellular carriers to obtain revenue from landline calling.

In use, a user would take advantage of the method and apparatus of the present invention by keeping his mobile telephone with him as he moves from place to place. When the user wants to place a call from his current location, he would find a convenient, nearby landline telephone and determine its telephone number. The user would then dial the destination telephone number and the nearby landline telephone number into the mobile telephone. The mobile telephone would then transmit this information in a message and ultimately the RTCO platform would call both the destination telephone number and the convenient, nearby landline telephone and connect the two calls together. In this way, the user could use a nearby landline telephone to complete a call, and have the charges routed to his own personal account, even though the landline telephone is not his telephone. For example, the landline telephone may be a public pay phone, a hotel phone, or another person's phone. In addition to allowing a user to move about and use whatever telephone is nearby and convenient, this method and apparatus allows multiple users to share a single landline

telephone and each user to have his or her own account for charging or billing purposes. For example, migrant workers who are living temporarily in migrant housing could use an available "house" landline telephone and share the telephone, with each migrant worker having his or her own phone account. This would allow a large number of people to effectively share a telephone. Moreover, as the migrant worker would move from one job location to another, they would still have continuous, uninterrupted telephone service by virtue of the quasi-mobile service provided herein.

The present invention is also useful for receiving an incoming telephone call, whereby an incoming telephone call is re-routed from the user's mobile telephone to instead be directed to a nearby landline telephone. The cellular telephone is modified to be specially programmed to allow the phone to receive a data message (such as the standard ring command for cellular telephones) to indicate that there is an inbound call being attempted. The mobile telephone would then prompt the user to key in (input) the desired destination telephone number of a convenient, nearby landline phone. The mobile telephone would then put together a data message and communicate it (such as by using the short message service ("SMS") capabilities of the global system for mobile communications ("GSM") network) containing at least a destination telephone number of the nearby landline telephone that the user desires to receive the incoming telephone call with and identifying the called number. The data message is then routed to a platform that would receive the incoming call and the outbound call to the mobile telephone. The platform would be programmed to bridge these calls together to form a complete conversation.

While the present invention preferably uses a data network to relay messages from the mobile telephone to the RTCO platform, those skilled in the art will recognize that it is possible to have the mobile telephone communicate directly with the RTCO platform. Moreover, while a mobile telephone is preferred for initiating and rerouting calls (largely because of the widespread availability and low cost of such devices), those skilled in the art will also recognize that other devices could be employed to initiate and reroute calls. U.S. Patent No. 5,546,444 of *Roach, et al.*, which is hereby incorporated herein by reference, discloses a way in which a control channel of a cellular mobile telephone can be used communicate data.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic illustration depicting a method and system for providing quasi-mobile telephone service according to a preferred form of the present invention, and specifically depicting the remote origination of telephone calls thereby.

Fig. 2 is a flow chart depicting the origination of telephone calls using the method and system of the present invention.

Fig. 3 is a schematic illustration of a method and system for providing quasi-mobile telephone service according to a preferred form of the present invention, and specifically depicting termination of an incoming telephone call.

Fig. 4 is a flow chart depicting the termination of telephone calls using the method and system of the present invention.

Fig. 5 is a schematic illustration of a method and system, according to a preferred form of the present invention, for establishing a telephone connection between a calling phone connected to a PBX or switchboard and a called phone, using a mobile phone to establish the connection.

Fig. 6 is a schematic illustration of a method and system, according to another preferred form of the present invention, for providing calling card-like calling features when placing a call between a calling phone and a called phone using a mobile phone to establish the connection.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Referring now to the drawing figures, in which like reference numerals represent like parts throughout, the present invention comprises a method and system 10 for providing quasi-mobile telephone service, using an initiating device 12 to establish a connection between a local device 14 and a remote device 16. The system of the present invention preferably comprises one or more computers and associated software for controlling the operation and switching according to the manner described herein. The associated software can be programmed into the memory of the computer or can be stored in a computer-readable medium according to known techniques. The method and system 10 preferably combine many of the advantages typical of one or the other

of mobile or landline telephone service, while eliminating many of the disadvantages of each. Particular embodiments and applications of the method and system of the present invention are described in greater detail below. Although the present invention is described herein primarily with reference to example embodiments directed to voice transmission applications conducted between telephones, it will be understood that the present invention is equally applicable to data transmission applications conducted between data transmission devices such as, for example, fax machines, computer modems, or the like.

In a preferred form of the present invention, described with particular reference to Figs. 1 and 2, a user (in this instance, the "calling party") utilizes a portable call initiating device 12 to establish a connection between a local (i.e., accessible for use by the caller) device 14 and a remote device 16. In preferred embodiments, the call initiating device 12 comprises a mobile cellular telephone or another device capable of receiving and sending signals to and from a remote location, the local device 14 comprises a local PSTN landline telephone in the vicinity of the calling party, and the remote device 16 comprises a landline or mobile telephone available to a remote party (in this instance, the "called party"). To initiate an outgoing call using the method and system of the present invention, the calling party (or a third party initiating the call) preferably enters the telephone number or other unique identifier of the remote phone 16 on the mobile phone 12, as by using the mobile phone's keypad or a menu of phone numbers stored in the mobile phone's memory. The telephone number or other unique identifier of the local phone 14 is optionally entered by the calling party into the mobile phone 12, or can be stored in the memory of the mobile phone for automatic transmission upon initiation of a call. Alternatively, a default local phone number can be associated with the calling party on the calling party's home carrier network, the remote origination gateway, or elsewhere in the system. If a default local phone number is provided, the system can be configured to allow the calling party to override the default by inputting an override local phone number, or alternatively can require that all calls be conducted from the default local phone for security or other reasons. The mobile phone 12 formats a message including data identifying the remote number and optionally the local number, and transmits the message according to a standard electronic data communication protocol to an existing telecommunications network,

such as a cellular telephone network. The message can be directly transmitted to the calling party's home cellular carrier network 20 or indirectly transmitted via a visited cellular carrier through one or more mobile switching centers ("MSCs") 22. The message preferably is transmitted over the network 20 using GSM SMS messaging. In a preferred form, the message is transmitted from the carrier network 20, preferably via an SMS gateway 24, to a remote origination gateway 26 comprising the RTCO platform. An SS7 message box is preferably provided, and the gateway is capable of originating voice and/or data telephone calls. The remote origination gateway 26 places a call to the local phone 14. A timer can be utilized to terminate the connection if the local phone 14 is not answered within a predetermined time interval, or if the local phone is busy. The calling party preferably answers the local phone 14, establishing a connection with the remote origination gateway 26. Upon completion of the connection with the local phone, the mobile phone can be disconnected automatically or manually by the calling party. The remote origination gateway 26 also places a call to the remote phone 16, simultaneously with or sequentially before or after the call is placed to the local phone 14. A timer can be utilized to terminate the connection if the remote phone 16 is not answered within a predetermined time interval. The called party preferably answers the remote phone 16, establishing a connection with the remote origination gateway 26. Upon connection with both the local phone 14 and the remote phone 16, the remote origination gateway 26 establishes a bridging connection between the local phone 14 and the remote phone 16, permitting voice or data transmission therebetween. The remote origination gateway 26 preferably monitors the call for disconnect at either the local phone 14 or the remote phone 16, and thereupon terminates the call. The system 10 can be configured for billing purposes to allocate all or a portion of the cost of the call to the account(s) of one or more of the initiating device 12, the local device 14, the remote device 16, and/or one or more third-party payers. According to optional and further preferred embodiments, the remote origination gateway 26 can be configured for conference calling. For example, users of one or more of the initiating device 12, the local device 14, and/or the remote device 16 can input the telephone number(s) or other unique identifiers of one or more additional parties to be conferenced in with the calling party and the called party.

Additionally or alternatively, one or more additional parties can call in to the remote origination gateway 26 to be conferenced in with the calling party and the called party.

Referring now with particular reference to Figs. 3 and 4, the method and system 10 of the present invention can be seen to also enable the connection of an incoming call from a remote party at a remote phone or other remote device 16' (in this instance, the "calling party") to a user (in this instance, the "called party") at the local phone or other local device 14, via the user's mobile phone or other initiating device 12. An incoming call from the remote phone 16', directed to a telephone number or other unique identifier associated with the mobile phone 12 via an existing telecommunications network, is received at the mobile switching center (MSC) 22 of the user's home cellular carrier network 20. The MSC preferably forwards the incoming call to the remote origination gateway 26 on a "call forwarding-don't answer" ("CFDA") basis, connecting the remote phone 16 with the remote origination gateway 26. The remote origination gateway 26 preferably receives the incoming call and places the calling party on hold pending connection with the local phone 14. Live or recorded music or other entertainment, informational messages, advertising or other audible material can be broadcast to the parties while on hold. Simultaneously with or sequentially before or after forwarding the incoming call to the remote origination gateway 26, the MSC announces the call to the called party via the mobile phone 12, typically by means of a ring or other audible, tactile or visual signal, according to standard telecommunications protocol. Preferably, the mobile phone is configured to prevent the user from answering the call on the mobile phone, or is switchable to selectively permit or prevent answering calls on the mobile phone. A timer can be provided to terminate the call if the called party does not respond within a predetermined interval of time. Preferably, the called party acknowledges the incoming call signal and inputs the telephone number or other unique identifier of the local phone 14 to be used for receiving the incoming call, as by using the mobile phone's keypad or the menu of phone numbers stored in the mobile phone's memory. The mobile phone 12 transmits a message containing the local telephone number to be used for receiving the incoming call to the MSC, which signals the remote origination gateway 26 via the SMS gateway to place a call to the local phone 14. Alternatively, a default local phone number associated with the called party is transmitted to the MSC, which signals the remote

origination gateway 26 to place a call to a default local phone 14. As discussed above, the default local phone number can be mandatory or subject to override. The called party then answers the local phone 14 to complete the connection between the local phone and the remote origination gateway 26. Upon connection between the local phone 14 and the remote origination gateway 26, the mobile phone 12 can be automatically or manually disconnected. The remote origination gateway 26 then establishes a bridging connection between the local phone 14 and the remote phone 16, permitting voice or data transmission therebetween. The remote origination gateway 26 preferably then monitors the call for disconnect at either the local phone 14 or the remote phone 16, and thereupon terminates the call. As described above, the system 10 optionally can be configured for conference calling with additional parties.

Figure 5 shows another preferred embodiment of the present invention, wherein the local phone 14 is part of a PBX or other switchboard type of network 50. Preferably, the system, method and components of this embodiment of the invention are substantially as described above, with certain specific additions or modifications that will now be described. The user (in this instance, the "calling party") preferably initiates an outgoing call to a remote user (in this instance, the "called party") using the mobile cellular phone 12. A short message containing information regarding the telephone number of the remote phone 16 and the PBX switchboard 50 containing the user's local phone 14 is transmitted from the mobile phone 12 over a cellular communications network to a location server/messaging server 42. The location server/messaging server 42 communicates with the user's home carrier network 20 and the remote origination switch 26 substantially in the manner described above. The remote origination switch 26 places calls to the remote phone 16 and the PBX switchboard 50 substantially in the manner described above. In addition, the remote origination switch 26 places a temporary call to the mobile phone 12. A temporary bridging connection is established between the mobile phone 12 and the PBX switchboard 50, permitting the user to communicate with the PBX 50, via the mobile phone 12, to connect the call through the PBX to the local phone 14. This connection can be accomplished, for example, by keying in the PBX extension number of the local phone 14 on the keypad of the mobile phone 12 in the case of an automated switchboard; or alternatively, can be accomplished by voice in the case of an operator-answered switchboard. Upon

connection of the local phone 14 to the remote origination switch 26, the temporary call from the remote origination switch to the mobile phone 12 is manually or automatically disconnected. The remote origination switch 26 then completes the bridging connection between the local phone 14 and the remote phone 16 substantially in the manner described above.

Figure 6 shows another preferred embodiment of the method and system of the present invention that is particularly adapted to provide telecommunication services having characteristics in the nature of an enhanced calling card. The user (in this instance, the "calling party") preferably initiates an outgoing call to a remote user (in this instance, the "called party") using the memory menu of the mobile cellular phone 12. A short message containing information regarding the telephone number of the remote phone 16 and the user's local phone 14 is transmitted from the mobile phone 12 over a cellular communications network, via a mobile switching center of a visited cellular carrier 40, to a location server/messaging server 42. In preferred form, the location server/messaging server 42 comprises an SS7-IP gateway. The SS7-IP gateway converts an SS7 message to Internet protocol, and preferably carries out any necessary logic operations. Alternatively, logic operations can be completed on an SS7 box. The user's home carrier network 20 communicates with the location server/messaging server 42 to send routing information and user authorization, and to collect information for billing or charging the call to a prepaid service package. The home location register (HLR) of the home carrier network 20 validates the identity of the calling party according to standard cellular telecommunications fraud-prevention protocol, eliminating the need for the user to key in a calling card number and PIN for every call. In addition, because the call is set up using the existing cellular communications network, the need for a dedicated toll-free access network is eliminated. The location server/messaging server 42 communicates with the remote origination switch 26, which places calls to the local phone 14 and the remote phone 16, and completes the bridging connection between the local phone 14 and the remote phone 16 substantially in the manner described above.

A number of advantages and increased efficiencies are obtained by the present invention. Billing information collected by the user's home carrier network 20 permits

the user to be billed for all calls on a single statement, or permits all calls to be charged to a prepaid service plan, regardless of the locations of the one or more local phones 14 used to complete the calls, in much the same manner as is permitted with calling card systems. Because the connection between the local phone 14 and the remote phone 16 is maintained by the bridging connection provided by the remote origination switch 26, the system and method of the present invention permit a cellular carrier to obtain revenue from what would otherwise be a non-revenue generating, wholly landline connection. Consumers, however, can benefit from rates lower than standard calling card rates for landline connections, as the cellular carrier can route calls and manage billing more efficiently using the method and system of the present invention than is the case with standard landline connections using calling cards. In addition, consumers benefit from increased convenience, as the present invention enables landline calls to be initiated using calling information stored in the memory registers of a mobile phone, and obviates the need for remembering and dialing access numbers, calling card numbers and PINs. The system and method of the present invention also, advantageously, are not reliant on the touch tone quality of the local phone. Some hotels, for example, modify the touch tone signals of room phones to prevent users from using calling cards and thereby require them to pay the hotel's rates for phone connections. The present invention allows the call to be initiated using a mobile phone, bypassing any effect of altered touch tone quality of a local phone within a hotel's PBX network.

According to optional and further preferred embodiments, the system 10 comprises voice mail messaging means, whereby an incoming call is directed to a recording device for recording a message from the calling party for later playback by the called party. The voice mail messaging means is preferably automatically activated in the event that the mobile phone 12 or the local phone 14 are in use at the time of the incoming call. The voice mail messaging means can preferably be selectively activated by the called party by signaling the MSC, via the mobile phone 12, to forward the call to voice mail upon receiving an incoming call signal. The system 10 optionally also comprises caller ID means for identifying the calling party to the called party upon signaling an incoming call on the mobile phone 12, permitting the called party to screen incoming calls.

One unique application of the present invention is the enablement and implementation of a region-wide prepaid service providing significant advantages over existing calling-card systems or prepaid service plans. Since both incoming and outgoing calls are routed through the remote origination platform, a cellular carrier can provide a prepaid service (local, long distance and international long distance) on a region-wide or worldwide basis. This is a significant improvement over the standard prepaid service offered by cellular carriers in that it can be extended beyond the subscriber's local service coverage area. Moreover, with this invention a cellular carrier can prohibit or selectively restrict the use of the cellular voice channels. The carrier can restrict the usage on a time of day basis, originating network basis (restrict roaming capabilities or home zone only capabilities), the input of an access code, etc. The restriction of voice channel capabilities can be remotely programmed using a data channel such as the short message service channel. In this embodiment, the mobile phone or other initiating device 12 functions solely as a control device for the system 10. This capability can be provided on a specially made device or on a standard cellular phone modified with special programming, such as a GSM phone using a subscriber identification module ("SIM") toolkit. The method and system of the present invention advantageously utilize the home location register (HLR) database, or other pre-existing user verification system of a cellular carrier to identify the mobile telephone or other initiating device from which the incoming call to the cellular network is being placed. By identifying the calling party upon receiving an incoming call to the network in this manner, the carrier can confirm that the calling party is an authorized user, collect information for billing and charging purposes, control the terms of connection, and conduct a variety of other operations. For example, the carrier can limit the duration of calls, specify authorized call destinations, limit the time periods during which calls can be placed, specify the types of calls (e.g., voice, data), etc.

The call set-up time for this quasi-mobile service may be slightly longer than standard call set-up times using existing wireless networks. This extra time will most likely result from the necessity of requesting and receiving user input to complete the conversation. A cellular carrier may desire to offer voice announcements during a call set-up. These announcements can be provided either to the originating party or the terminating party during the call set-up.

Once the phone conversation is established through the remote origination gateway (RTCO) it is possible to provide other features through the cellular telephone. These features optionally include advanced call conferencing, call forwarding, special announcements, or any other telephony features. For mobile originated calls it is possible for the cellular carrier to populate the calling line ID field, from the remote gateway, with the telephone number of the user's mobile telephone (i.e., the initiating device 12), the user's home telephone number, or another designated telephone number or identification field, regardless of the location and telephone number of the local phone 14 that is the actual destination of the telephone call used by the calling party to complete the call. This will allow the called party to receive the calling line ID of the calling party, and will allow the calling party to have the appearance of maintaining a consistent telephone number regardless of their location and regardless of the telephone number of the local phone actually used by the calling party. Optionally, the calling line ID of the calling party can be transmitted from the remote gateway to the calling party's local phone 14, as well as the remote phone 16, in order to identify the incoming call to the calling party for call screening purposes.

While the present invention has been described with reference to various preferred embodiments, it will be readily apparent to those of ordinary skill in the art that many additions, deletions and modifications can be made thereto without departing from the spirit and scope of the invention as broadly defined in the claims which follow.

CLAIMS

WHAT IS CLAIMED IS:

1. A method of providing quasi-mobile telephone service using an RTCO platform, a data network, and a mobile telephone of the type capable of communicating with the data network, the method comprising the steps of:

using the mobile telephone to dial a first telephone number and a second telephone number;

capturing the first telephone number and a second telephone number;

transmitting a data message to the data network, with the data message including the first and second telephone numbers;

relaying the data message from the data network to the RTCO platform;

placing a first call from the RTCO platform to the first telephone number; and

placing a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

2. A method as claimed in Claim 1 wherein the mobile telephone uses short messaging for communicating with the data network.

3. A method as claimed in Claim 1 wherein the mobile telephone is used to reroute incoming calls to another telephone by detecting that an incoming call is being placed to the mobile telephone and sending a message to the RTCO platform to redirect the incoming call to the other telephone.

4. A method as claimed in Claim 1 wherein the data network identifies the mobile telephone through a home location register.

5. A method as claimed in Claim 1 wherein the data network transmits caller identification information to at least one of the first and second telephone numbers.

6. A method of providing quasi-mobile telephone service using an RTCO platform and a mobile telephone, the method comprising the steps of:

using the mobile telephone to dial a first telephone number and a second telephone number;

capturing the first telephone number and a second telephone number;

transmitting a data message to the RTCO platform, with the data message including the first and second telephone numbers;

placing a first call from the RTCO platform to the first telephone number; and

placing a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

7. A method as claimed in Claim 6 wherein the RTCO platform identifies the mobile telephone through a home location register.

8. A method as claimed in Claim 6 wherein the RTCO platform transmits caller identification information to at least one of the first and second telephone numbers.

9. A system for providing communication between a local device and a remote device, said system comprising:

an initiating device for receiving an input identifier of the remote device, and communicating a message containing the identifier of the remote device to a telecommunications network;

remote telephone call origination means for receiving the message containing the identifier of the remote device from a telecommunications network, and for effecting a bridging connection between the local device and the remote device.

10. The system of Claim 9, wherein said initiating device comprises a mobile telephone.

11. The system of Claim 10, wherein said local device comprises a landline telephone.

12. The system of Claim 9, wherein said initiating device receives input identifiers of the local device and the remote device and communicates a message containing both identifiers to the telecommunications network, and wherein said remote telephone call origination means receives the message containing both identifiers and effects the bridging connection by calling the local device and the remote device.

13. The system of Claim 12, wherein the telecommunications network identifies the initiating device through a home location register.

14. A method as claimed in Claim 12 wherein the telecommunications network transmits caller identification information to at least one of the local and remote devices.

15. The system of Claim 9, wherein said remote telephone call origination means effects connection of at least one additional device with the local device and the remote device for conference communications.

16. The system of Claim 9, further comprising means for charging at least a portion of the cost of the communication to an account associated with said initiating device.

17. The system of Claim 16, wherein said means for charging at least a portion of the cost of the communication to an account associated with said initiating device comprises means for identifying said initiating device without the need for inputting identification information into said initiating device.

18. The system of Claim 9, wherein said remote telephone call origination means comprises a remote origination gateway.

19. The system of Claim 9, wherein said initiating device further comprises a signaling device for announcing an incoming call from a remote calling device, and means for communicating a message to said remote telephone call origination means containing an identifier of a local receiving device; and wherein said remote telephone call origination means comprises means for effecting a bridging connection between the remote calling device and the local receiving device.

20. The system of Claim 9, wherein the local device is one of a plurality of devices within a network, and wherein said initiating device communicates a message through said remote telephone call origination means to specify the local device and effect said bridging connection.

21. A system for providing communication between a remote device and a local device, said system comprising remote telephone call origination means for receiving an incoming call from the remote device over a telecommunications network and for communicating a message to announce the incoming call to an initiating device, wherein said initiating device comprises means for inputting an identifier of the local device and communicating a message containing the identifier of the local device to said remote telephone call origination means, whereby the remote telephone call origination means receives the message containing the identifier of the local device and initiates a bridging connection between the local device and the remote device.

22. The system of Claim 21, further comprising voice mail messaging means for recording a message from the remote device if the bridging connection is not completed.

23. A method of establishing communication between a local device and a remote device, said method comprising:

inputting an identifier of the remote device into an initiating device;

communicating a message containing the identifier of the remote device via a telecommunications network to a remote telephone call origination means; and

effecting a bridging connection between the local device and the remote device.

24. The method of Claim 23, comprising inputting identifiers of the local device and the remote device into the initiating device, and communicating a message containing both identifiers via the telecommunications network to the remote telephone call origination means.

25. The method of Claim 23, further comprising connecting at least one additional device with the local device and the remote device to establish a conference communication.

26. The method of Claim 23, further comprising collecting billing information regarding the communication and charging at least a portion of the cost of the communication to an account associated with the initiating device.

27. The method of Claim 26, wherein the step of charging at least a portion of the cost of the communication to an account associated with the initiating device comprises identifying the initiating device without inputting identification information into the initiating device.

28. The method of Claim 23, further comprising communicating a message from the initiating device to the remote telephone call origination means to specify the local device among a plurality of devices within a network.

29. The method of Claim 23, further comprising identifying the initiating device through a home location register of the telecommunications network.

30. The method of Claim 23, further comprising transmiting caller identification information to at least one of the local and remote devices.

31. A method for providing communication between a remote device and a local device, said method comprising:

receiving an incoming call from the remote device, via a telecommunications network, into a remote telephone call origination means;

communicating a message to announce the incoming call to an initiating device;

inputting into the initiating device an identifier of the local device; and

communicating a message containing the identifier of the local device to the remote telephone call origination means, whereby a bridging connection can be effected between the local device and the remote device.

32. The method of Claim 31, further comprising recording a message from the remote device on a recording device if the bridging connection is not effected.

33. A method of charging for the cost of a telephone call comprising:

initiating a telephone call between a local device and a remote device using an initiating device;

communicating a message containing information identifying the initiating device to a communications network;

effecting a bridging connection between the local device and the remote device; and

collecting billing information regarding the telephone call and charging at least a portion of the cost of the communication to an account associated with the initiating device.

34. The method of Claim 33, comprising identifying the initiating device via a home location register of the communications network.

Figure 1
Landline Remote Origination

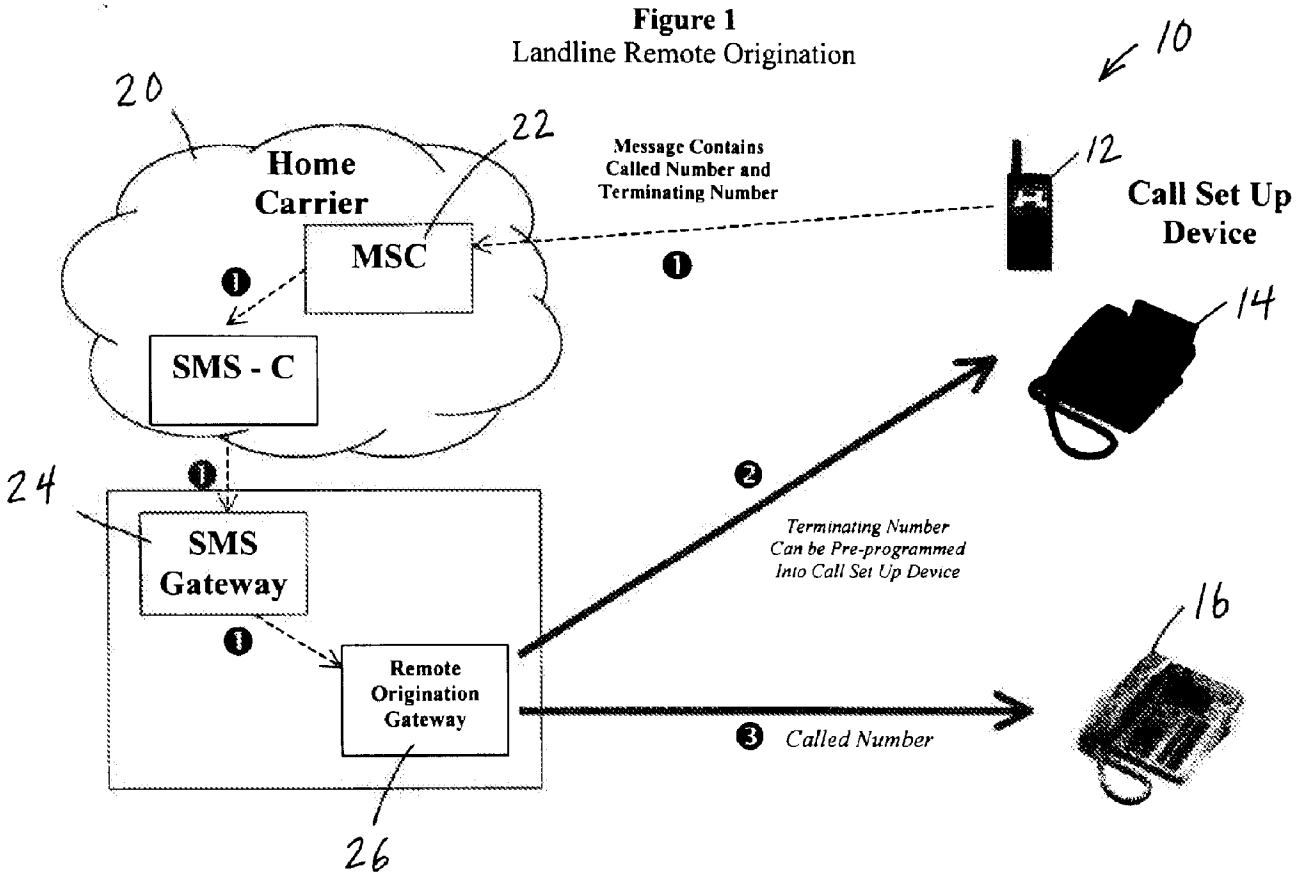


Figure 3
Landline Remote Termination

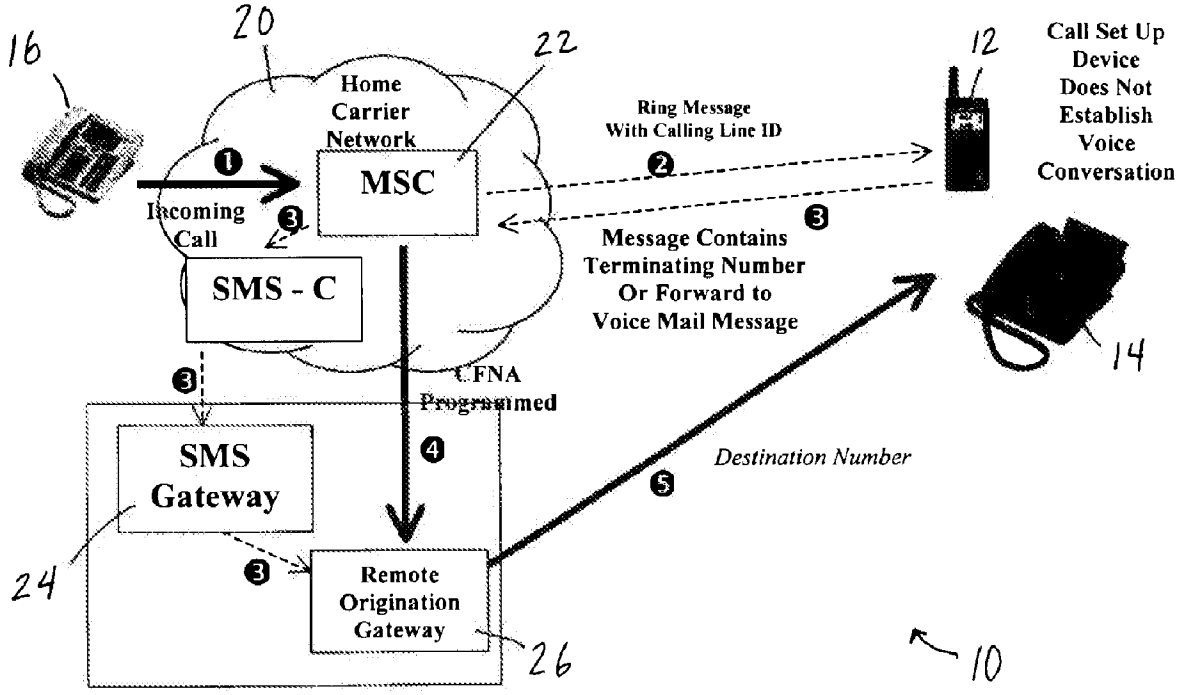


FIGURE 2

(Origination of telephone calls)

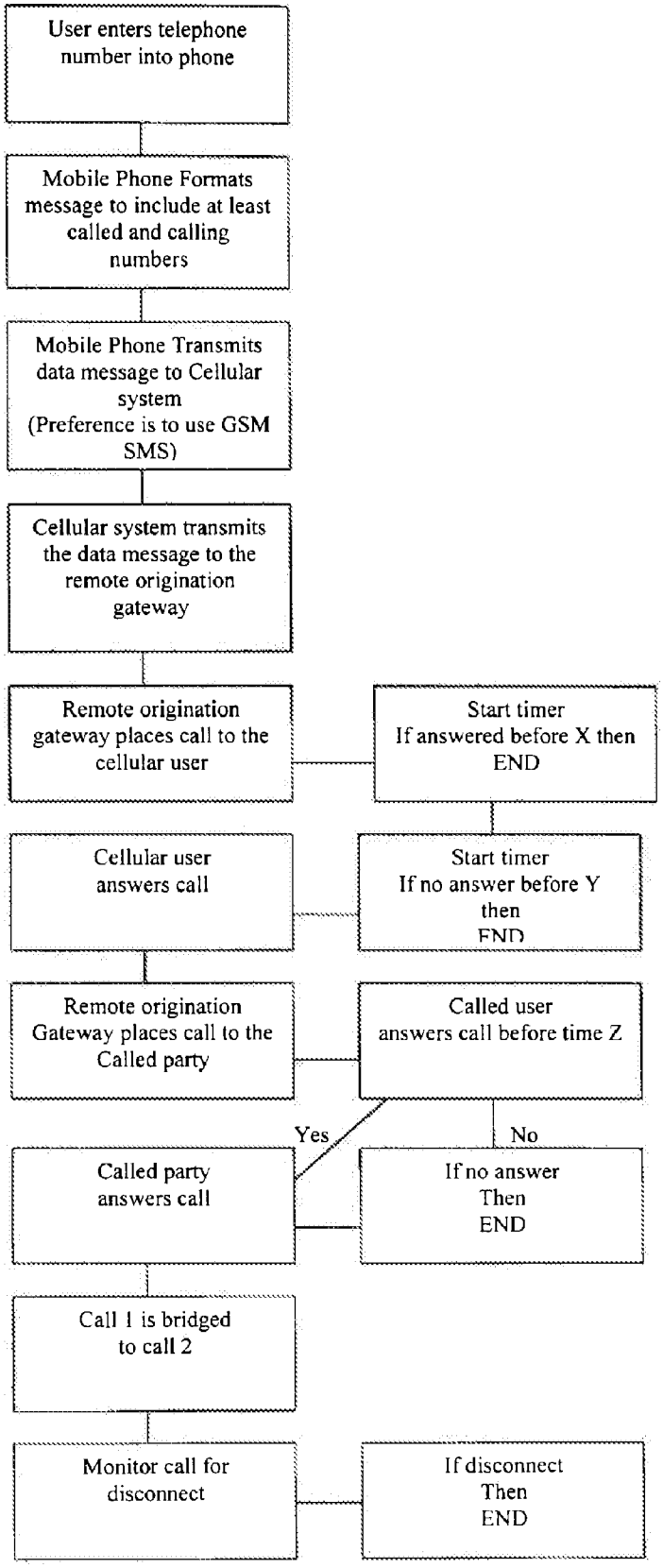


FIGURE 4
(Termination of telephone calls)

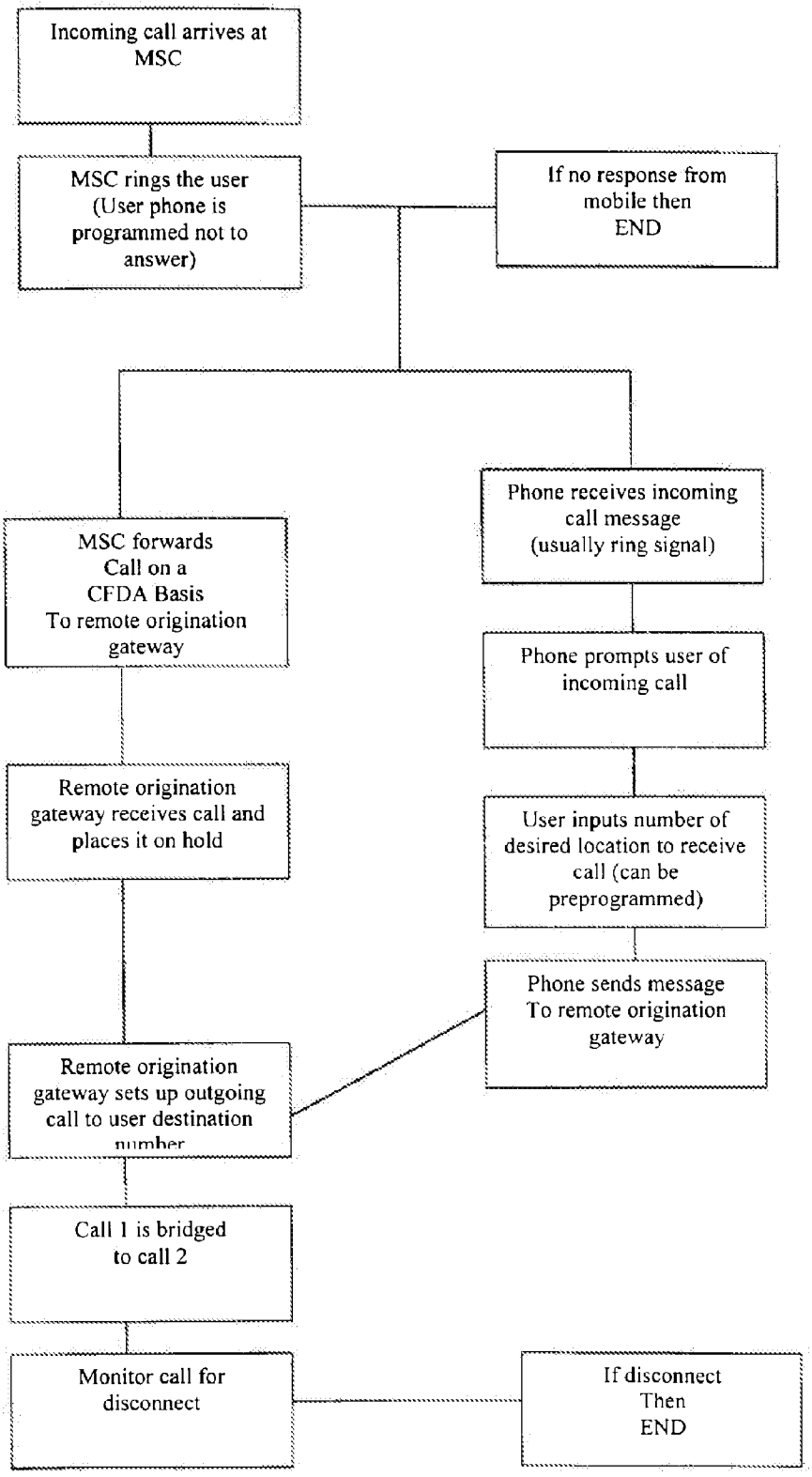


Figure 5

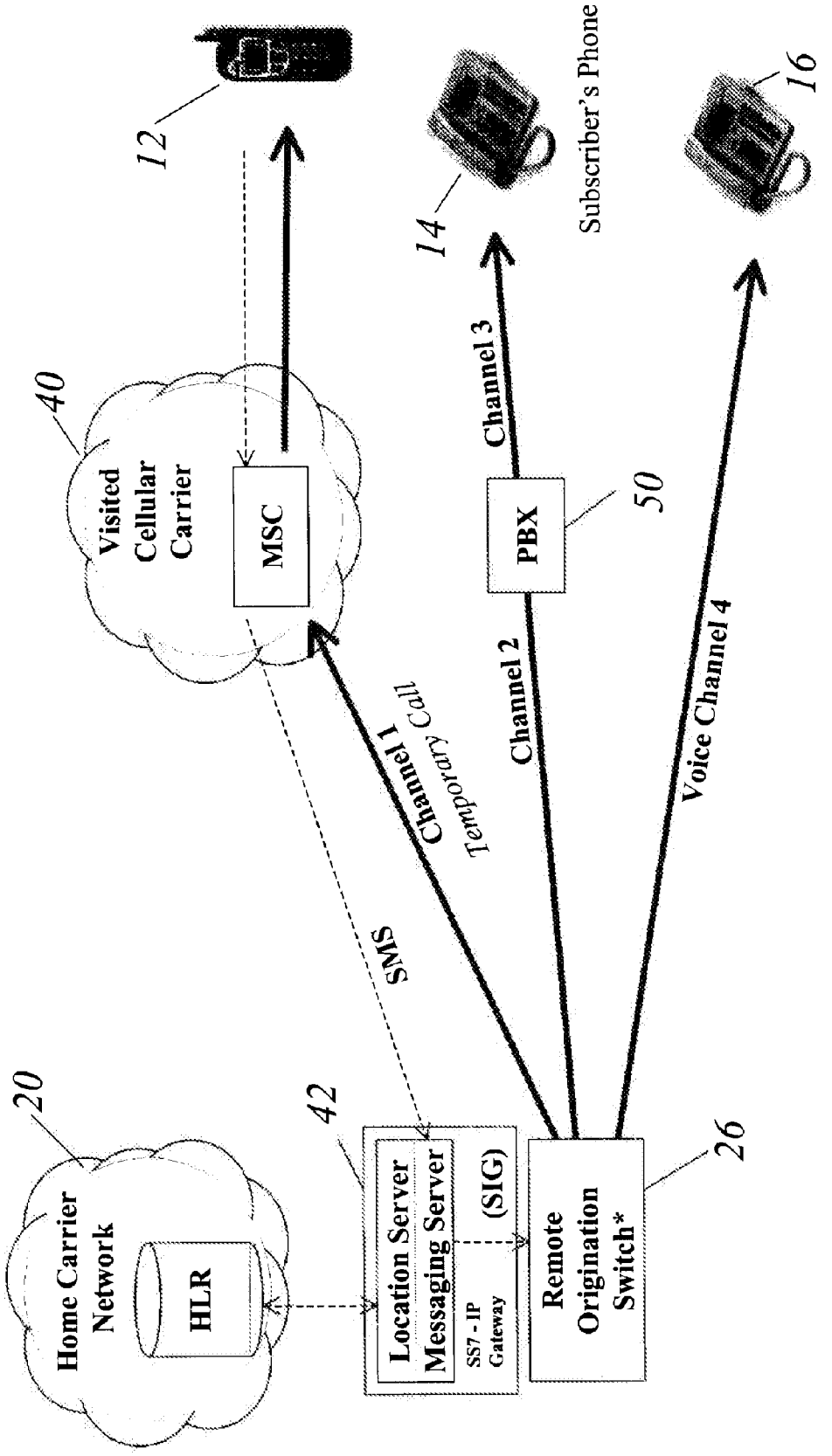
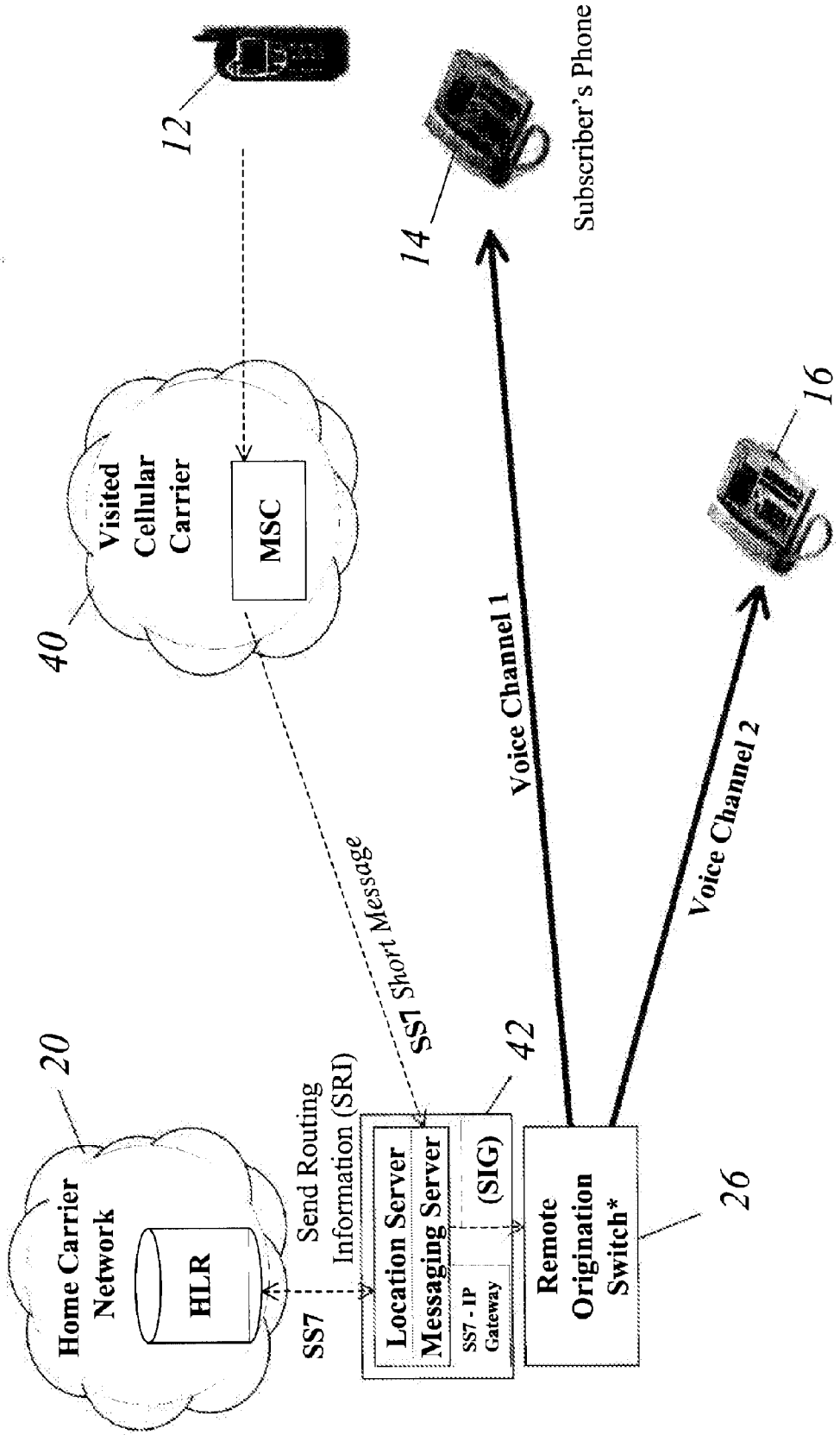

12
14
16
Subscriber's Phone
40
Visited Cellular Carrier
MSC
Channel 3
PBX
50
Channel 2
Channel 1
Temporary Call
SMS
Voice Channel 4
20
Home Carrier Network
HLR
42
Location Server
Messaging Server
(SIG)
SS7 - IP Gateway
Remote Origination Switch*
26

Figure 6



Gowling Strathy & Henderson

Espacenet

Bibliographic data: CA2437275 (A1) — 2002-10-17

SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS

Inventor(s): PYKE CRAIK R [CA]; HERN WILLIAM [GB]; MOUNJI HALIMA H [CA]; CARON SERGE S [CA]; THOMPSON ROGER L [US]; WELHAM MICHAEL [DE]; GOERENS MICHAEL [DE]; EWOTI CHARLES B [DE]; STRENG PETE J [CA]; KITTLITZ CHRISTIAN [CA]; TAYLOR RICHARD C [CA]; GOERTZEN CHRISTOPHER J [CA] ± (PYKE, CRAIK R, ; HERN, WILLIAM, ; MOUNJI, HALIMA H, ; CARON, SERGE S, ; THOMPSON, ROGER L, ; WELHAM, MICHAEL, ; GOERENS, MICHAEL, ; EWOTI, CHARLES B, ; STRENG, PETE J, ; KITTLITZ, CHRISTIAN, ; TAYLOR, RICHARD C, ; GOERTZEN, CHRISTOPHER J)

Applicant(s): NORTEL NETWORKS LTD [CA] ± (NORTEL NETWORKS LIMITED)

Classification: **- international:** ***H04L12/26; H04L29/06; H04M3/22; H04M7/00;*** (IPC1-7): H04L12/56

- cooperative: **H04L29/06**; **H04L63/30**; **H04L69/22**; **H04M3/2281**; **H04M7/006**; H04Q2213/13034; H04Q2213/13196; H04Q2213/13372; H04Q2213/13389

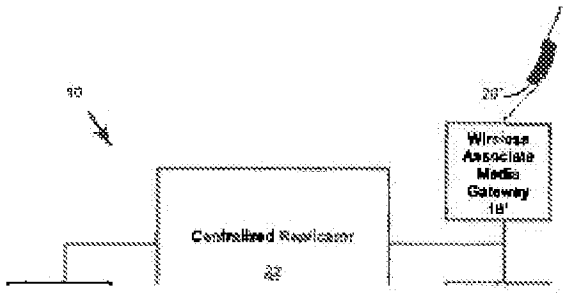
Application number: CA20012437275 20011009

Priority number(s): US20000239048P 20001010 ; WO2001US31548 20011009

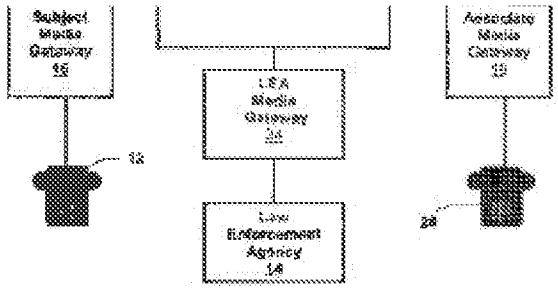
Also published as: WO02082782 (A2) WO02082782 (A3) US2003179747 (A1) EP1362456 (A2) EP1362456 (A4) EP1362456 (B1) DE60133316 (T2) AU2001297701 (A1) less

Abstract of CA2437275 (A1)

A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a firs t header from the packet, replicating the



payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96) .



(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 437 275 (13) A1

(40) 17.10.2002
(43) 17.10.2002

(12)

(21) 2 437 275

(22) 09.10.2001

(51) Int. Cl.[7]: H04L 12/56

(85) 28.07.2003

(86) PCT/US01/31548

(87) WO02/082782

(30) 60/239,048 US 10.10.2000

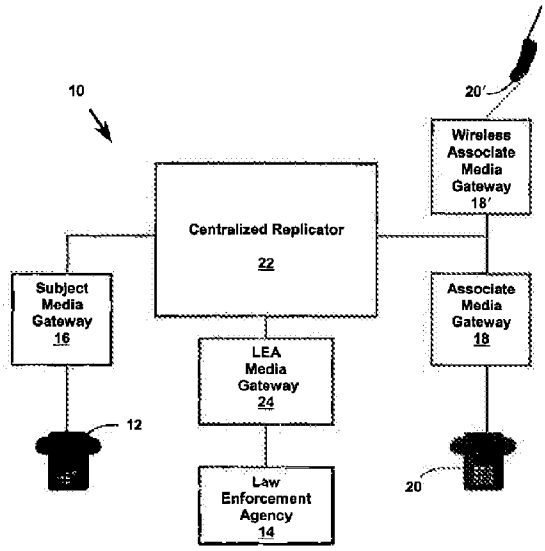
(71)
NORTEL NETWORKS LIMITED,
2351 Boulevard Alfred-Nobel, ST.
LAURENT , Q1 (CA).

(72)
KITTLITZ, CHRISTIAN (CA).
GOERTZEN, CHRISTOPHER J. (CA).
WELHAM, MICHAEL (DE).
TAYLOR, RICHARD C. (CA).
MOUNJI, HALIMA H. (CA).
EWOTI, CHARLES B. (DE).
GOERENS, MICHAEL (DE).
STRENG, PETE J. (CA).
CARON, SERGE S. (CA).
HERN, WILLIAM (GB).
THOMPSON, ROGER L. (US).
PYKE, CRAIK R. (CA).

(74)
SHAPIRO COHEN

(54) SYSTEME ET PROCEDE D'INTERCEPTION DE TELECOMMUNICATIONS
(54) SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS

(57)
A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).



Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2437275 A1 2002/10/17

(21) 2 437 275

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2001/10/09
(87) Date publication PCT/PCT Publication Date: 2002/10/17
(85) Entrée phase nationale/National Entry: 2003/07/28
(86) N° demande PCT/PCT Application No.: US 2001/031548
(87) N° publication PCT/PCT Publication No.: 2002/082782
(30) Priorité/Priority: 2000/10/10 (60/239,048) US

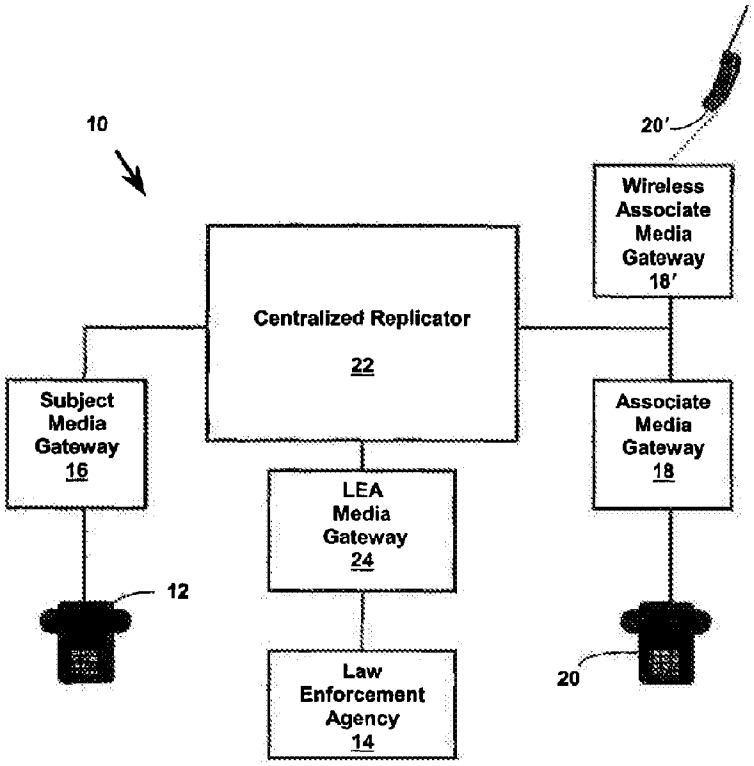
(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/56

(71) Demandeur/Applicant:
NORTEL NETWORKS LIMITED, CA

(72) Inventeurs/Inventors:
PYKE, CRAIK R., CA;
HERN, WILLIAM, GB;
THOMPSON, ROGER L., US;
CARON, SERGE S., CA;
MOUNJI, HALIMA H., CA;
EWOTI, CHARLES B., DE;
GOERENS, MICHAEL, DE;
...

(74) Agent: SHAPIRO COHEN

(54) Titre : SYSTEME ET PROCEDE D'INTERCEPTION DE TELECOMMUNICATIONS
(54) Title: SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS



(57) Abrégé/Abstract:
A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

CA 2437275 A1 2002/10/17
(21) 2 437 275
(13) A1

(72) Inventeurs(suite)/Inventors(continued): STRENG, PETE J., CA; GOERTZEN, CHRISTOPHER J., CA; KITTLITZ, CHRISTIAN, CA; TAYLOR, RICHARD C., CA; WELHAM, MICHAEL, DE

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082782 A3

(51) International Patent Classification[7]: H04L 12/56

(21) International Application Number: PCT/US01/31548

(22) International Filing Date: 9 October 2001 (09.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/239,048 10 October 2000 (10.10.2000) US

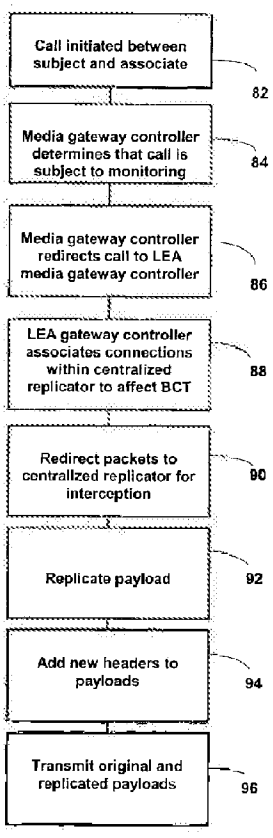
(71) Applicant *(for all designated States except US)*: **NORTEL NETWORKS LIMITED** [CA/CA]; 2351 Boulevard Alfred-Nobel, St. Lanrent, PQ H4S 2A9 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PYKE, Craik, R.** [CA/CA]; 426A Moodie Drive, Nepean, ON K2H 8A6 (CA). **HERN, William** [GB/GB]; "Feliz" Whyteladyes Lane, Maidenhead, SL6 9LA (GB). **THOMPSON, Roger, L.** [US/US]; Dept. ND840, P.O. Box 13955, RTP, NC 27709 (US). **CARON, Serge, S.** [CA/CA]; 52 Limbour, Gatineau. PQ J8V 1X9 (CA). **MOUNJI, Halima, H.** [CA/CA]; 60 Hemlo Cres., Kanata, ON K2T 1E2 (CA). **EWOTI, Charles, B.** [DE/DE]; Oberer Garwiedenweg 2, 88677, Markdorf (DE). **GOERENS, Michael** [DE/DE]; Kenzelweg 17, 88045 Friedrichshafen (DE). **STRENG, Pete, J.** [CA/CA]; 5436 West River Drive, Manotick, ON K4M 1G5 (CA). **GOERTZEN, Christopher, J.** [CA/CA]; #10-1701 Blohm Drive, Ottawa, ON K1G 6N6 (CA). **KITTLITZ, Christian** [CA/CA]; 2-2418 Carlson Avenue, Ottawa, ON K1V 8G1 (CA). **TAYLOR, Richard, C.** [CA/CA]; P.O. Box 22, Manotick, ON K4M 1A2 (CA). **WELHAM, Michael** [DE/DE]; Bruckfelder Strasse 27, 88662 Lippertsreute (DE).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS



(57) Abstract: A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

WO 02/082782 A3

WO 02/082782 A3

(74) **Agent: VYNALEK, John, H.**; Nortel Networks Inc., P.O. Box 13828, Research Triangle Park, NC 27709-3828 (US).

(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, EC, 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, US, 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, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

(88) **Date of publication of the international search report:**
24 April 2003

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.

Cross Reference to Related Applications

This application claims priority to United States Provisional Patent Application serial number 60/239,048, filed October 10, 2000, entitled LAWFUL INTERCEPT VIA CENTRALIZED REPLICATOR and is incorporated herein by this reference.

Background of the Invention

In law enforcement, it is sometimes necessary to monitor an individual or group of individuals to support allegations of illegal activity. Indeed, many countries mandate that telecommunications service providers and equipment manufacturers provide a law enforcement agency the ability to perform lawful interception of telecommunications to and from a subject being monitored.

Historically, lawful intercept consisted of using alligator clips which a law enforcement agency would physically clip to, thereby tapping into, the telecommunication line of a subject (the monitored party) and monitor calls to or from an associate (a party calling or being called by the subject.)

There are two categories of intercept, call data and call content. Call data intercept includes monitoring call events, for example, monitoring if the subject originates a call, or if a call is terminated on the subject, or if a call is forwarded elsewhere. This type of monitoring, known as pen register, provides the phone number of both the person called and the person calling, along with call events and time-date stamps of when the events occurred. In contrast, call content includes the actual content of the call, i.e., the conversation that takes place, plus

call data. Call content is transmitted to the law enforcement agency in real time so that the law enforcement agency can monitor the conversation as it happens. This transmission must be transparent to the subject and the associates so that they are not aware that they are being monitored.

As telecommunications equipment evolved, modules were provided in the telecommunication switch that provided the law enforcement agency the ability to lawfully intercept telecommunications. For example in a Time Division Multiplexed (TDM) switch such as the Nortel Networks DMS -100, a switch network fabric provides an access point that allows a law enforcement agency to tap the subject's phone line. This type of centrally located access point is known as an Intercept Access Point (IAP). The resulting information is then provided to the law enforcement agency.

As telecommunications have evolved to packet based communications, to include Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) protocols, the changing architecture of the telecommunications switches has necessarily made the interception of content more difficult.

In September of 1998, the Federal Communications Committee (FCC) ruled that new TDM equipment must have lawful intercept capability built in. Moreover, in August of 1999 the FCC ruled that packet communications interception capability will be required by September 30, 2001.

Accordingly, there is a need to be able to intercept voice over packet communications in a manner that satisfies governmental requirements, is

transparent to the subject and the associate, in real time, and works with standard protocols such as IP and ATM applications.

Summary of the Invention

The invention results from the realization that a truly efficient and effective system and method for intercepting voice over packet communications is achieved in which a packet communication signal directed to or from a subject is received by a centralized replicator. The header is stripped from the packet leaving only the payload, the payload is replicated, a header is added to the replicated payload and the replicated payload is transmitted to a Law Enforcement Agency. A header is added to the original payload and the packet is retransmitted to the intended recipient. Alternatively, the entire packet can be replicated and the headers stripped off both the original packet and the replicated packet and a new header added to each payload. The payloads are then transmitted to the intended recipient and the Law Enforcement Agency.

In one embodiment, there is provided a method of intercepting a telecommunication signal including receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload, adding a new header to replicated payload and directing the replicated payload to the address associated with the new header.

It can be determined whether a telecommunication packet is to be monitored. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with the second predetermined header.

In another embodiment there is provided a system for intercepting a telecommunication signal. The system includes an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet comprising a predetermined header and a payload, a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to replicated payload and a relay point for directing the replicated payload to the address associated with the new header.

The new header can be associated with one of an intended recipient and a law enforcement agency. There can be a media gateway for directing the telecommunication signal to the audio server and also a media gateway controller, responsive to the media gateway, for determining that the telecommunication packet is to be intercepted. The media gateway controller can include a call discriminator, responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception. There can be a second termination point for adding a second predetermined header to

the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. There can be a second relay point for directing the payload to the address associated with the second predetermined header.

In yet another embodiment, there is provided a method for intercepting a telecommunication signal by receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload, adding a new header to replicated payload and directing the replicated payload to the address associated with the new header.

It can be determined whether the telecommunication packet is to be intercepted. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be removed from the payload and replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with second predetermined header.

There is further provided a method of redirecting a telecommunication signal. The method includes receiving a telecommunication packet comprising a header and a payload, removing the predetermined header from the packet, adding a second predetermined header to payload and directing the replicated payload to the address associated with the second predetermined header.

It can be determined whether a telecommunication packet is to be redirected. The second predetermined header can be associated with one of an intended recipient and a law enforcement agency. The payload can be replicated. This replication can occur before or after the predetermined header is removed. A new header can be added to the replicated payload and the replicated payload can be directed to the address associated with second predetermined header. The new header can be associated with the other of the intended recipient and the law enforcement agency.

There is still further provided a method of monitoring a telecommunication signal to or from a subject being monitored from or to an associate. The method includes determining that a telecommunication signal is subject to being monitored, establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject, establishing a connection between the second gateway and a second termination point representing the first gateway and establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connection directly.

A connection can be established from at least one of the first termination point and the second termination point to a gateway associated with other than the subject and the associate concurrently with the connection between the first termination point and the second termination point.

There is provided even still further a method of redirecting a telecommunications signal intended for one of a subject and an associate by associating a first termination point with a first intended termination point of a first media gateway, associating a second termination point with a second intended termination point of a second media gateway, establishing a connection between the first intended termination point and the second termination point, establishing a connection between the second intended termination point and the first termination point and establishing a connection between the first termination point and the second termination point wherein the first intended termination point and the second termination point appear to be connected directly.

Brief Description of the Drawings

Figure 1 is a schematic block diagram generally representing a system for intercepting packet communications including a centralized replicator according to the present invention;

Figure 2 is a more detailed schematic block diagram, similar to Figure 1, including a media gateway controller associated with each media gateway for implementing the necessary connections to affect interception of packet communications;

Figure 3 is a schematic block diagram, similar to Figure 1, demonstrating the actual and ephemeral connections when implementing the call intercept according to one aspect of the present invention;

Figure 4 is a schematic block diagram demonstrating associated connections internal to the centralized replicator for affecting bearer channel tandeming for intercepting packet communications;

Figure 5 is a schematic block diagram representing bearer channel tandeming by the call discriminator in response to a requirement to intercept packet communications;

Figure 6 is a flow chart representing one method of intercepting packet communications according to the present invention;

Figure 7 is a schematic block diagram, similar to Figure 2, in which a second associate establishes a call to a subject being monitored and a call waiting feature is invoked;

Figure 8 is a schematic block diagram, similar to figure 4, demonstrating the connection topology within the centralized replicator when the call-waiting feature is invoked; and

Figure 9 is a schematic block diagram, similar to Figure 8, demonstrating the connection topology within the centralized replicator when a conference call feature is invoked.

Detailed Description

According to the present invention there is generally provided a system 10, Figure 1, which can intercept a packet telecommunication signal to or from a subject 12 being monitored, for example, by a Law Enforcement Agency (LEA)

14. There is a first, or subject, media gateway **16** associated with subject **12** being monitored and a second, or associate, media gateway **18** associated with an associate **20** who is calling or being called by subject **12**. There can also be a wireless associate media gateway **18'** where an associate **20'** is communicating with subject **12** over a wireless phone.

A call is initiated between subject **12** and associate **20**. It is determined that the telecommunication signal is one targeted for monitoring and is to be intercepted. Accordingly, for a call from associate **20** to subject **18**, the telecommunication signal, rather than being sent directly to the intended associate media gateway **18**, is redirected from subject media gateway **16** to a centralized replicator **22** which may, for example, comprise a universal audio server associated with LEA **14**. When centralized replicator **22** receives the telecommunication signal, comprised of individual packets with each packet including a header and a payload, centralized replicator **22** removes the header from the packet leaving the payload intact. Centralized replicator **22** replicates the payload, adds a header to the replicated payload and transmits the replicated payload to a law enforcement agency gateway **24**. Once the payload has been replicated a header is added to the original payload and that packet is retransmitted by centralized replicator **22** to associate media gateway **18/18'** for delivery to associate **20/20'**.

Alternatively, the entire incoming packet can be replicated, including header and payload. Once the packet has been replicated, the headers of the original and replicated packets are removed. A new header is added to the

replicated payload for delivery to law enforcement agency **14** and a new header is added to the original payload for delivery to the respective intended recipient, subject **12** or associate **20**.

Referring now to Figure 2, associated with each media gateway **16, 24** and **18**, can be a media gateway controller **26, 28** and **30**, respectively. As used herein, a media gateway controller refers to one or more devices whose functionality can include performing media gateway control signaling and call processing functions. Each associated gateway controller can include a call discriminator **32** comprising call processing software that determines that a call from or between associated gateways, for example subject media gateway **16** to associate media gateway **18**, is in fact subject to monitoring. There can be included within discriminator **32**, for example, a lawful intercept database that identifies subscribers, e.g., subject **12**, who are subject to a surveillance order.

Once it has been determined that the call is subject to monitoring, subject media gateway controller **26** sends a first message, for example using Media Gateway Control Protocol (MGCP) or H.248 protocol, to LEA media gateway **28** to effect a connection between subject media gateway **16** and centralized replicator **22** and another message to effect a connection between associate media gateway **18** and centralized replicator **22**. The redirection of the call through centralized replicator **22** is transparent to call processing and service functions and the call appears to be set up normally as if subject media gateway **16** and associate media gateway **18** were connected directly. The above example assumes that subject **12** and associate **20** do not share a common

gateway. However, a shared gateway would not change the operation of the subject invention as call discrimination and packet replication would take place in the same manner, transparent to the caller.

LEA Media gateway controller **28** effects redirection of the call from the intended recipient and instructs centralized replicator **22** to make internal connections, referred to as bearer channel tandeming, in order to facilitate packet replication as will be discussed further in reference to Figure 4. Once media gateway controller **28** has established the necessary connections between subject media gateway **16**, centralized replicator **22** and associate media gateway **18**, media gateway controller **28** initiates the connections between centralized replicator **22** and law enforcement agency media gateway **24** which is then connected to LEA **14.**

Accordingly, a call subject to monitoring will contain packets whose headers have been altered or substituted such that instead of the packets being transmitted to and from gateways **16** and **18** directly (the intended recipients), the packets are redirected to centralized replicator **22** for replication. Media gateway controller **28** alters the address information of the messages such that it appears to subject media gateway **16** that the message is coming from associate media gateway **18** and messages sent to associate media gateway **18** appear to come from subject media gateway **16.**

As shown in Figure 3, subject media gateway controller **26** sends a message **27** with the session description information, for example using a protocol such as the Session Description Protocol (SDP), of subject media

gateway **16** to LEA media gateway controller **28**. Media gateway controller **28** sends a message **29** including the session information of media gateway **16** to associate media gateway controller **30**, but with the address of centralized replicator **22**.

Similarly, associate media gateway controller **30** sends a message **31** acknowledging the session description of media gateway **16** with the session description of associate media gateway **18**. LEA media gateway controller **28** sends a message **33** acknowledging the session description of subject media gateway **16** with the session description of associate media gateway **18**, but with the address of centralized replicator **22**.

Accordingly, a communication path from subject media gateway **16** to associate media gateway **18** is tandemed through centralized replicator **22**, but is transparent to subject **12** or associate **20**.

Figure 4 further demonstrates how bearer channel tandeming can be accomplished through centralized replicator **22** by modifying the association between packet streams and endpoints to affect the connections and representations demonstrated in Figure 3.

Packet streams **34, 36, 38** and **40** originate from associated endpoints **42, 44, 46** and **48**, respectively. Accordingly, the respective transmit and receive streams **34/36** of endpoint **42**, while appearing to be associated with endpoint **46** (associate media gateway **18**), are associated with end point **44** within centralized replicator **22**. Similarly, respective transmit and receive streams **38/40** of endpoint **46** are associated with end point **48** while appearing to be

associated with end point **42** (subject media gateway **16**). Finally, internal streams **50** and **52** are associated with end points **44** and **48**. Connections to end points **42, 44, 46** and **48** are initiated from media gateway controller **28** (Figure 3) where endpoints **42** and **46** are the recognized originator and terminator endpoints.

Endpoints **42** and **46** are typically configured to convert the TDM information from subject **12** or associate **20** into, for example, IP or ATM packets or cells depending upon the fabric of centralized replicator **22**. Similarly, information received at these endpoints from centralized replicator **22** is converted from IP/ATM to TDM. In contrast, endpoints **44** and **48** within centralized replicator **22** are typically configured only as packet relay points and do not provide any transcoding or jitter correction in order to minimize latency and reduce the risk of detection by subject **12** or associate **20** of the monitoring. Flow control buffers (not shown) can be provided to avoid loosing packets.

Packet relay endpoints **44** and **48**, respectively, strip the header off incoming packet streams **34** and **38** that they receive from respective endpoints **42** and **46**, replicate the payload, add a new header to the replicated payload and transmit replicated packet streams **54** and **56** to law enforcement agency gateway **24** via endpoints **58** and **60**. Packet relay endpoints **44** and **48** also transmit the original payload via streams **50** and **52**, respectively, to each other, adding new headers directing the packets to respective gateways **16** and **18**. Alternatively, the entire packet may be replicated, then the replicated headers are

stripped off and new headers added to redirect the replicated packets to their respective gateways.

In order to ensure transparency to subject **12** and associate **20** of the intercept, streams **54** and **56** destined for law enforcement agency **14** should be unidirectional. Accordingly, endpoints **58** and **60** should be configured as send only in the direction of law enforcement agency gateway **24**. Endpoints **58**, **60** should be from the same resource pool as endpoints **44** and **48** so that the resource pools reflect what endpoints within centralized replicator **22** have internal connections between them so that media gateway controller **28** can send the appropriate connectivity messages to centralized replicator **22**. Accordingly, a resource manager **62** is provided. Moreover, endpoints **58** and **60**, as with packet relay endpoints **44** and **48**, should achieve a transmission time between endpoints that maintains low latency such that the total trip delay of the packets, including time to traverse centralized replicator 22, does not exceed the engineered threshold of the echo cancellers of the respective media gateways.

Resource manager **62** performs several basic functions to include allocation of resources, returning resources to a free pool and reporting on resources. Resource manager **62** can provide an interface to operating personnel to indicate what resources in centralized replicator **22** are to be used for bearer channel tandeming. The connection to law enforcement agency **14** can occur in several forms to include dedicated lines, switched local links, dedicated trunks or switched remote links without departing from the scope of the invention.

A monitoring point **64** within law enforcement agency **14**, which may include an audio device, can receive the call content via a TDM multiplexed mixing bridge **66**. Monitoring point **64** receives the call content in real time, thus at the same time subject **12** hears the ring from associate **20**, law enforcement agency **14** also hears the ring back. As will be apparent to those skilled in the art, law enforcement agency gateway **24** should be able to support all possible CODEC's that can be negotiated between a subject **12** and an associate **20**.

While system **10** has been described as only performing a single replication for a single law enforcement agency, it should be understood that this is not a limitation of the present invention, as the incoming packet streams can be replicated at endpoints **44** and **48** multiple times, depending on the number of law enforcement agencies monitoring subject **12**, by configuring the hardware comprising endpoints **44** and **48** for multiple replications.

Despite the changes in the connection messages as described above, neither subject **12** nor associate **20** are provided an indication that the call is being redirected through centralized replicator **22**.

When it is determined that a call is to be monitored, the standard connectivity message from the call server can either be altered to perform the appropriate connection or the message can be split into multiple messages to perform the requested connection.

By way of example, the connection operation from the call server requesting a connection between subject **12** and associate **20** is modified into three separate connectivity operations. This is done by requesting separate

connections from endpoints **42** and **44**, from endpoints **46** and **48** and from endpoints **44** to **48**.

As shown in Figure 5, a call agent or call processing **68**, in response to electronic surveillance software **69**, issues a connectivity message **70** to call discriminator **32** to make a subject to associate connection from a discriminator layer in connectivity software **72** to bearer channel tandeming connectivity software **74** which issues three separate media gateway control messages. A first message **76** can initiate a connection from subject media gateway **16** (Figure 4) to centralized replicator **22**. A second message **78** can initiate a connection from associate media gateway **18** to centralized replicator **22**. A third message **80** can instruct centralized replicator **22** to make an internal association between the centralized replicator **22** to subject media gateway **16** connection and the centralized replicator **22** to associate media gateway **18** connection.

Once the associated connection between subject **12** and associate **20** has been configured, media gateway controller **28** (Figure 3) initiates the respective connections to law enforcement media gateway **24** by requesting two connections from endpoints **44** to **58** and **48** to **60** (Figure 4) within centralized replicator **22** to law enforcement media gateway **24**, where endpoints **58** and **60** connect to law enforcement media gateway **24**, as illustrated in Figure 4 above.

A flowchart of the present invention is presented in Figure **6**. A call is initiated between a subject and an associate, Block **82**. The media gateway controller associated with the subject being monitored determines that the call is to be monitored, Block **84**, and redirects the call to the media gateway controller

of the LEA by associating the LEA media gateway with the destination (associate) media gateway, Block **86**. The media gateway controller associated with the law enforcement agency effects bearer channel tandeming by associating the endpoints of the subject and associate media gateways with endpoints within the centralized replicator, Block **88**.

Once tandeming of the bearer channel has been affected, packets to and from the subject are redirected to the centralized replicator, Block **90**, where the payload is replicated, Block **92**, and new headers added to both the replicated payload and the original payload, Block **94**. The respective payloads are then transmitted to the recipient subject or associate and the LEA, Block **96**.

Figure 7 represents generally the situation where a call-waiting feature is invoked. For illustrative purposes, each agent is serviced by a different media gateway controller. A call is originated between subject **12** and first associate **20**, as discussed above, until subject **12** and first associate **20** enter the talking state as discussed above with the law enforcement agency **14** receiving the call content.

A second associate **20'** originates a call to subject **12**. Associate media gateway controller **30'** performs call processing routing the call to subject media gateway **16** and it is determined that the call is subject to interception. Centralized replicator **22** recognizes that subject **12** is engaged in an existing call. LEA media gateway controller **28** instructs media gateway **16** to play a call waiting tone to subject **12**.

Referring now to Figure 8, subject **12** invokes a feature flash to receive the call originated by second associate **20'**. Subject media gateway controller **26** (Figure 7) instructs centralized replicator **22** to break the connection between subject **12** and first associate **20**. However, Tandeming Connectivity software **74** (Figure 5) intercepts this message, and alters it to only break the connection between endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA **14** be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** remain in tact.

Tandeming Connectivity software **74** obtains two more endpoints **44'** and **48'** from resource manager **62** to tandem the call between subject **12**, second associate **20'** and LEA **14**. Tandeming Connectivity software **74** initiates a connection between end points **42** and **44'**. Tandeming Connectivity software **74** further initiates a connection between endpoints **44'** and **48'** within centralized replicator **22**. The session description information of endpoints **42** and **44'** are exchanged, and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel.

Subject media gateway controller **26** acknowledges endpoint **46'** and responds with the session information of endpoint **48'**, in order to facilitate the completion of the bearer channel configuration.

At this point a bearer channel is configured between end points **42** and **44'**, **44'** and **48'** and **48'**and **46'**. Subject **12** and second associate **20'** now enter

the talking state with law enforcement agency **14** receiving the call content. Second associate **20'** terminates the call and subject **12** invokes a feature flash to return to first associate **20**. Subject media gateway controller **26** sends a message to break the connection between subject **12** and the message is intercepted and altered to only break the connection between end points **42** and **44'**. The connection with Law enforcement agency **14** is also broken, but the connections between endpoints **44'** and **48'** and **48'** and **46'** remain intact. Second associate media gateway controller **30'** (not shown) passes a clear forward message to subject media gateway controller **26** instructing connectivity to break the connection with second associate **20'**. Tandeming Connectivity software **74** (Figure 5) intercepts the message and, determining that the other external agent has been removed from,the bearer channel tandem, instructs a break of the connections between end points **44'** and **48'**, and **48'** and **46'**.

Endpoints **44'** and **46'** are returned to resource manager **62** to be reentered into the free pool. Subject media gateway controller **26** (Figure 7) sends a message to reestablish a connection between subject **12** and first associate **20**. Tandeming Connectivity software **74** (Figure 5) intercepts this message, determines the given communication is already associated with a tandemed connection, and retrieving the endpoints in use, issues connectivity messages to reestablish the connection between endpoints **42** and **44**.

The session information of end points **42** and **44** are exchanged as previously discussed completing the bearer channel tandem. Electronic Surveillance software 69 (Figure 5) requests notification of the endpoints being

used to tandem the bearer channel through centralized replicator **22**. Endpoints **58** and **60** are then connected to LEA media gateway **24** in order to provide capture of the call content. Subject **12** and associate **20** are again in a talking state through a bearer channel established via endpoints **42** and **44**, **44** and **48** and **48** and **46**.

Referring to Figure 7 once again, a conference call feature is established in a manner similar to call waiting. A call is originated between subject **12** and first associate **20**. Subject media gateway controller **26** determines that the call is subject to monitoring and bearer channel tandeming is initiated connecting subject media gateway **16** and associate media gateway **18** via centralized replicator **22** as discussed above by LEA media gateway controller **26** associating respective end points within centralized replicator **22** with subject media gateway **16** and associate media gateway **18**. A connection is then initiated between end points within centralized replicator **22**.

Associate media gateway **18** acknowledges the associated endpoint within centralized replicator **22**, as if it were acknowledging subject media gateway **16**, as discussed above with reference to Figure 3, and responds with the session description information of associate media gateway **18** and a bearer channel is configured between endpoints **42**, **44**, **46** and 48 (Figure 4).

A connection between law enforcement agency gateway **24** and end points within centralized replicator **22** as discussed in Figure 4 above, is established. Subject **12** and associate **20** now enter a talking state and law

enforcement agency **14** receives the replicated packet streams and monitors the call.

Referring again to Figure 8, subject **12** can invoke a flash feature and originate or receive a call with a second associate **20'**. Subject media gateway controller **26** (Figure 7) receives a message from the call agent of subject **12** to break the connection with first associate **20**, which is intercepted due to the bearer channel tandeming, and media gateway controller **28** sends a modified message to centralized replicator **22** (rather than to associate media gateway **18**) to break the connectivity of endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA 14 be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** temporarily remain in tact.

With respect to the new caller, the media gateway determines that the call is subject to monitoring, and two more endpoints **44'** and **48'** within centralized replicator **22** are allocated by resource manager **62** and configured to tandem the call to second associate **20'**. A connection is then initiated between endpoints **42** and **44'** and media gateway controller **28** passes the endpoint of **48'** to the media gateway controller **30'** associated with second associate **20'**. A connection is then initiated between **44'** and **48'** within centralized replicator **22**. The session description information of **42** and **44'** are exchanged and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel tandeming.

At this point a bearer channel is configured between **42** and **44'**, **44'** and **48'**, and **48'** and **46'**. A connection is then initiated from centralized replicator **22** to LEA **14** via endpoints **44'**and **58'** and **48'** and **60'**. Subject **12** can now talk with second associate **20'** and LEA **14** can intercept the content. Subject **12** then invokes a feature flash to join first associate **20** in a three-way call. Connectivity software (Figure 5) requests that all connections associated with the previous legs be broken (shown in phantom) to enable the three-way call. Accordingly, the connection of end points **44** and **48**, **48** and **46** and **44'** and **48'** and **48'** and **46'** are broken along with the corresponding LEA connection and all resources are returned to the resource pool. Media gateway controller **28** requests a connection between subject **12**, first associate **20** and second associate **20'** through conferenced ports **98**, **100** and **102**, as shown in Figure 9.

Claims

What is claimed is:

1. A method of intercepting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a predetermined header and a payload;

(b) removing the predetermined header from the packet;

(c) replicating the payload;

(d) adding a new header to replicated payload; and

(e) directing the replicated payload to the address associated with the new header.

2. The method of claim 1 further comprising the step of determining that a telecommunication packet is to be monitored.

3. The method of claim 1 further comprising the step of associating the new header with one of an intended recipient and a law enforcement agency.

4. The method of claim 3 further comprising the step of replacing the predetermined header with a second predetermined header.

5. The method of claim 4 further comprising the step of associating the second predetermined header with the other of the intended recipient and the law enforcement agency.

6. The method of claim 4 in which the step of replacing occurs after the step of replicating.

7. The method of claim 5 further comprising the step of directing the payload to the address associated with the second predetermined header.

8. A system for intercepting a telecommunication signal, the system comprising:

(a) an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet comprising a predetermined header and a payload;

(b) a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to replicated payload; and

(c) a relay point for directing the replicated payload to the address associated with the new header.

9. The system of claim 8 further comprising a media gateway for directing the telecommunication signal to the audio server.

10 The system of claim 8 in which the new header is associated with one of an intended recipient and a law enforcement agency.

11. The system of claim 9 further comprising a media gateway controller, responsive to a media gateway, for determining that a telecommunication packet is to be intercepted.

12. The system of claim 11 in which the media gateway controller includes a call discriminator, responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception.

13. The system of claim 12 further comprising a second termination point for adding a second predetermined header to the payload.

14. The system of claim 13 in which the second predetermined header is associated with the other of the intended recipient and the law enforcement agency.

15. The system of claim 14 further comprising a second relay point for directing the payload to the address associated with second predetermined header.

16. A method of intercepting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a predetermined header and a payload;

(b) removing the predetermined header from the packet;

(c) replicating the payload;

(d) adding a new header to replicated payload; and

(e) directing the replicated payload to the address associated with the new header.

17. The method of claim 16 further including the step of determining that a telecommunication packet is to be intercepted.

18. The method of claim 16 further comprising the step of associating the new header with one of an intended recipient and a law enforcement agency.

19. The method of claim 18 further including the step of replacing the predetermined header removed from the payload with a second predetermined header.

20. The method of claim 19 further comprising the step of associating the second predetermined header with the other of the intended recipient and the law enforcement agency.

21. The method of claim 19 in which the step of replacing occurs after the step of replicating.

22. The method of claim 20 further comprising the step of directing the payload to the address associated with second predetermined header.

23. A method of redirecting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a header and a payload;

(b) removing the predetermined header from the packet;

(c) adding a second predetermined header to payload; and

(d) directing the replicated payload to the address associated with the second predetermined header.

24. The method of claim 23 further comprising the step of determining that a telecommunication packet is to be redirected.

25. The method of claim 23 further comprising the step of replicating the payload.

26. The method of claim 25 wherein the step of replicating includes replicating the payload before the predetermined header is removed.

27. The method of claim 23 further comprising the step of associating the second predetermined header with one of an intended recipient and a law enforcement agency.

28. The method of claim 27 further comprising the step of adding a new header to the replicated payload.

29. The method of claim 28 further comprising the step of associating the new header with the other of the intended recipient and the law enforcement agency.

30. The method of claim 29 further comprising the step of directing the replicated payload to the address associated with the new header.

31. A method of monitoring a telecommunication signal to or from a subject being monitored from or to an associate, the method comprising the steps of:

(a) determining that a telecommunication signal is subject to being monitored;

(b) establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject;

(c) establishing a connection between the second gateway and a second termination point representing the first gateway; and

(d) establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connection directly.

32. The method of claim 31, further comprising the step of establishing a connection from at least one of the first termination point and the second termination point to a gateway associated with other than the subject and the associate concurrently with the connection between the first termination point and the second termination point.

33. A method of redirecting a telecommunications signal intended for one of a subject and an associate, the method comprising:

(a) associating a first termination point with a first intended termination point of a first media gateway;

(b) associating a second termination point with a second intended termination point of a second media gateway;

(c) establishing a connection between the first intended termination point and the second termination point;

(d) establishing a connection between the second intended termination point and the first termination point; and

(e) establishing a connection between the first termination point and the second termination point wherein the first intended termination point and the second termination point appear to be connected directly.

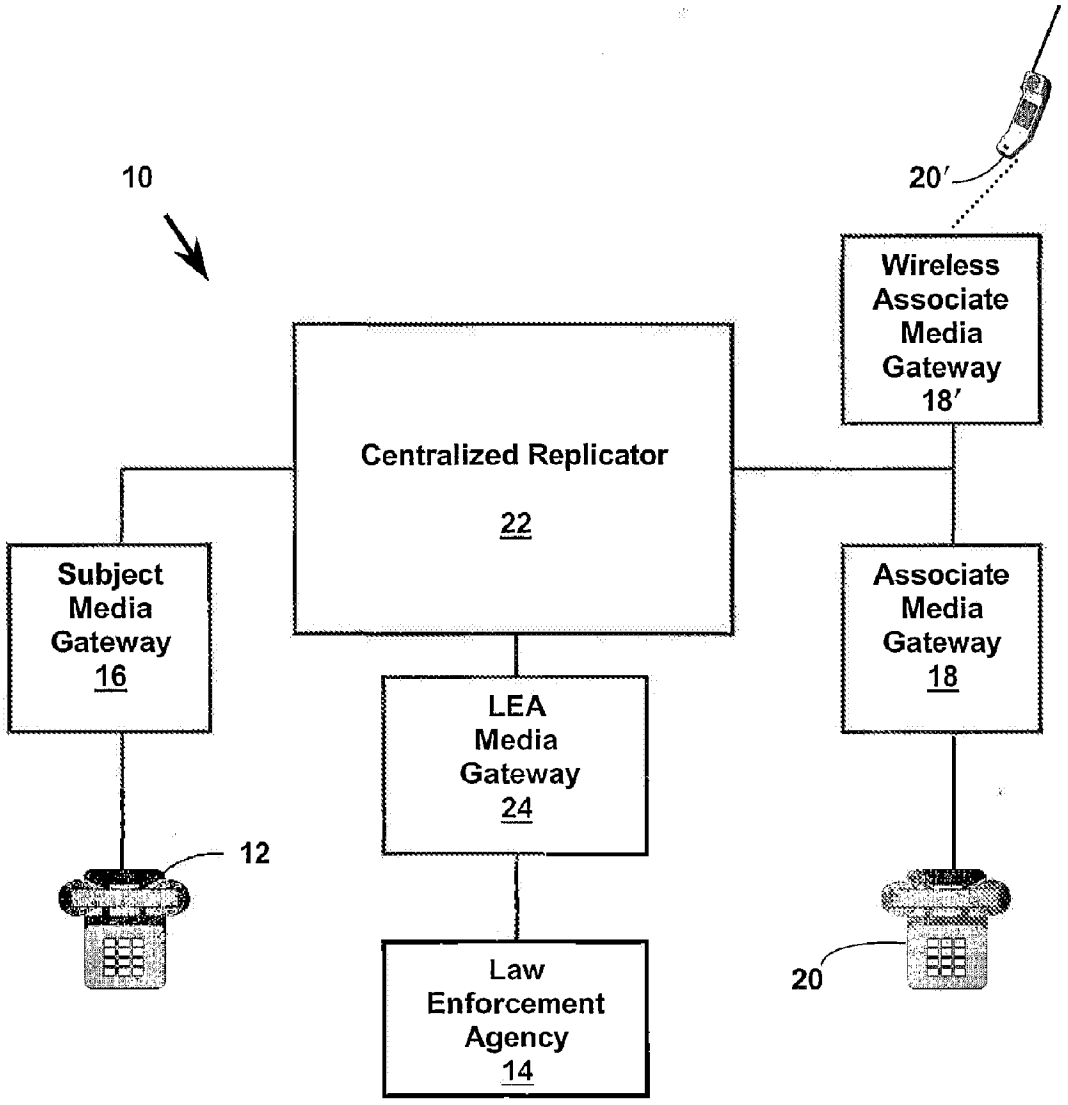

10
20′
Wireless Associate Media Gateway 18′
Centralized Replicator 22
Subject Media Gateway 16
Associate Media Gateway 18
LEA Media Gateway 24
12
20
Law Enforcement Agency 14

Figure 1

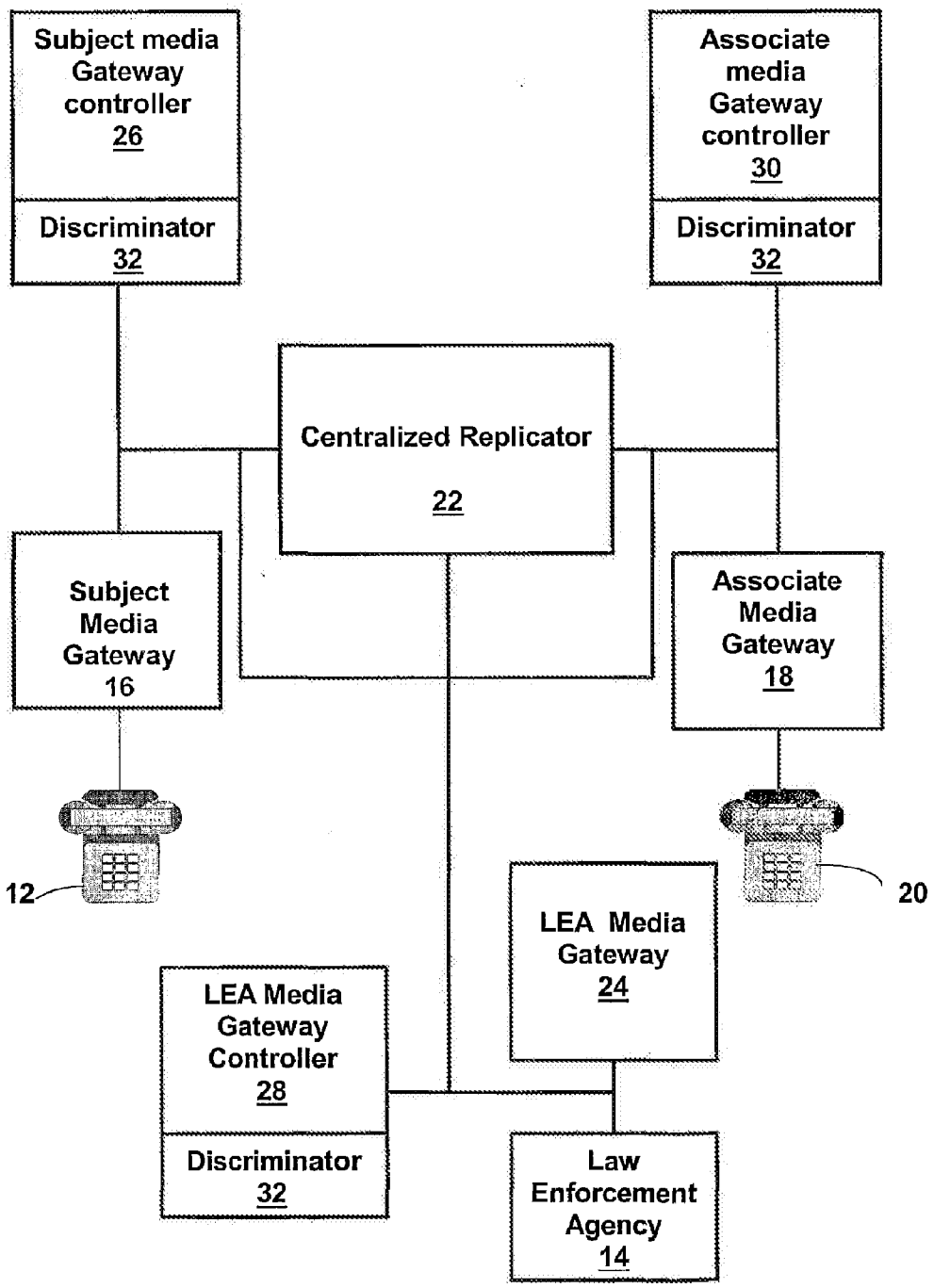

Subject media Gateway controller 26
Discriminator 32
Associate media Gateway controller 30
Discriminator 32
Centralized Replicator 22
Subject Media Gateway 16
Associate Media Gateway 18
12
20
LEA Media Gateway 24
LEA Media Gateway Controller 28
Discriminator 32
Law Enforcement Agency 14

Figure 2

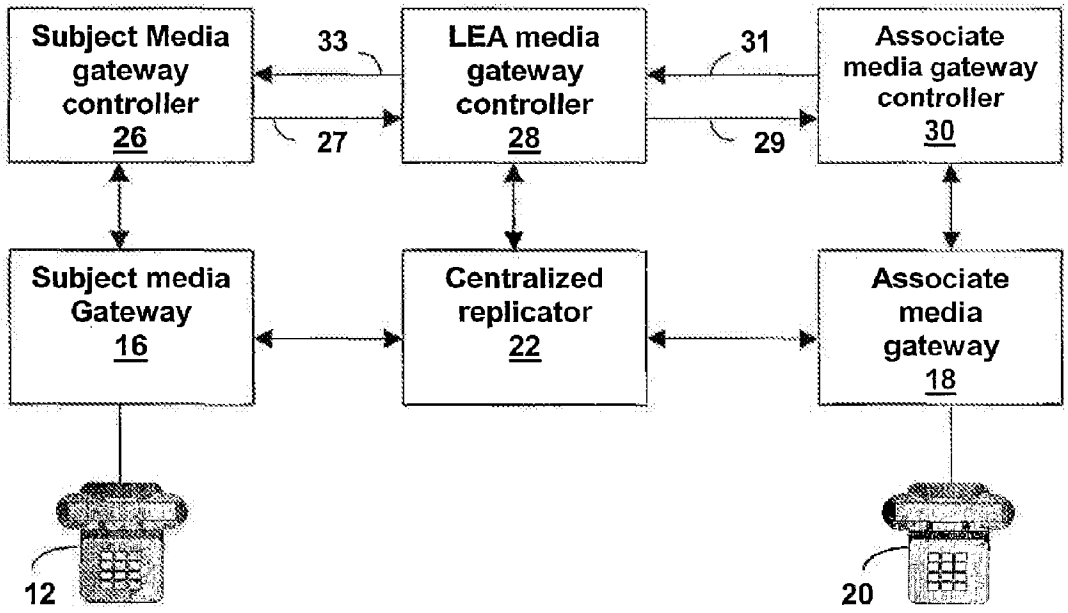

Subject Media gateway controller 26
33
27
LEA media gateway controller 28
31
29
Associate media gateway controller 30
Subject media Gateway 16
Centralized replicator 22
Associate media gateway 18
12
20

Figure 3

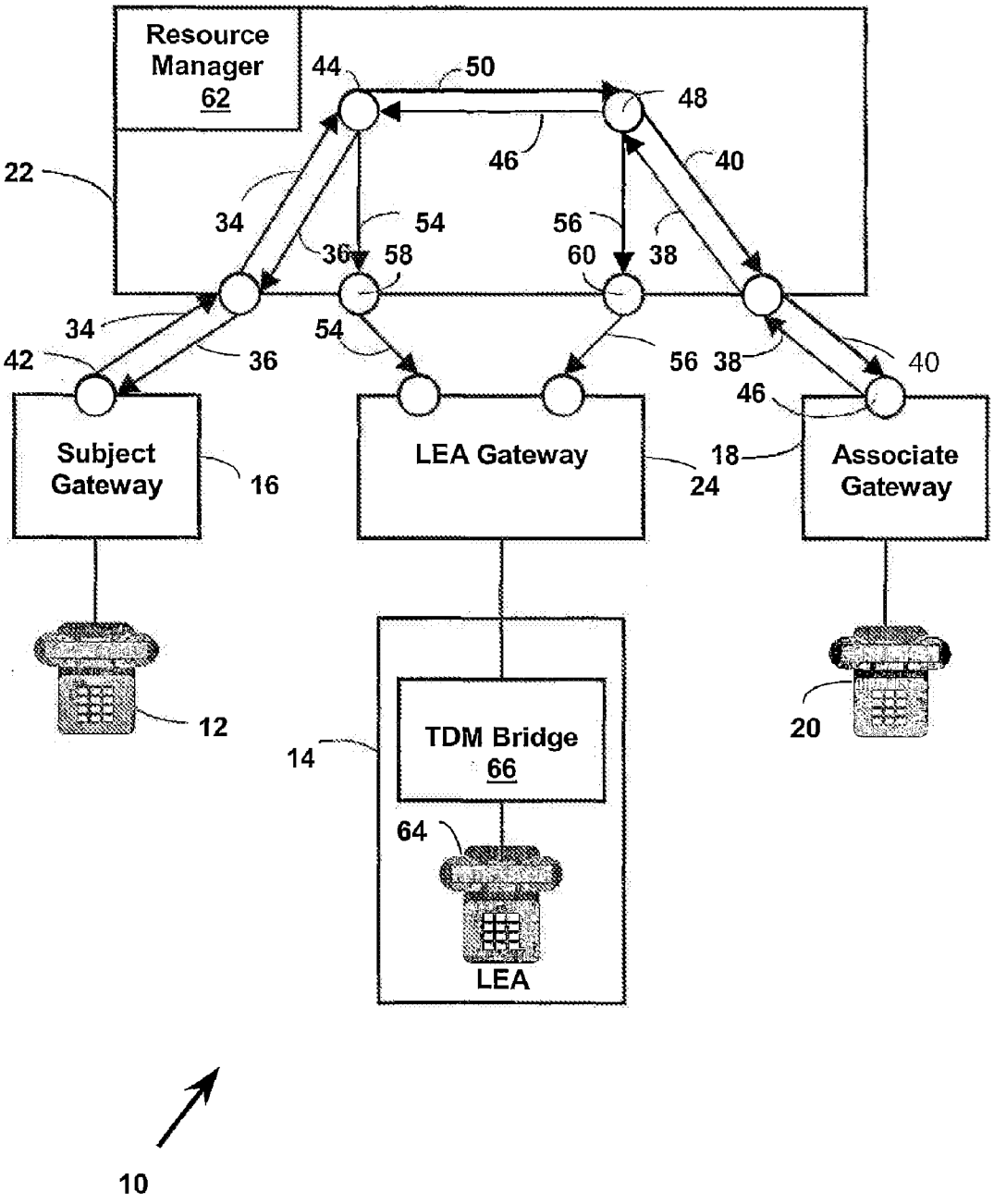

Resource Manager 62
44
50
48
46
40
22
34
54
56
36
58
60
38
34
54
42
36
56
38
40
46
Subject Gateway
16
LEA Gateway
18
24
Associate Gateway
12
14
TDM Bridge 66
64
LEA
20
10

Figure 4

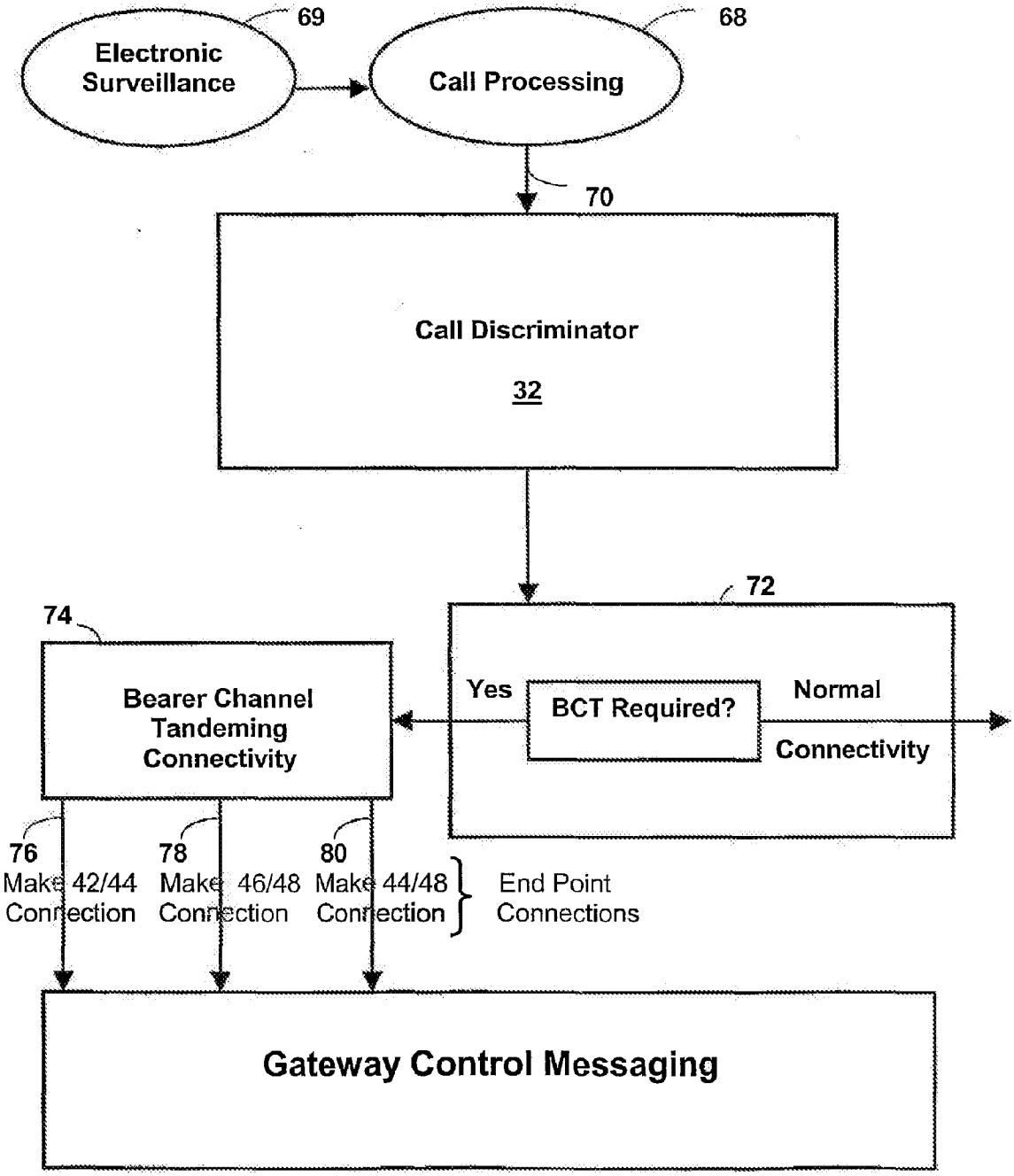

69
Electronic Surveillance
68
Call Processing
70
Call Discriminator
32
72
74
Bearer Channel Tandeming Connectivity
Yes
BCT Required?
Normal
Connectivity
76
Make 42/44 Connection
78
Make 46/48 Connection
80
Make 44/48 Connection
End Point Connections
Gateway Control Messaging

Figure 5

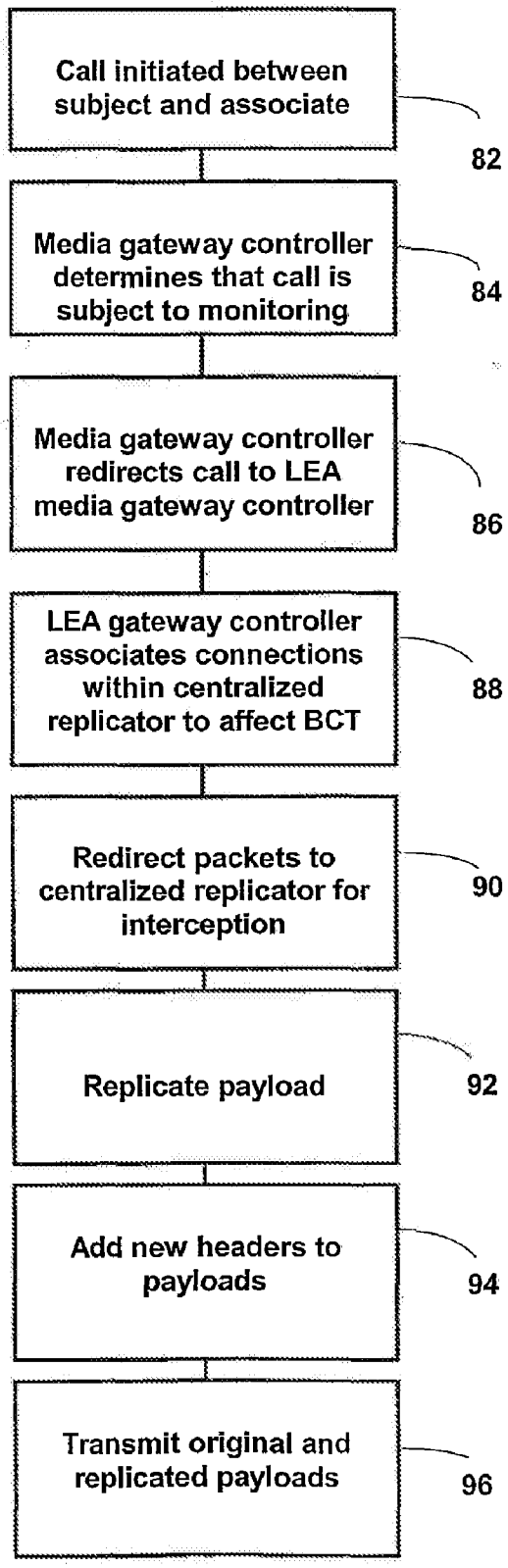

Call initiated between subject and associate
82
Media gateway controller determines that call is subject to monitoring
84
Media gateway controller redirects call to LEA media gateway controller
86
LEA gateway controller associates connections within centralized replicator to affect BCT
88
Redirect packets to centralized replicator for interception
90
Replicate payload
92
Add new headers to payloads
94
Transmit original and replicated payloads
96

Figure 6

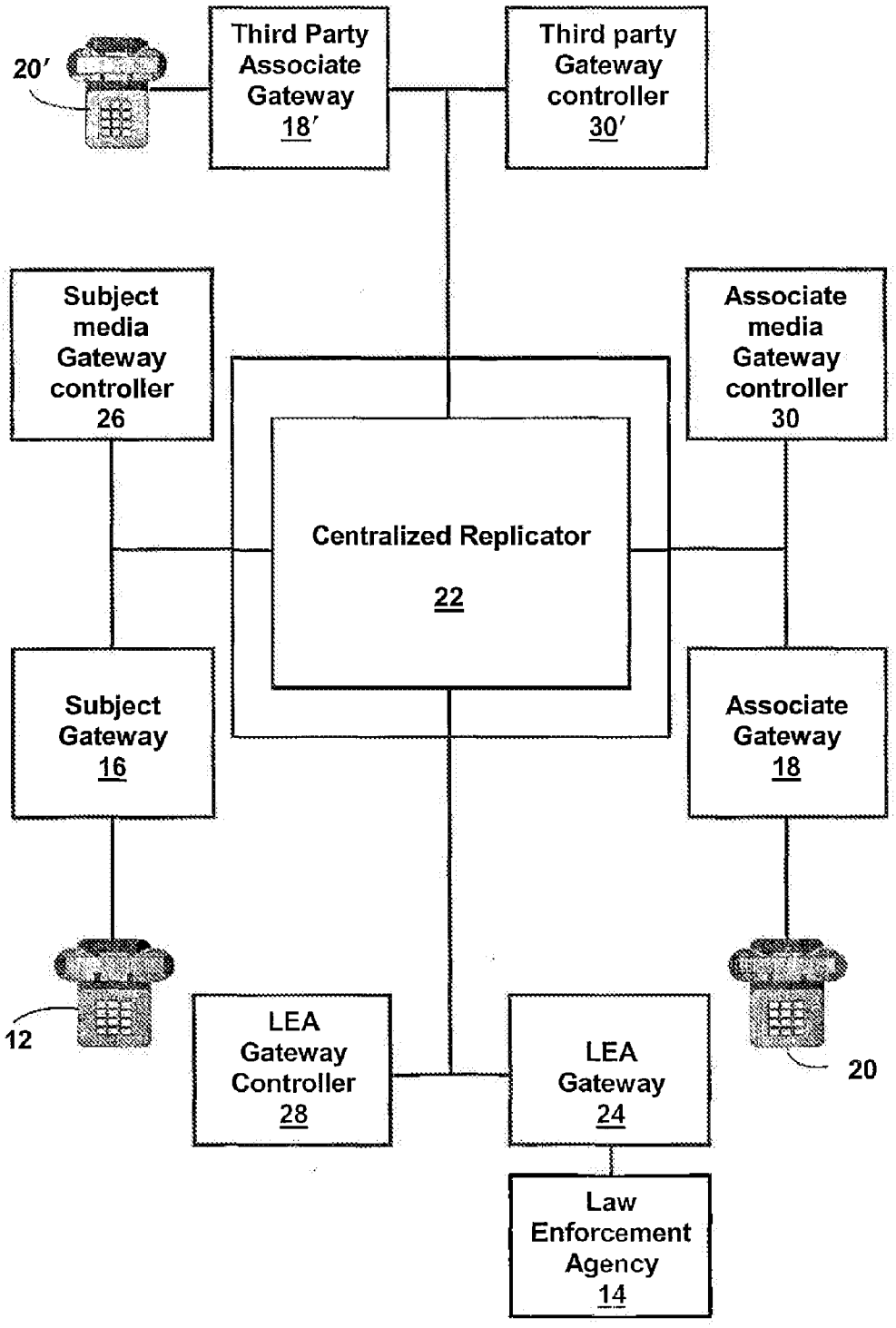

20′
Third Party Associate Gateway 18′
Third party Gateway controller 30′
Subject media Gateway controller 26
Associate media Gateway controller 30
Centralized Replicator 22
Subject Gateway 16
Associate Gateway 18
12
20
LEA Gateway Controller 28
LEA Gateway 24
Law Enforcement Agency 14

Figure 7

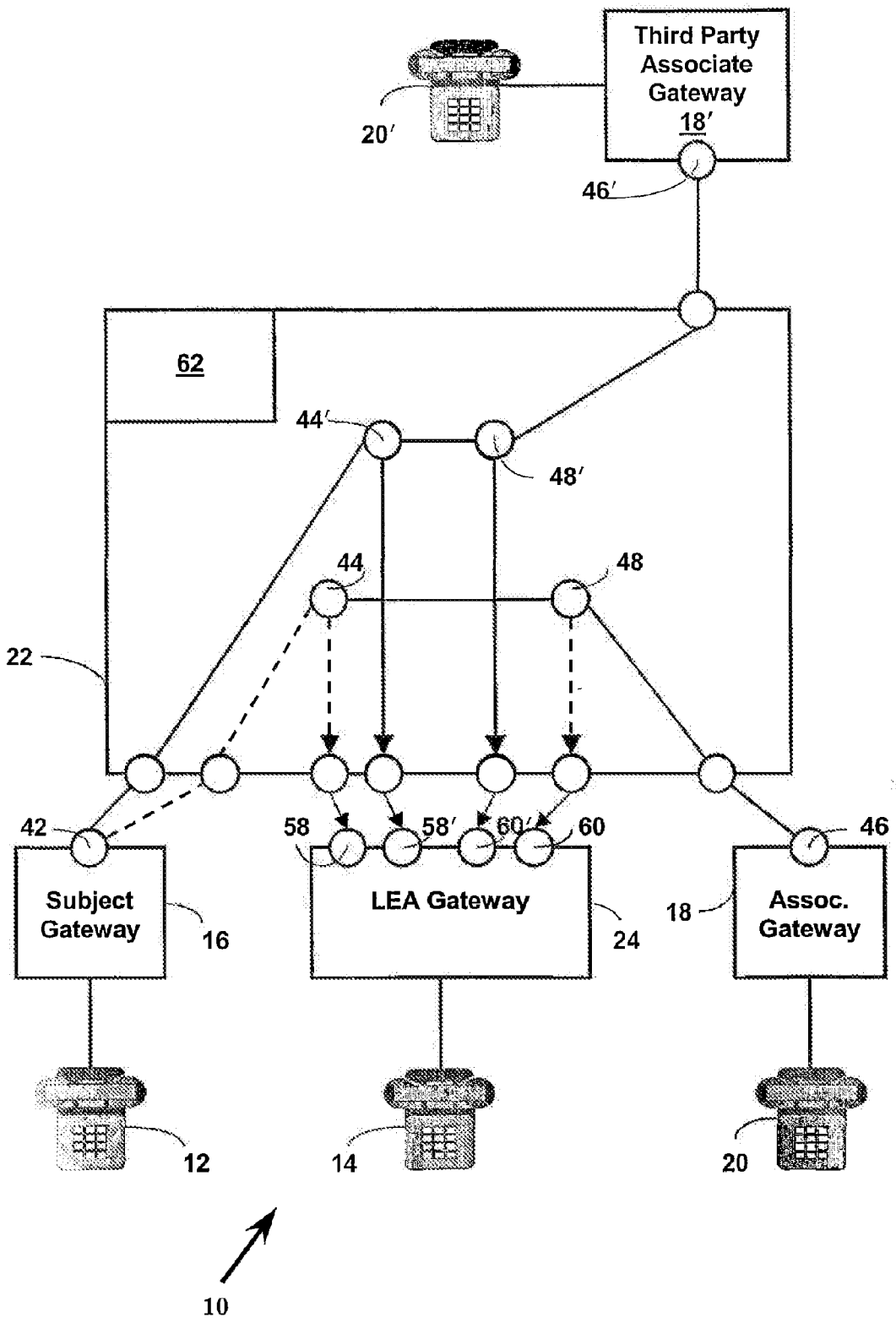

Third Party Associate Gateway 18′
20′
46′
62
44′
48′
44
48
22
42
58
58′
60′
60
46
Subject Gateway
16
LEA Gateway
24
18
Assoc. Gateway
12
14
20
10

Figure 8

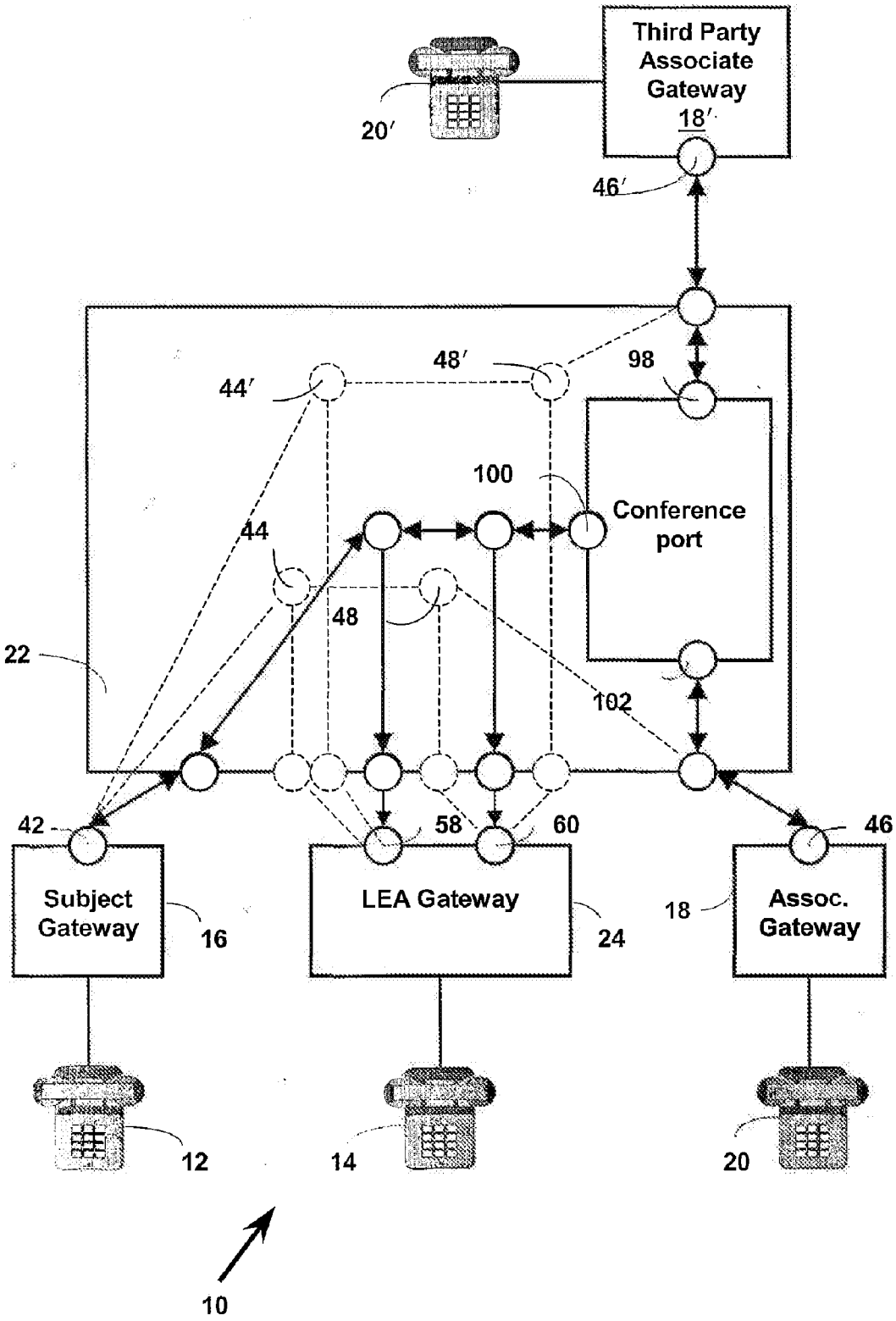

Third Party Associate Gateway
18′
20′
46′
48′
44′
98
100
Conference port
44
48
22
102
42
58
60
46
Subject Gateway
16
LEA Gateway
24
18
Assoc. Gateway
12
14
20
10

Figure 9

Espacenet

Bibliographic data: CA2690236 (A1) — 2008-12-18

SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

Inventor(s): PURNADI RENE W [US]; ISLAM M KHALEDUL [CA] + (PURNADI, RENE W, ; ISLAM, M. KHALEDUL)

Applicant(s): RESEARCH IN MOTION LTD [CA] + (RESEARCH IN MOTION LIMITED)

Classification: - international: ***H04L12/66; H04M11/06; H04Q3/64***
- cooperative: **H04M3/5116**; **H04Q3/64**; H04L65/1016; H04M1/72538; H04Q2213/13152; H04Q2213/13176; H04Q2213/13204; H04Q2213/13248; H04Q2213/13348; H04Q2213/1337; H04Q2213/13389

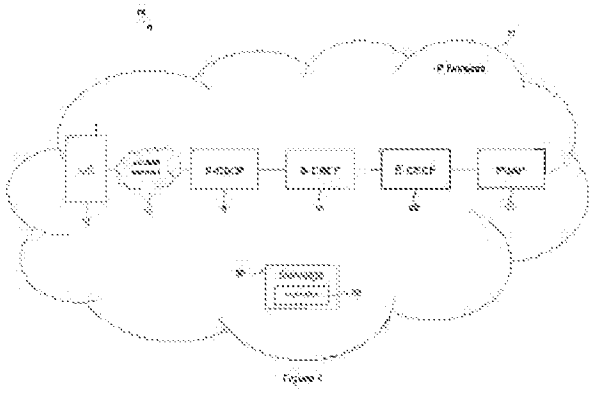
Application number: CA20072690236 20071204

Priority number(s): US20070944258P 20070615 ; WO2007CA02176 20071204

Also published as: WO2008151406 (A1) WO2008151406 (A8) US2008310599 (A1) MX2009013633 (A) KR20120051078 (A) KR101162903 (B1) KR20100029124 (A) KR101162847 (B1) EP2165489 (A1) EP2165489 (A4) CN101772929 (A) CN101772929 (B) less

Abstract of CA2690236 (A1)

A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.



Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2690236 A1 2008/12/18

(21) 2 690 236

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/12/04
(87) Date publication PCT/PCT Publication Date: 2008/12/18
(85) Entrée phase nationale/National Entry: 2009/12/09
(86) N° demande PCT/PCT Application No.: CA 2007/002176
(87) N° publication PCT/PCT Publication No.: 2008/151406
(30) Priorité/Priority: 2007/06/15 (US60/944,258)

(51) Cl.Int./Int.Cl. *H04L 12/66* (2006.01),
H04M 11/06 (2006.01), *H04Q 3/64* (2006.01)

(71) Demandeur/Applicant:
RESEARCH IN MOTION LIMITED, CA

(72) Inventeurs/Inventors:
PURNADI, RENE W., US;
ISLAM, M. KHALEDUL, CA

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME ET PROCEDE POUR INDIQUER UN RAPPEL D'URGENCE A UN EQUIPEMENT UTILISATEUR
(54) Title: SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

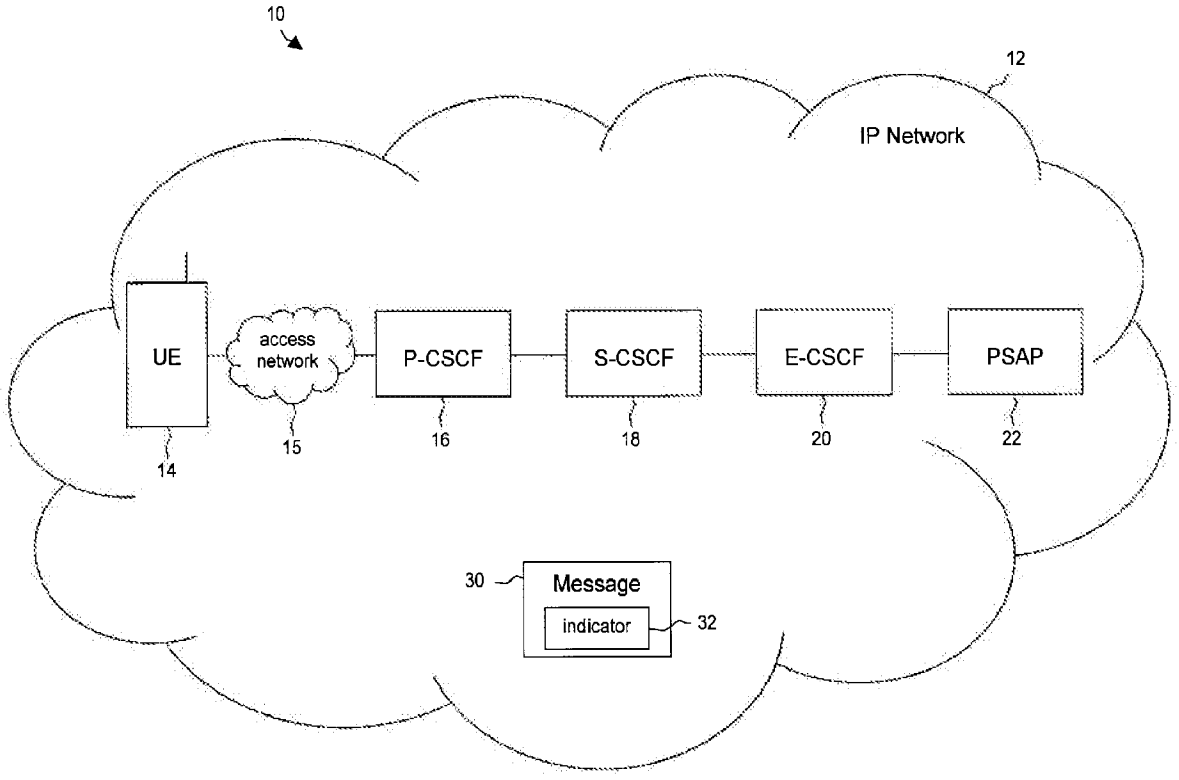


Figure 1

(57) Abrégé/Abstract:
A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.

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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 December 2008 (18.12.2008)

PCT

(10) International Publication Number
WO 2008/151406 A8

(51) International Patent Classification:
H04L 12/66 (2006.01) *H04Q 3/64* (2006.01)
H04M 11/06 (2006.01)

(21) International Application Number:
PCT/CA2007/002176

(22) International Filing Date:
4 December 2007 (04.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/944,258 15 June 2007 (15.06.2007) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PURNADI, Rene W.** [US/US]; 118 Elm Fork Drive, Coppell, Texas 75019 (US). **ISLAM, M. Khaledul** [CA/CA]; 88 Broughton Street, Ottawa, Ontario K2K 3N4 (CA).

(74) Agents: **WONG, Jeffrey W.** et al.; Borden Ladner Gervais LLP, World Exchange Plaza, 100 Queen Street, Suite 1100, Ottawa, Ontario K1P 1J9 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, 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:
with international search report (Art. 21(3))

(48) Date of publication of this corrected version:
28 January 2010

(15) Information about Correction:
see Notice of 28 January 2010

(54) Title: SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

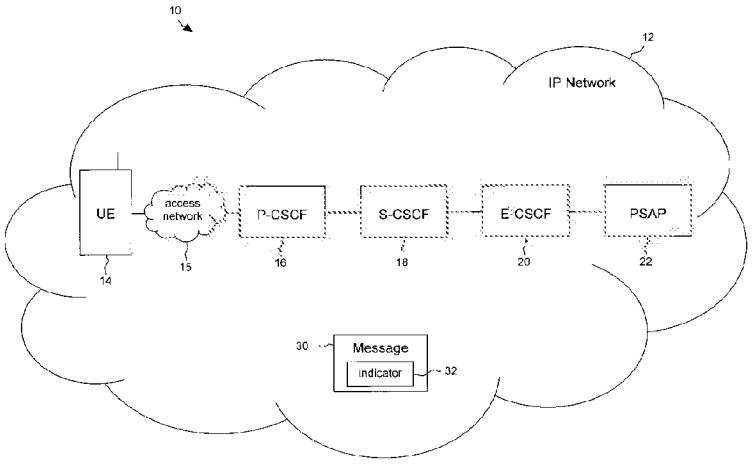


Figure 1

(57) Abstract: A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.

WO 2008/151406 A8

SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority to U.S. Provisional Patent Application No. 60/944,258, filed 6/15/07 by Purnadi et al., entitled "System and Method for Indicating IMS Emergency Call Back to User Equipment" which is incorporated by reference herein as if reproduced in its entirety.

BACKGROUND

The IP (Internet Protocol) Multimedia Subsystem (IMS) is a standardized architecture for providing both mobile and fixed multimedia services that many telephony service providers are beginning to implement. The IMS architecture can include a collection of different functions (*i.e.*, network elements) that communicate using standard protocols.

A user of an IMS network using a mobile device or any user equipment (UE) may place an emergency call, such as a 911 call (in North America) or a 112 call (in most of Europe). Such calls are typically handled by a Public Safety Answering Point (PSAP), which might coordinate an appropriate response to the emergency. After an emergency call is terminated, the PSAP may place a call back to the user for various reasons. For example, if the emergency call appears to have terminated abnormally, the PSAP might call the user back to determine if the user wishes to convey any additional information. Alternatively, the PSAP might call the user back to ask for information that was inadvertently not requested in the initial call. Other reasons for a call back from a PSAP to an emergency caller after the termination of an emergency call may be familiar to one of skill in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of this disclosure, reference is now made to the following brief description, taken in connection with the accompanying drawings and detailed description, wherein like reference numerals represent like parts.

Figure 1 is a diagram of an illustrative IP network including a user equipment and a Public Safety Answering Point according to an embodiment of the disclosure.

Figure 2 is a sequence diagram illustrating a call flow according to an embodiment of the disclosure.

Figure 3 is a diagram of a wireless communications system including user equipment operable for some of the various embodiments of the disclosure.

Figure 4 is a block diagram of user equipment operable for some of the various embodiments of the disclosure.

Figure 5 is a diagram of a software environment that may be implemented on user equipment operable for some of the various embodiments of the disclosure.

Figure 6 is an illustrative general purpose computer system suitable for some of the various embodiments of the disclosure.

DETAILED DESCRIPTION

It should be understood at the outset that although illustrative implementations of one or more embodiments of the present disclosure are provided below, the disclosed systems and/or methods may be implemented using any number of techniques, whether currently known or in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, including the exemplary designs and implementations illustrated and described herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

In an embodiment, a method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment and an access network. The method comprises including in a message from a PSAP (Public Safety Answering Point) to the user equipment and the access network an indication that the emergency call back is from the PSAP.

In another embodiment, a user equipment is provided that includes a processor configured to recognize an IMS (Internet Protocol Multimedia Subsystem) call as an emergency call back from a PSAP.

In another embodiment, a system is provided that includes one or more processors and instructions. The instructions when executed by the one or more processors promote providing an emergency call back indicator in a message from a PSAP to user equipment (UE).

When a PSAP attempts an IMS call back to a UE after an IMS emergency call from the UE to the PSAP is terminated, undesirable results may occur if the UE does not recognize that the call back is from the PSAP. For example, the UE may treat the call back as a regular call and place it on hold or call waiting, the call back could be blocked, or the UE might otherwise fail to respond appropriately to the call back. The present disclosure provides for indicating an IMS emergency call back from a PSAP to a UE by including in the call back an indication to the UE that the call back is from the PSAP. This allows the UE to distinguish between emergency call backs and regular calls. The indication or indicator that identifies the call to the UE as a call back from a PSAP may be associated with the call in various manners, some of which will be discussed in greater detail below. Others will readily suggest themselves to one skilled in the art in light of the present disclosure. Other techniques are provided in U.S. Patent Nos. 7,050,785 and 7,139,549, both by Islam et al, which are incorporated herein by reference for all purposes.

Figure 1 illustrates a system 10 including an IP (Internet Protocol) network 12, which may also include one or more components of an IMS network. A UE 14 is shown and may include any end user device or system (*e.g.*, mobile phone, mobile wireless device (including digital, cellular, or dual mode devices) personal digital assistant, laptop/tablet/notebook computer, desktop computer, etc.) that connects to an IMS network. A CSCF (Call Session Control Function) (not explicitly shown) is a well known element in an IMS network responsible, for example, for maintaining a SIP (Session Initiation Protocol) call and providing session control for subscribers accessing services within an IMS network.

The UE 14 communicates via an access network 15 with a P-CSCF (Proxy CSCF) 16. The access network 15 might be any well known set of components, such as base stations and other radio transmission and reception equipment, that can promote wireless connections to subsequent network components. The P-CSCF 16 is a SIP proxy that may be the first point of contact for the IMS terminal and may be located in the visited network in full IMS networks or in the home network if the visited network is not yet IMS-compliant. The P-CSCF 16 communicates with an S-CSCF (Serving CSCF) 18. The S-CSCF 18 is a SIP server that may be located in the home network and that may perform session control, downloading and uploading of user profiles, and other functions. The S-CSCF 18 communicates with an E-

CSCF (Emergency CSCF) 20. The E-CSCF 20 provides session control functions for a PSAP (Public Safety Answering Point) 22, which may be a 911 system or another emergency call center or system.

To make an emergency or 911 call, the UE 14 might communicate with the PSAP 22 via the P-CSCF 16, S-CSCF 18, and E-CSCF 20. However, communication via the P-CSCF 16 might occur only when the UE 14 is roaming. When the UE 14 is in its home network, there may be no need for the P-CSCF 16, and the UE 14 might communicate directly with the S-CSCF 18. Hereinafter, any communication that is described as occurring via the P-CSCF 16 should be understood as possibly occurring without the presence of the P-CSCF 16.

Current 3GPP (3rd Generation Partnership Project) and 3GPP2 (3rd Generation Partnership Project 2) specifications (TS 23.167 in 3GPP and X.P0049 in 3GPP2) do not specify a method for the UE 14 to determine whether an incoming call is in fact a call back from an emergency system, such as the PSAP 22. According to one embodiment, the PSAP 22 provides an IMS emergency call back message 30, such as a SIP Invite, that includes an emergency call back indication or indicator 32. The UE 14 can use the indicator 32 to identify a call as an IMS emergency call back from the PSAP 22 and can then respond appropriately to the call back. For example, the UE 14 might use the indicator 32 to set a proper priority during bearer setup with the access network 15, might drop and block other calls if necessary, or might take other actions to promote or increase the likelihood of successfully completing the emergency call back. The indicator 32 may also allow the UE 14 to provide events, such as audible or video displayed alerts, that notify the UE user about the incoming emergency call back.

The UE 14 may also use the indicator 32 to trigger an action if the UE user has not responded to the call back after a certain time has elapsed. A failure to answer an emergency call back in a timely manner might be an indication that the user is incapacitated or is otherwise in need of emergency services. When no response to an emergency call back occurs within a predefined length of time after the indicator 32 is received, the UE 14 might initiate an automatic reply to the PSAP 22 that indicates that the user is unable to respond, might send the location coordinates of the UE 14, might send an automated message to another emergency system, or might trigger other actions. For example, the UE 14 might complete the call without

physical input from the user, which might be useful when the user is unable to physically activate the UE 14 to receive the call. The P-CSCF 16 can provide the emergency call back indicator 32 to the access network 15 and the access network 15 can use the emergency call back indicator 32 to prepare and prioritize the appropriate resources for the emergency call back.

The emergency call back indicator 32 may be conveyed based on the current specifications in a variety of manners. However, the present disclosure is not so limited and is applicable in a variety of different systems and environments. In one embodiment, the indicator 32 may be provided by including the PSAP public identifier (PSAP PUID) in a SIP message sent from the PSAP 22 to the UE 14 after termination of an emergency call from the UE 14. More specifically, the PSAP PUID could be included in a SIP Invite message as the indicator 32. In this case, it may be useful for the PSAP PUID to have a standard naming convention or format, such as name@sos.domain, psap@domain, and so on, that identifies the PSAP 22 as an emergency-related entity. That is, words or arrangements of letters, numbers, or other characters, such as 'psap', 'sos', or 'emergency', might be used in the SIP Invite to indicate that the message 30 is from an emergency system, such as the PSAP 22.

The PSAP PUID may be provided in various locations in the SIP Invite message sent from the PSAP 22 to the UE 14. For example, the PSAP PUID could be placed in the 'From Header' that typically provides information on the identify of the sender of a SIP message. The standardized PSAP PUID format in the SIP Invite 'From Header' may make the SIP Invite readily recognizable by the UE 14 as a message associated with an emergency call back from PSAP 22. That is, the UE 14 might check the 'From Header' for a name or string, such as 'psap', 'sos', or 'emergency', that indicates that the SIP Invite is from the PSAP 22. If such a string is found, the UE 14 knows that the message is from the PSAP 22 and responds accordingly. The UE 14 might check every SIP Invite message for the name or string or might check only for some period of time after the UE 14 places a 911 or other emergency call.

In another embodiment, the UE emergency public identifier (ePUID) may be used as the indicator 32. As background, the UE 14 currently obtains an ePUID, which is different from the standard PUID, only when it performs an IMS emergency registration. However, under the current guidelines, the UE 14 performs an IMS emergency registration only when the UE 14

places an emergency call while outside its home network or only when the UE 14 does not have enough credentials to perform IMS regular registration. Therefore, the ePUID might not always be available for use as the indicator 32.

The present embodiment provides that the UE 14 performs an emergency IMS registration whenever the UE 14 places an emergency call, regardless of whether it is in its home network or roaming and regardless of whether it has enough credentials for regular registration. The UE 14 would then have an ePUID even when it makes an emergency call from within its home network and could provide the ePUID to the PSAP 22 whenever it makes an emergency call. When the PSAP 22 makes an emergency call back to the UE 14, the PSAP 22 could then use the ePUID as the indicator 32 in the message 30. More specifically, the ePUID could be placed in the SIP Invite 'To Header', which identifies the recipient of a SIP message. When the UE 14 receives a message that includes its own ePUID, such as a SIP Invite that has the UE ePUID in the 'To Header', the UE 14 could recognize the message as being associated with an emergency call back from the PSAP 22 and could respond appropriately.

In other embodiments, the emergency call back indicator 32 may be included in a SIP Invite from the PSAP 22 to the UE 14 in numerous other ways. For example, an explicit new emergency call back header might be added, or an implicit emergency call back indicator 32 might be placed inside an existing header, such as the P-Asserted-Identity header. Alternatively, other messages 30 may include or may be used as the indicator 32, or a myriad of other ways or techniques could be employed which will readily suggest themselves to one skilled in the art in view of the present disclosure.

Figure 2 illustrates an exemplary call flow diagram for a UE 14 that has previously initiated an IMS emergency call session using its standard PUID. In this embodiment, when the emergency call is terminated, the PSAP 22 attempts an emergency call back to the UE 14 using a SIP Invite message. The SIP Invite includes the UE PUID in the 'To Header' and includes a standardized or recognized PSAP PUID, such as name@sos.domain, in the 'From Header'. The standardized PSAP PUID format used in the 'From Header' is recognized by the P-CSCF 16 (or the S-CSCF 18 when the P-CSCF 16 is not present) and by the UE 14 as an indication of an emergency call back from the PSAP 22. The P-CSCF 16 or S-CSCF 20 triggers the access

network 15 so UE 14 and the access network 15 may then set the highest priority for the call to ensure a successful emergency call back and/or may perform other actions, as discussed above.

At event 202, responsive to abnormal emergency call termination, or for some other reason, the PSAP 22 initiates a call back to the UE 14. The PSAP 22 forms a SIP Invite message that includes the UE PUID in the 'To Header' and uses the standardized or recognized PSAP PUID format as the indicator in the 'From Header'. In this example, the PSAP PUID uses name@sos.domain as the standard format. The 'sos' in the SIP Invite originating from the PSAP 22 indicates to the UE 14 that this is an emergency call back. However, other parameters placed in other locations in the SIP Invite message or in other messages may also be used as the indicator. The SIP Invite formed in this manner is then sent to the E-CSCF 20.

At event 204, the E-CSCF 20 forwards the SIP Invite to the S-CSCF 18. At event 206, the S-CSCF 18 forwards the SIP Invite to the P-CSCF 16. At event 208, the P-CSCF 16 forwards the SIP Invite to the UE 14. The P-CSCF 16 may use the emergency call back indicator as a trigger to inform an access network to prepare and prioritize resources for the emergency call back. At event 210, the UE 14 examines the 'From Header' in the incoming SIP Invite and recognizes 'sos' as the standardized format indicating that the SIP Invite is from the PSAP 22 and is associated with an emergency call back. The UE 14 may then use this indication to put the call in the highest priority to assure a successful emergency call back. The UE 14 may take other actions as well, including dropping other ongoing calls, setting proper priority during the radio bearer setup procedure, and so on.

At event 212, the UE 14 forms a SIP 200OK message to respond to the SIP Invite. The UE 14 places the PSAP PUID in the 'To Header' and its own UE PUID in the 'From Header'. The SIP 200OK is then sent to the P-CSCF 16. As a note, according to the 3GPP2 specification, the P-CSCF 16 may not allow an emergency call initialization by means of a SIP Invite that has a PSAP PUID in the 'To Header'. However, the message sent at event 212 is not a SIP Invite initialization message, but instead may be a SIP 200OK. Therefore, as indicated at event 214, the P-CSCF 16 does allow the message that has the PSAP PUID in the 'To Header'. It should be noted that the P-CSCF 16 typically needs to be aware of and ready to receive the SIP 200OK or else it might reject the SIP 200OK. After the P-CSCF 16 has received the SIP

Invite from the PSAP 22, the P-CSCF 16 can be made aware that the UE 14 might send the 200OK.

At events 216, 218, and 220, the P-CSCF 16 routes the SIP 200OK, via the S-CSCF 18 and the E-CSCF 20, to the PSAP 22. At event 222, the PSAP 22 forms a SIP ACK message to respond to the SIP 200OK. The PSAP 22 puts the UE PUID in the 'To Header' and its own PSAP PUID in the 'From Header' and sends the SIP ACK to the E-CSCF 20. At events 224, 226, and 228, the SIP ACK is then routed via the S-CSCF 18 and the P-CSCF 16 to the UE 14. At this point, the setup of the emergency call back is complete, as indicated at event 230. It should be appreciated that Figure 2 is merely illustrative of one call flow for one embodiment of the present disclosure and that the present disclosure is not limited to only the illustrated call flow. Other call flows would occur for the numerous other embodiments disclosed herein.

Figure 3 illustrates a wireless communications system including an embodiment of the UE 14. The UE 14 is operable for implementing aspects of the disclosure, but the disclosure should not be limited to these implementations. Though illustrated as a mobile phone, the UE 14 may take various forms including a wireless handset, a pager, a personal digital assistant (PDA), a portable computer, a tablet computer, or a laptop computer. Many suitable devices combine some or all of these functions. In some embodiments of the disclosure, the UE 14 is not a general purpose computing device like a portable, laptop or tablet computer, but rather is a special-purpose communications device such as a mobile phone, a wireless handset, a pager, a PDA, or a telecommunications device installed in a vehicle. In another embodiment, the UE 14 may be a portable, laptop or other computing device. The UE 14 may support specialized activities such as gaming, inventory control, job control, and/or task management functions, and so on.

The UE 14 includes a display 402. The UE 14 also includes a touch-sensitive surface, a keyboard or other input keys generally referred as 404 for input by a user. The keyboard may be a full or reduced alphanumeric keyboard such as QWERTY, Dvorak, AZERTY, and sequential types, or a traditional numeric keypad with alphabet letters associated with a telephone keypad. The input keys may include a trackwheel, an exit or escape key, a trackball, and other navigational or functional keys, which may be inwardly depressed to provide further

input function. The UE 14 may present options for the user to select, controls for the user to actuate, and/or cursors or other indicators for the user to direct.

The UE 14 may further accept data entry from the user, including numbers to dial or various parameter values for configuring the operation of the UE 14. The UE 14 may further execute one or more software or firmware applications in response to user commands. These applications may configure the UE 14 to perform various customized functions in response to user interaction. Additionally, the UE 14 may be programmed and/or configured over-the-air, for example from a wireless base station, a wireless access point, or a peer UE 14.

Among the various applications executable by the UE 14 are a web browser, which enables the display 402 to show a web page. The web page may be obtained via wireless communications with a wireless network access node, a cell tower, a peer UE 14, or any other wireless communication network or system 400. The network 400 is coupled to a wired network 408, such as the Internet. Via the wireless link and the wired network, the UE 14 has access to information on various servers, such as a server 410. The server 410 may provide content that may be shown on the display 402. Alternately, the UE 14 may access the network 400 through a peer UE 14 acting as an intermediary, in a relay type or hop type of connection.

Figure 4 shows a block diagram of the UE 14. While a variety of known components of UEs 14 are depicted, in an embodiment a subset of the listed components and/or additional components not listed may be included in the UE 14. The UE 14 includes a digital signal processor (DSP) 502 and a memory 504. As shown, the UE 14 may further include an antenna and front end unit 506, a radio frequency (RF) transceiver 508, an analog baseband processing unit 510, a microphone 512, an earpiece speaker 514, a headset port 516, an input/output interface 518, a removable memory card 520, a universal serial bus (USB) port 522, a short range wireless communication sub-system 524, an alert 526, a keypad 528, a liquid crystal display (LCD), which may include a touch sensitive surface 530, an LCD controller 532, a charge-coupled device (CCD) camera 534, a camera controller 536, and a global positioning system (GPS) sensor 538. In an embodiment, the UE 14 may include another kind of display that does not provide a touch sensitive screen. In an embodiment, the DSP 502 may communicate directly with the memory 504 without passing through the input/output interface 518.

The DSP 502 or some other form of controller or central processing unit operates to control the various components of the UE 14 in accordance with embedded software or firmware stored in memory 504 or stored in memory contained within the DSP 502 itself. In addition to the embedded software or firmware, the DSP 502 may execute other applications stored in the memory 504 or made available via information carrier media such as portable data storage media like the removable memory card 520 or via wired or wireless network communications. The application software may comprise a compiled set of machine-readable instructions that configure the DSP 502 to provide the desired functionality, or the application software may be high-level software instructions to be processed by an interpreter or compiler to indirectly configure the DSP 502.

The antenna and front end unit 506 may be provided to convert between wireless signals and electrical signals, enabling the UE 14 to send and receive information from a cellular network or some other available wireless communications network or from a peer UE 14. In an embodiment, the antenna and front end unit 506 may include multiple antennas to support beam forming and/or multiple input multiple output (MIMO) operations. As is known to those skilled in the art, MIMO operations may provide spatial diversity which can be used to overcome difficult channel conditions and/or increase channel throughput. The antenna and front end unit 506 may include antenna tuning and/or impedance matching components, RF power amplifiers, and/or low noise amplifiers.

The RF transceiver 508 provides frequency shifting, converting received RF signals to baseband and converting baseband transmit signals to RF. In some descriptions a radio transceiver or RF transceiver may be understood to include other signal processing functionality such as modulation/demodulation, coding/decoding, interleaving/deinterleaving, spreading/despreading, inverse fast Fourier transforming (IFFT)/fast Fourier transforming (FFT), cyclic prefix appending/removal, and other signal processing functions. For the purposes of clarity, the description here separates the description of this signal processing from the RF and/or radio stage and conceptually allocates that signal processing to the analog baseband processing unit 510 and/or the DSP 502 or other central processing unit. In some embodiments, the RF Transceiver 508, portions of the Antenna and Front End 506, and the

analog baseband processing unit 510 may be combined in one or more processing units and/or application specific integrated circuits (ASICs).

The analog baseband processing unit 510 may provide various analog processing of inputs and outputs, for example analog processing of inputs from the microphone 512 and the headset 516 and outputs to the earpiece 514 and the headset 516. To that end, the analog baseband processing unit 510 may have ports for connecting to the built-in microphone 512 and the earpiece speaker 514 that enable the UE 14 to be used as a cell phone. The analog baseband processing unit 510 may further include a port for connecting to a headset or other hands-free microphone and speaker configuration. The analog baseband processing unit 510 may provide digital-to-analog conversion in one signal direction and analog-to-digital conversion in the opposing signal direction. In some embodiments, at least some of the functionality of the analog baseband processing unit 510 may be provided by digital processing components, for example by the DSP 502 or by other central processing units.

The DSP 502 may perform modulation/demodulation, coding/decoding, interleaving/deinterleaving, spreading/despreading, inverse fast Fourier transforming (IFFT)/fast Fourier transforming (FFT), cyclic prefix appending/removal, and other signal processing functions associated with wireless communications. In an embodiment, for example in a code division multiple access (CDMA) technology application, for a transmitter function the DSP 502 may perform modulation, coding, interleaving, and spreading, and for a receiver function the DSP 502 may perform despreading, deinterleaving, decoding, and demodulation. In another embodiment, for example in an orthogonal frequency division multiplex access (OFDMA) technology application, for the transmitter function the DSP 502 may perform modulation, coding, interleaving, inverse fast Fourier transforming, and cyclic prefix appending, and for a receiver function the DSP 502 may perform cyclic prefix removal, fast Fourier transforming, deinterleaving, decoding, and demodulation. In other wireless technology applications, yet other signal processing functions and combinations of signal processing functions may be performed by the DSP 502.

The DSP 502 may communicate with a wireless network via the analog baseband processing unit 510. In some embodiments, the communication may provide Internet connectivity, enabling a user to gain access to content on the Internet and to send and receive e-

mail or text messages. The input/output interface 518 interconnects the DSP 502 and various memories and interfaces. The memory 504 and the removable memory card 520 may provide software and data to configure the operation of the DSP 502. Among the interfaces may be the USB interface 522 and the short range wireless communication sub-system 524. The USB interface 522 may be used to charge the UE 14 and may also enable the UE 14 to function as a peripheral device to exchange information with a personal computer or other computer system. The short range wireless communication sub-system 524 may include an infrared port, a Bluetooth interface, an IEEE 802.11 compliant wireless interface, or any other short range wireless communication sub-system, which may enable the UE 14 to communicate wirelessly with other nearby mobile devices and/or wireless base stations.

The input/output interface 518 may further connect the DSP 502 to the alert 526 that, when triggered, causes the UE 14 to provide a notice to the user, for example, by ringing, playing a melody, or vibrating. The alert 526 may serve as a mechanism for alerting the user to any of various events such as an incoming call, a new text message, and an appointment reminder by silently vibrating, or by playing a specific pre-assigned melody for a particular caller.

The keypad 528 couples to the DSP 502 via the interface 518 to provide one mechanism for the user to make selections, enter information, and otherwise provide input to the UE 14. The keyboard 528 may be a full or reduced alphanumeric keyboard such as QWERTY, Dvorak, AZERTY and sequential types, or a traditional numeric keypad with alphabet letters associated with a telephone keypad. The input keys may include a trackwheel, an exit or escape key, a trackball, and other navigational or functional keys, which may be inwardly depressed to provide further input function. Another input mechanism may be the LCD 530, which may include touch screen capability and also display text and/or graphics to the user. The LCD controller 532 couples the DSP 502 to the LCD 530.

The CCD camera 534, if equipped, enables the UE 14 to take digital pictures. The DSP 502 communicates with the CCD camera 534 via the camera controller 536. In another embodiment, a camera operating according to a technology other than Charge Coupled Device cameras may be employed. The GPS sensor 538 is coupled to the DSP 502 to decode global positioning system signals, thereby enabling the UE 14 to determine its position. Various other

peripherals may also be included to provide additional functions, e.g., radio and television reception.

Figure 5 illustrates a software environment 602 that may be implemented by the DSP 502. The DSP 502 executes operating system drivers 604 that provide a platform from which the rest of the software operates. The operating system drivers 604 provide drivers for the wireless device hardware with standardized interfaces that are accessible to application software. The operating system drivers 604 include application management services ("AMS") 606 that transfer control between applications running on the UE 14. Also shown in Figure 5 are a web browser application 608, a media player application 610, and Java applets 612. The web browser application 608 configures the UE 14 to operate as a web browser, allowing a user to enter information into forms and select links to retrieve and view web pages. The media player application 610 configures the UE 14 to retrieve and play audio or audiovisual media. The Java applets 612 configure the UE 14 to provide games, utilities, and other functionality. A component 614 might provide functionality related to emergency calls.

The UE 14, P-CSCF 16, S-CSCF 18, E-CSCF 20, and PSAP 22, as well as other components described herein, may be implemented in whole or part on, or may include, a general-purpose computer with sufficient processing power, memory resources, and network throughput capability to handle the necessary workload placed upon it. Figure 6 illustrates a typical, general-purpose computer system 700 that may be suitable for implementing one or more embodiments disclosed herein. The computer system 700 includes a processor 720 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 750, read only memory (ROM) 740, random access memory (RAM) 730, input/output (I/O) devices 710, and network connectivity devices 760. The processor may be implemented as one or more CPU chips.

The secondary storage 750 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 730 is not large enough to hold all working data. Secondary storage 750 may be used to store programs which are loaded into RAM 730 when such programs are selected for execution. The ROM 740 is used to store instructions and perhaps data which are read during program execution. ROM 740 is a non-volatile memory device which typically has a small memory

capacity relative to the larger memory capacity of secondary storage. The RAM 730 is used to store volatile data and perhaps to store instructions. Access to both ROM 740 and RAM 730 is typically faster than to secondary storage 750.

I/O devices 710 may include printers, video monitors, liquid crystal displays (LCDs), touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices.

The network connectivity devices 760 may take the form of modems, modem banks, ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards such as code division multiple access (CDMA) and/or global system for mobile communications (GSM) radio transceiver cards, and other well-known network devices. These network connectivity 760 devices may enable the processor 720 to communicate with an Internet or one or more intranets. With such a network connection, it is contemplated that the processor 720 might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Such information, which is often represented as a sequence of instructions to be executed using processor 720, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

Such information, which may include data or instructions to be executed using processor 720 for example, may be received from and outputted to the network, for example, in the form of a computer data baseband signal or signal embodied in a carrier wave. The baseband signal or signal embodied in the carrier wave generated by the network connectivity 760 devices may propagate in or on the surface of electrical conductors, in coaxial cables, in waveguides, in optical media, for example optical fiber, or in the air or free space. The information contained in the baseband signal or signal embedded in the carrier wave may be ordered according to different events, as may be desirable for either processing or generating the information or transmitting or receiving the information. The baseband signal or signal embedded in the carrier wave, or other types of signals currently used or hereafter developed, referred to herein as the transmission medium, may be generated according to several methods well known to one skilled in the art.

The processor 720 executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage 750), ROM 740, RAM 730, or the network connectivity devices 760. Although only one processor 720 is shown, multiple processors may be present. Instructions or processing discussed as accomplished by the processor may be simultaneously, serially, or otherwise a processed by one or more processors.

While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods may be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted, or not implemented.

Also, techniques, systems, subsystems and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as coupled or directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component, whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

CLAIMS

What is claimed is:

1. A method for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment and an access network, comprising:

including in a message from a PSAP (Public Safety Answering Point) to the user equipment and the access network an indication that the emergency call back is from the PSAP.

2. The method of claim 1, wherein the message is a SIP (Session Initiation Protocol) Invite message.

3. The method of claim 1, wherein the indication is included in a From Header.

4. The method of claim 1, wherein the indication is a string of characters that identifies the PSAP as an emergency-related entity.

5. The method of claim 1, wherein the indication is included in a To Header.

6. The method of claim 1, wherein the indication is an emergency public identifier of the user equipment.

7. The method of claim 6, wherein the emergency public identifier is created whenever the user equipment initiates an IMS emergency call.

8. The method of claim 1, further comprising the user equipment and the access network responding to the indication in a manner that promotes a successful completion of the emergency call back.

9. The method of claim 1, further comprising the user equipment triggering an autonomous action when the user equipment does not receive an input in response to the emergency call back within a predefined length of time after the user equipment receives the indication.

10. The method of claim 9, wherein the autonomous action is at least one of:
sending an automated message to the PSAP;
sending a location of the user equipment to the PSAP; and
sending an automated message to an emergency-related entity other than the PSAP.

11. The method of claim 2, wherein the user equipment inspects all incoming SIP Invite messages for the indication, and wherein a Proxy Call Session Control Function inspects all incoming SIP Invite messages for the indication to inform the access network to prepare and prioritize resources for the emergency call back.

12. The method of claim 2, wherein the user equipment inspects incoming SIP Invite messages for the indication only for a predefined length of time after the user equipment initiates an IMS emergency call to the PSAP.

13. A user equipment, comprising:
a processor configured to recognize an IMS (Internet Protocol Multimedia Subsystem) call as an emergency call back from a PSAP (Public Safety Answering Point).

14. The user equipment of claim 13, wherein the processor recognizes the IMS call as the emergency call back from the PSAP by the IMS call including an emergency call back indicator.

15. The user equipment of claim 14, wherein the emergency call back indicator is a string of characters that identifies the PSAP as an emergency-related entity and that is included in a SIP (Session Initiation Protocol) Invite message from the PSAP to the user equipment.

16. The user equipment of claim 14, wherein the emergency call back indicator is included in a From Header.

17. The user equipment of claim 14, wherein the emergency call back indicator is an emergency public identifier of the user equipment that is included in a To Header.

18. The user equipment of claim 17, wherein the emergency public identifier is created whenever the user equipment initiates an IMS emergency call.

19. The user equipment of claim 14, wherein the user equipment triggers an autonomous action when the user equipment does not receive an input in response to the emergency call back within a predefined length of time after the user equipment receives the emergency call back indicator.

20. The user equipment of claim 19, wherein the autonomous action is at least one of:
sending an automated message to the PSAP;
sending a location of the user equipment to the PSAP; and
sending an automated message to an emergency-related entity other than the PSAP.

21. The user equipment of claim 14, wherein a Proxy Call Session Control Function inspects all incoming SIP Invite messages for the emergency call back indicator to inform the access network to prepare and prioritize resources for the emergency call back.

22. A system, comprising:
one or more processors; and
instructions that when executed by the one or more processors promote providing an emergency call back indicator in a message from a PSAP (Public Safety Answering Point) to user equipment.

23. The system of claim 22, wherein the emergency call back indicator is one of:
a string of characters that identifies the PSAP as an emergency-related entity and that is included in a From Header of a SIP (Session Initiation Protocol) Invite message from the PSAP to the user equipment; and
an emergency public identifier of the user equipment that is included in a To Header of the SIP Invite message and that is created whenever the user equipment initiates an IMS emergency call.

24. The system of claim 22, wherein the user equipment triggers an autonomous action when the user equipment does not receive an input in response to the emergency call back within a predefined length of time after the user equipment receives the emergency call back indicator.

25. The system of claim 24, wherein the autonomous action is at least one of:
sending an automated message to the PSAP;
sending a location of the user equipment to the PSAP; and
sending an automated message to an emergency-related entity other than the PSAP.

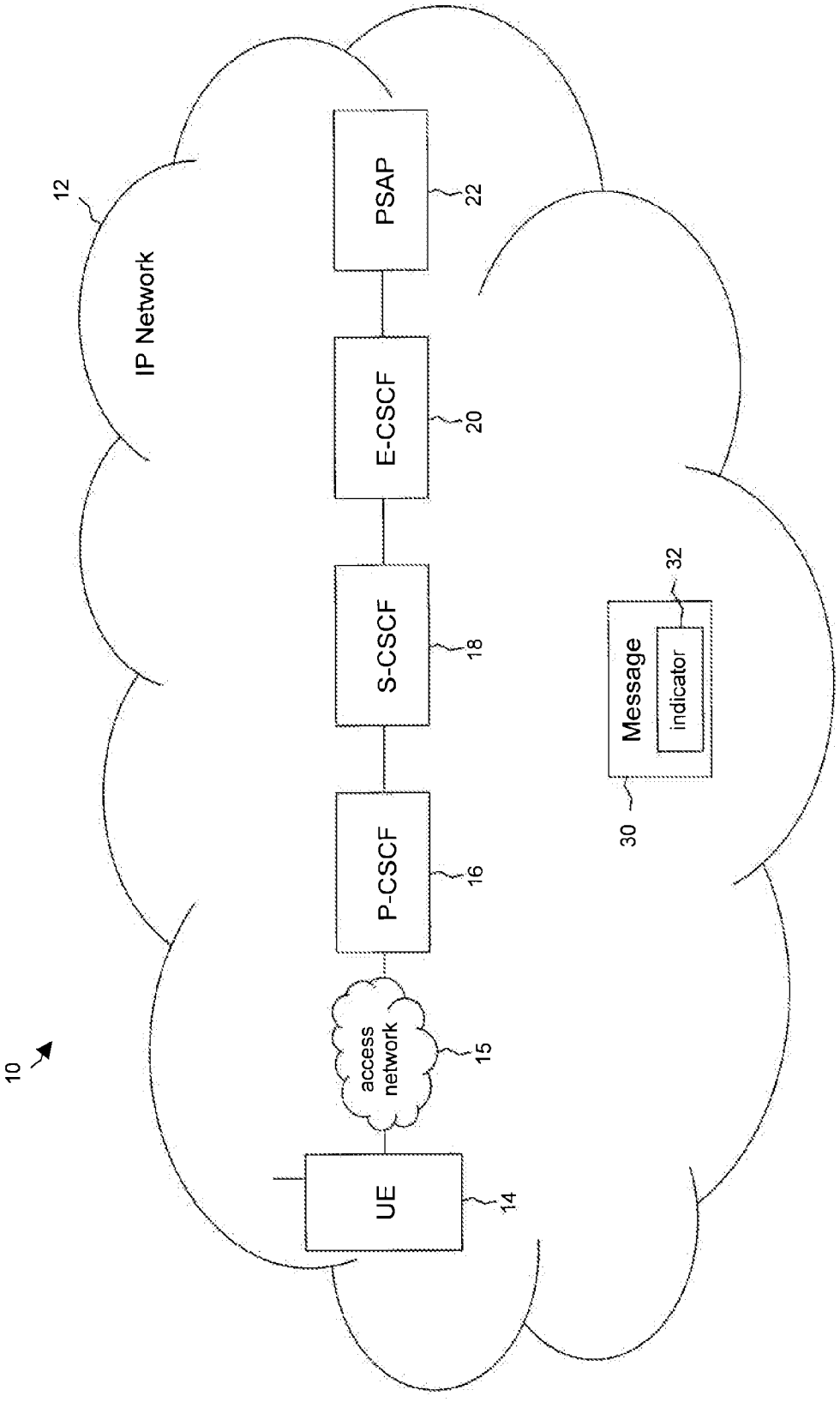

10
12
IP Network
PSAP
22
E-CSCF
20
S-CSCF
18
P-CSCF
16
access network
15
UE
14
Message
indicator
30
32

Figure 1

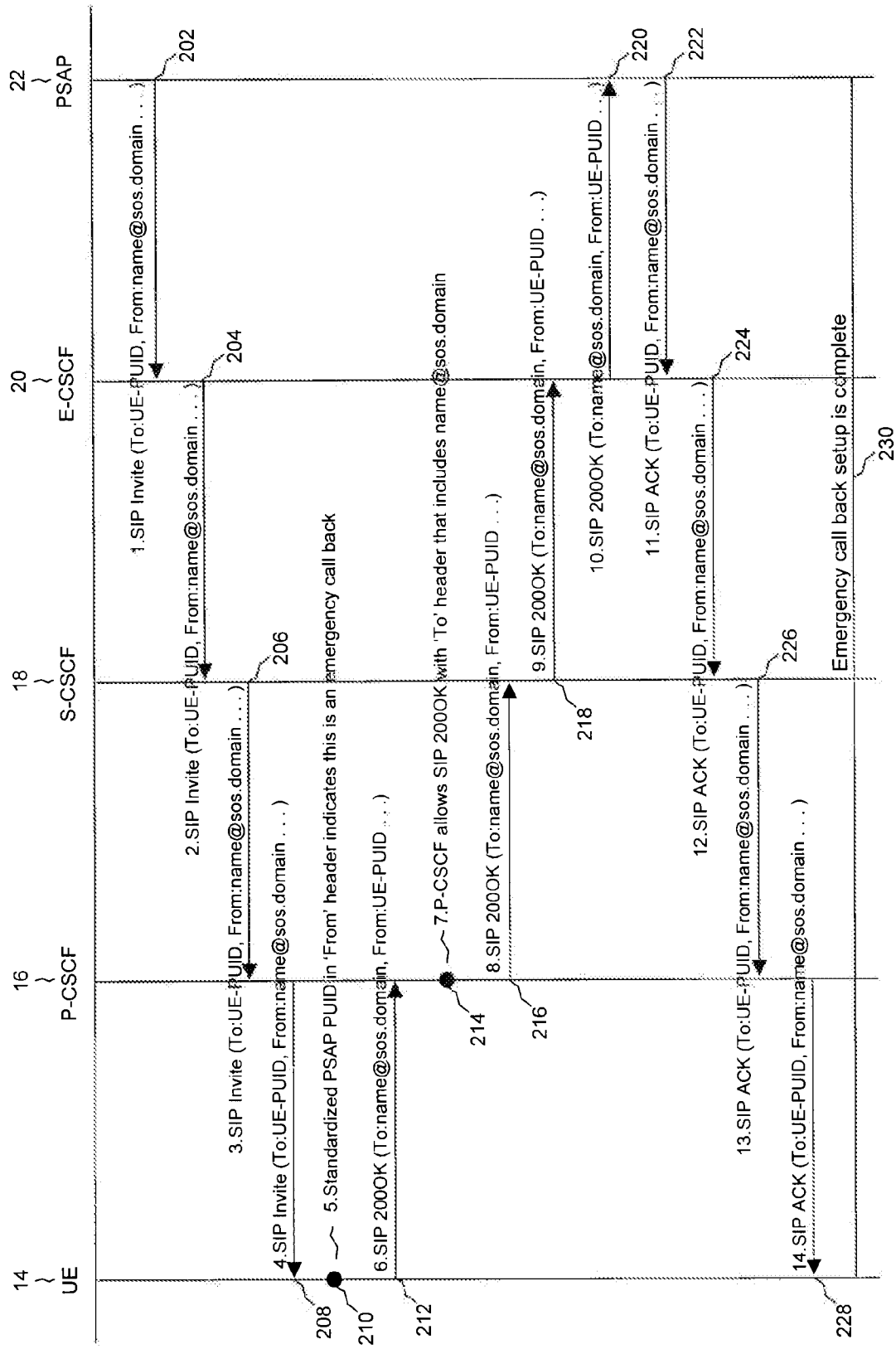

14 UE
16 P-CSCF
18 S-CSCF
20 E-CSCF
22 PSAP
1.SIP Invite (To:UE-PUID, From:name@sos.domain . . .)
2.SIP Invite (To:UE-PUID, From:name@sos.domain . . .)
3.SIP Invite (To:UE-PUID, From:name@sos.domain . . .)
4.SIP Invite (To:UE-PUID, From:name@sos.domain . . .)
5.Standardized PSAP PUID in 'From' header indicates this is an emergency call back
6.SIP 200OK (To:name@sos.domain, From:UE-PUID . . .)
7.P-CSCF allows SIP 200OK with 'To' header that includes name@sos.domain
8.SIP 200OK (To:name@sos.domain, From:UE-PUID . . .)
9.SIP 200OK (To:name@sos.domain, From:UE-PUID . . .)
10.SIP 200OK (To:name@sos.domain, From:UE-PUID . . .)
11.SIP ACK (To:UE-PUID, From:name@sos.domain . . .)
12.SIP ACK (To:UE-PUID, From:name@sos.domain . . .)
13.SIP ACK (To:UE-PUID, From:name@sos.domain . . .)
14.SIP ACK (To:UE-PUID, From:name@sos.domain . . .)
Emergency call back setup is complete
202
204
206
208
210
212
214
216
218
220
222
224
226
228
230

Figure 2

Fig. 3

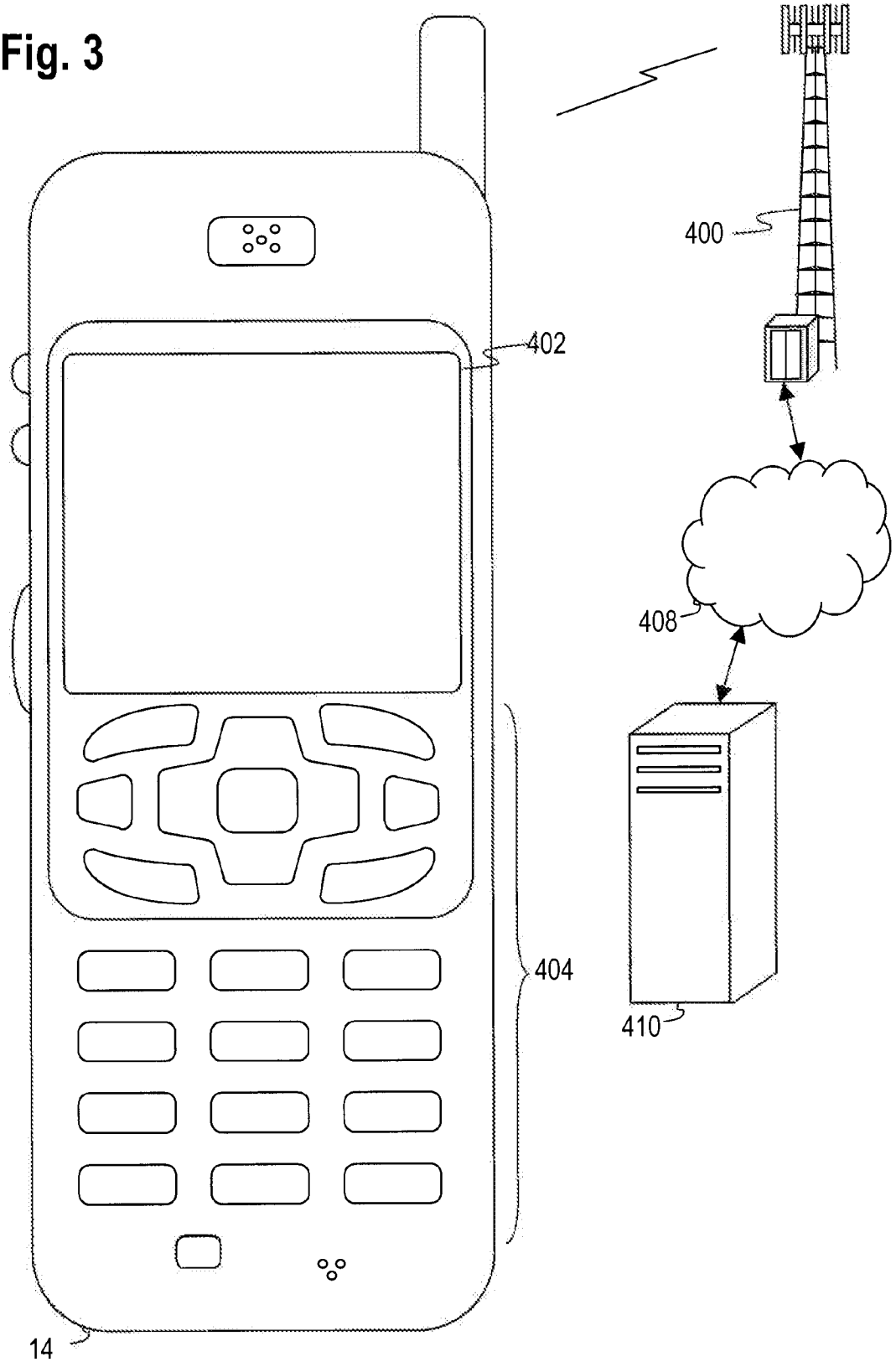
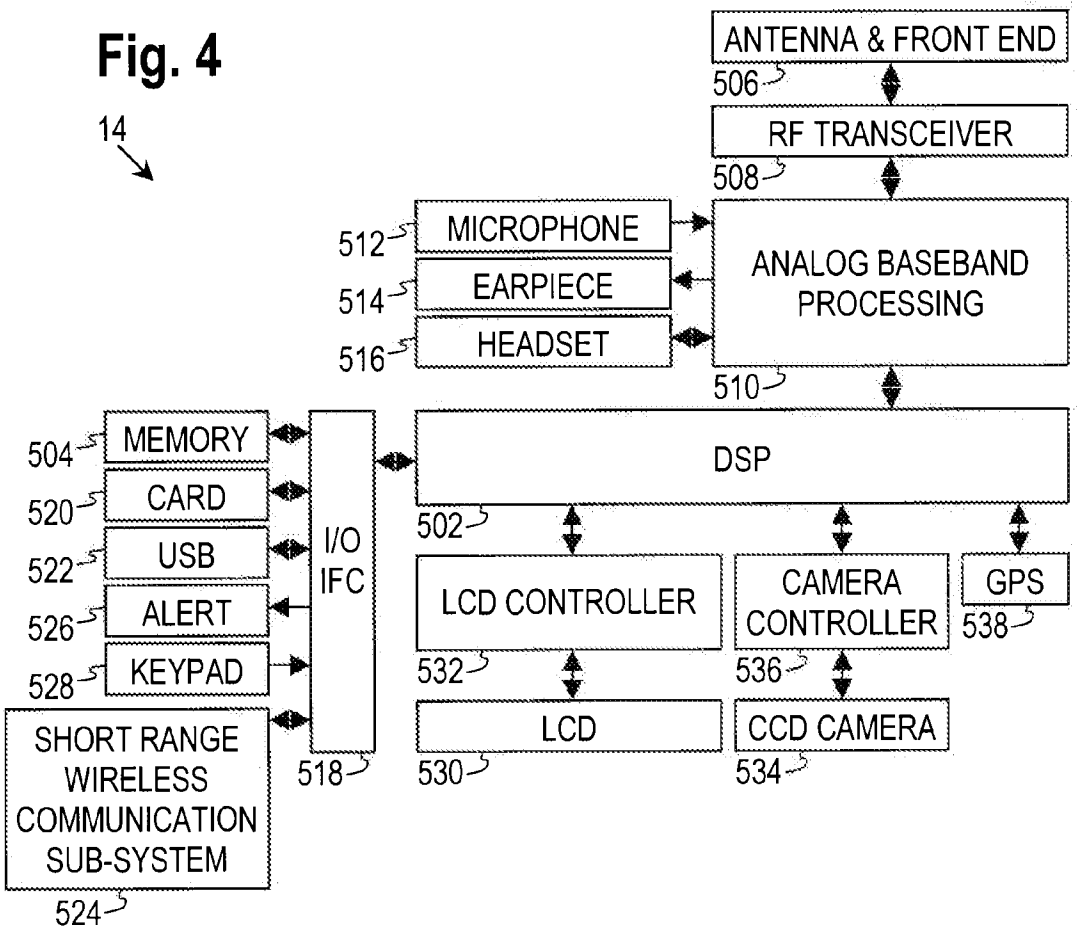


Fig. 4


14
ANTENNA & FRONT END
506
RF TRANSCEIVER
508
MICROPHONE
512
EARPIECE
514
HEADSET
516
ANALOG BASEBAND PROCESSING
510
MEMORY
504
CARD
520
USB
522
ALERT
526
KEYPAD
528
I/O IFC
518
DSP
502
LCD CONTROLLER
532
CAMERA CONTROLLER
536
GPS
538
LCD
530
CCD CAMERA
534
SHORT RANGE WIRELESS COMMUNICATION SUB-SYSTEM
524

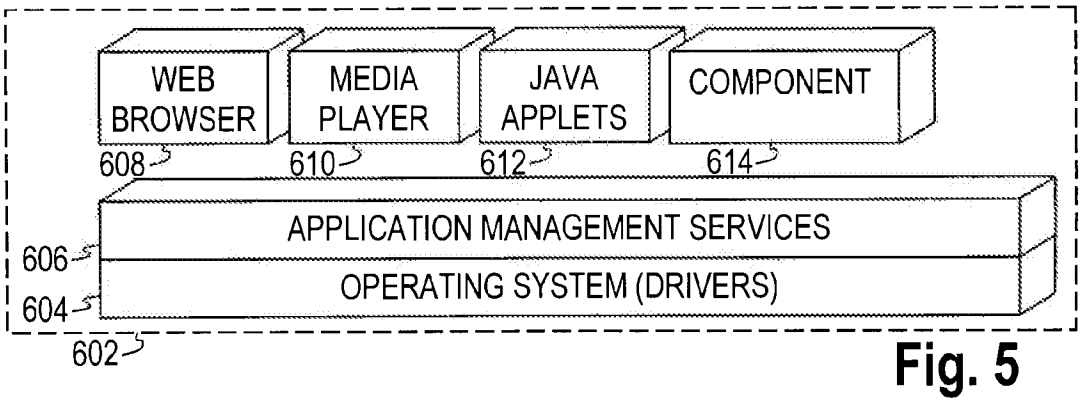

WEB BROWSER
608
MEDIA PLAYER
610
JAVA APPLETS
612
COMPONENT
614
APPLICATION MANAGEMENT SERVICES
606
OPERATING SYSTEM (DRIVERS)
604
602

Fig. 5

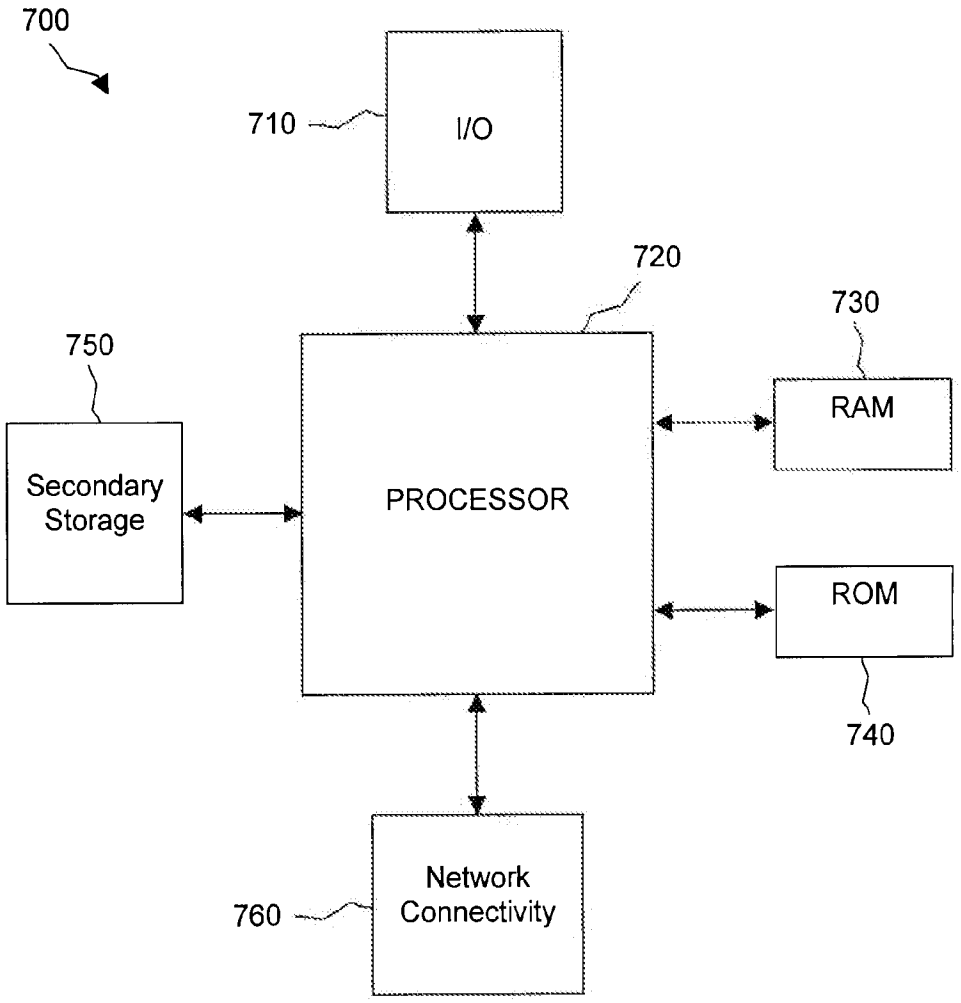

700
710
I/O
720
730
750
RAM
Secondary Storage
PROCESSOR
ROM
740
Network Connectivity
760

Figure 6

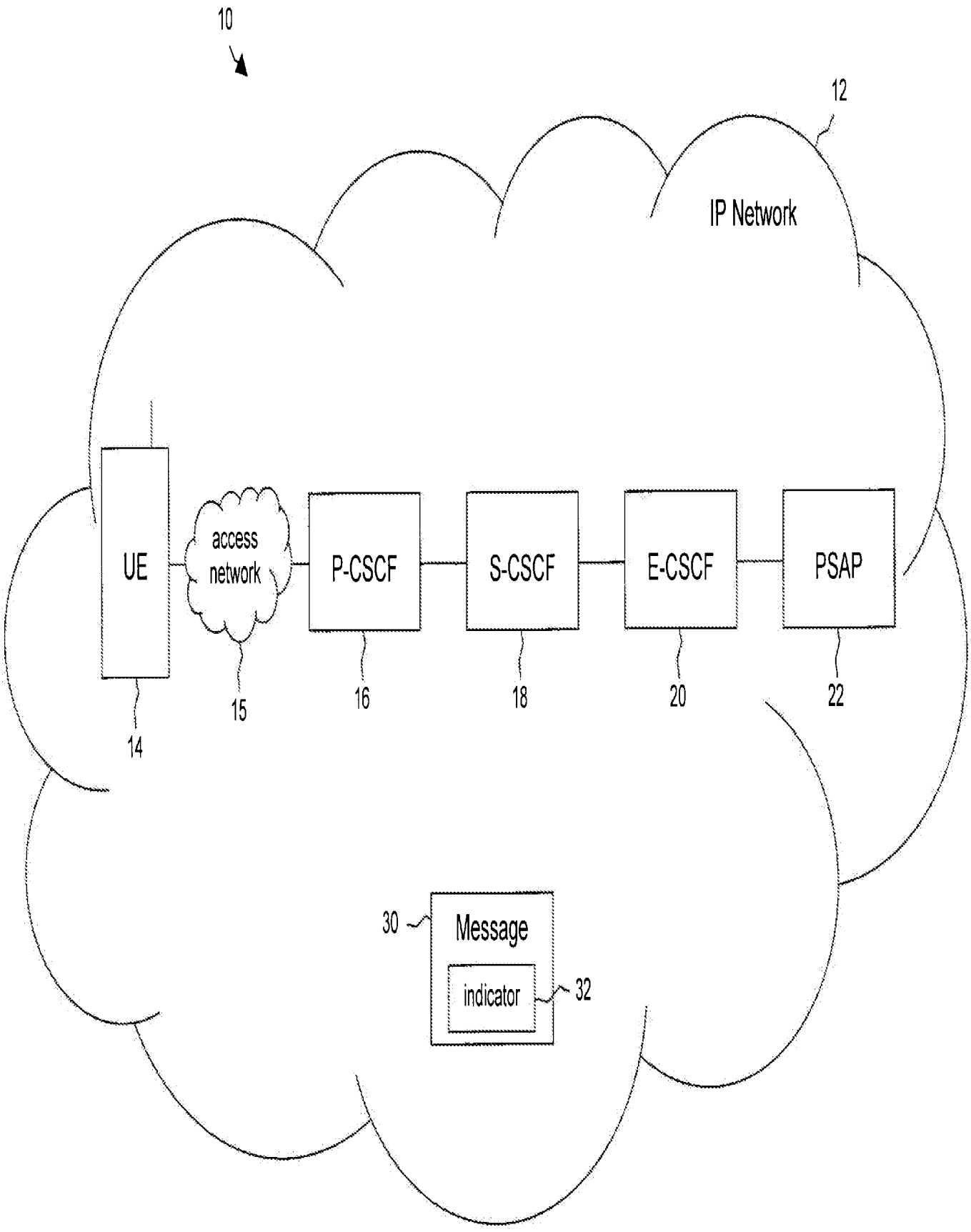

10
12
IP Network
UE
access network
P-CSCF
S-CSCF
E-CSCF
PSAP
14
15
16
18
20
22
30
Message
indicator
32

Figure 1

Espacenet

Bibliographic data: CN1498029 (A) — 2004-05-19

Emergency call-back method

Inventor(s): CHEN MARRY W [US]; ROLAND DOUGLAS H [US] ± (MARRY W. CHEN, ; DOUGLAS H. ROLAND)

Applicant(s): LUCENT TECHNOLOGIES INC [US] ± (LUCENT TECHNOLOGIES INC)

Classification: - international: ***H04B7/26; H04M1/26; H04M3/42; H04W4/16; H04W4/22; H04W76/02;*** (IPC1-7): H04M1/26; H04M3/42; H04Q7/38
- cooperative: **H04W4/22; H04W76/007**

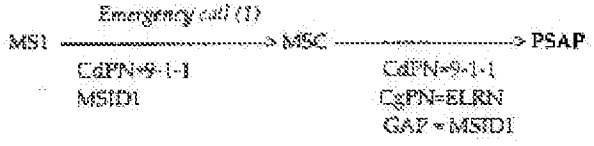
Application number: CN20031101083 20031015

Priority number (s): US20020270629 20021016

Also published as: CN1498029 (B) EP1411743 (A1) EP1411743 (B1) US2004203565 (A1) US7676215 (B2) more

Abstract of CN1498029 (B)

Fig. 1



An emergency routing number is assigned to each switch in a wireless network. When a switch of the wireless network routes an emergency call to a Public Service Answering Point (PSAP), the switch sends the emergency routing number as the calling party number and provides the PSAP with the identifier of the mobile station. If the emergency call drops, the PSAP performs a call back using the emergency routing number as the called party number. The switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. When a switch receives its emergency routing number as the called party number, the switch recognizes an emergency call back situation and pages the mobile station identified by the mobile station identifier received in association with the emergency routing number.; The mobile station is then reconnected with the PSAP.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04M 1/26 H04M 3/42

[12] 发明专利申请公开说明书

[21] 申请号 200310101083.5

[43] 公开日 2004 年 5 月 19 日

[11] 公开号 CN 1498029A

[22] 申请日 2003.10.15
[21] 申请号 200310101083.5
[30] 优先权
[32] 2002.10.16 [33] US [31] 10/270，629
[71] 申请人 朗迅科技公司
地址 美国新泽西州
[72] 发明人 玛丽·W·陈
道格拉斯·H·罗兰德

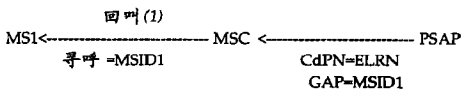
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李 强

权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称 应急回叫方法

[57] 摘要

对无线网内的每个交换机分配一个应急路由选择号码。 在无线网内的交换机使应急呼叫路由选择到公用业务应答中心(PSAP)时，该交换机发送所述应急路由选择号码作为主叫方号码，并将移动台的标识符送到 PSAP。 如果应急呼叫中断，则 PSAP 利用所述应急路由选择号码作为被叫方号码进行回叫。 使应急呼叫从移动台路由选择到 PSAP 的交换机接收该回叫。 PSAP 还将移动台标识符发送到该交换机。 在交换机接收作为被叫方号码的其应急路由选择号码时，该交换机识别应急回叫情况，并寻呼利用与应急路由选择号码相关接收的移动台标识符识别的移动台。 然后，该移动台重新连接到该 PSAP。



ISSN1008-4274

1、一种应急回叫方法，该应急回叫方法包括:

对无线网内的每个交换机分配一个应急路由选择号码，用作通过每个交换机路由选择到公用业务应答中心 PSAP 的各应急无线呼叫的主叫方号码。

2、根据权利要求 1 所述的方法，其中分配的每个应急路由选择号码是不可移植的。

3、一种应急回叫方法，该应急回叫方法包括:

发送无线网内一个用于处理发出应急呼叫的移动台的通信需要的交换机的应急路由选择号码和该移动台的标识符到公用业务应答中心 PSAP。

4、一种应急回叫方法，该应急回叫方法包括:

在公用业务应答中心 PSAP 接收无线网内一个用于处理发出应急呼叫的移动台的通信需要的交换机的应急路由选择号码和该移动台的标识符；以及

在该移动台发出的应急呼叫中断时，在 PSAP 通过呼叫所述应急路由选择号码向该移动台发出回叫。

5、根据权利要求 1 所述的方法，该方法进一步包括:

在发出回叫时，将所述移动台的标识符发送到所述交换机。

6、根据权利要求 5 所述的方法，其中所述发送步骤在通用地址参数中发送所述移动台的标识符。

7、一种应急回叫方法，该应急回叫方法包括:

在无线通信系统的一个交换机接收被叫方号码和移动台标识符；以及

当所述被叫方号码与分配给该交换机的应急路由选择号码匹配时，寻呼由所述移动台标识符识别的移动台。

8、根据权利要求 7 所述的方法，其中所述接收步骤在通用地址参数中接收所述移动台标识符。

9、根据权利要求 7 所述的方法，其中在所述交换机处以比其它任务高的优先级执行所述寻呼步骤。

10、根据权利要求 7 所述的方法，其中所述交换机是移动交换中心。

应急回叫方法

背景技术

在北美地区，通过拨“9-1-1”发出应急业务呼叫。世界上的其他地区可能使用某个其他简化可拨号数字串，例如在墨西哥使用“6-1-1”，它们的共同之处是意在有助于主叫用户利用容易记忆的数字以简单方式进行呼叫以寻求帮助。这些呼叫路由选择到本地公用业务应答中心（Public Service Answering Point，PSAP），在这里，在主叫用户通话的同时，可以启动应急响应（警察、消防队、公路抢修、救护车等）。如果在完全报告紧急情况之前或响应者到达之前该呼叫由于某种原因断线或中断，则 PSAP 可以利用其数据库提供的回叫号码回叫始发者。

例如，通过有线网始发 911 呼叫的呼叫记录可以包括自动线路标识（ANI）或通过其始发呼叫的用户接入线的电话号码。然而，无线用户的移动电话薄号码（MDN）或电话号码与物理线路或移动台不相关。不是利用 MDN，而是利用移动台标识（MSID），将对无线用户的呼叫路由选择到移动台。因此，对移动台进行应急回叫遇到了用例如陆线设备不会遇到的障碍。

通常，MSID 是由移动台用户已经与其达成业务协议的业务提供商编程到移动台内的 10 位数字移动标识号码（MIN）或 15 位数字国际移动用户标识符（IMSI）。因此，MSID 不必是可拨号号码。

移动台的 MDN 是可拨号号码。主叫用户拨 MDN，并利用 MDN 通过网络使呼叫路由选择到无线用户的归属系统。在用户的归属系统，归属位置寄存器（HLR）含有与用户的 MDN 相关的 MSID。然后，不利用 MDN，而利用 MSID，通过网络使呼叫路由选择到在服务无线系统并寻呼该用户。归属系统将用户的 MDN 在一个被称为用户概况的单独数据文件中提供给在服务系统。

对 MDN 和 MSID 使用单独号码对于某些系统是新的。历史上，在 TIA/EIA-41 系统中，在根据本地路由选择号码（LRN）方法和国际漫游（IR）实现无线号码可移植性（WNP）或成千块号码汇集（TBNP）之前，移动台的移动标识号码（MIN）与 MDN 相同。然而，利用 WNP 和 TBNP，MDN 变得可以从一个业务提供商“移植”或“汇集”到另一个业务提供商。由于 MSID 不可移植或汇集，所以接收者业务提供商对用户分配带有被植入或被汇集的 MDN 的新 MSID。

国际漫游也迫使 MSID 与 MDN 分离。尽管 MIN 是按照北美编号方案的 10 位数字 MDN 编制的 10 位数字号码，但是采用不同电话薄编号方案的其他国家的电信公司可能不允许其 MDN 等效于国际识别的 MIN 格式。另一个标准 MSID 是 IMSI。它用于世界各地的 TIA/EIA－41 系统和 GSM 系统。IMSI 是 15 位数字号码，因此，不能用作 10 位数字的 MDN。

历史上，在 MDN 与 MIN 相同时，MIN 可被传送到 PSAP，而且可以用作回叫号码。如上所述，如果将 MIN 与 MDN 分离，就必须将 MDN 作为单独回叫号码与主叫用户的 MSID 一起传送到 PSAP。存在某些与实现该解决方案相关的问题。主要问题是，在服务系统可能仅使 MSID 与呼叫一起传送到 PSAP，而不使主叫用户的 MDN 传送到 PSAP。其中一些原因与根据标准实现 MSID－MDN 分离的方式相关。

老式在服务 TIA/EIA－41 系统可能不支持 WNP、TBNP 或 IR。这意味着，老式在服务系统可能希望 MIN 与 MDN 相同。更老式系统甚至可能不知道在用户业务概况（不是以 MDN 而是以 MIN 为关键字的）中查找单独的 MDN。因为该限制，可以不允许这些用户使用基本业务，但是必须允许他们呼叫应急业务。因此，通过老式系统拨“9－1－1”的漫游用户将使他或她的呼叫带有 MSID 而没有 MDN 传送到 PSAP。因此，不可能进行回叫。

一个支持 WNP 和 IR 的新式在服务系统可能不能将 MDN 传送

到 PSAP。如果主叫移动台未注册到任何业务提供商（例如，存在仅用于应急呼叫的移动电话机），可能发生这种情况。此外，用户还可以在 HLR 利用含有 MDN 的用户业务概况响应在服务系统之前发出应急呼叫。

国际漫游用户的回叫 MDN 可以要求 PSAP 发出国际呼叫以传送到其本地应急业务区（ESZ）内的用户。对于通常不发出国际呼叫而且为了挽救某人的生命可能需要立即回叫信息的 PSAP，这不是一个实用的、及时的或充分可靠的解决方案。此外，不能将全部国际 MDN（多至包括国家代码的 15 位数字）送到 PSAP 用于回叫。

对这些问题的一种已建议的解决方案要求，在 MDN 不可用时，将 9－1－1＋主叫移动台的电子序列号（ESN）的后 7 位传送到 PSAP，作为回叫号码。尽管这可以用于对 PSAP 和在服务系统识别主叫用户，但是不能通过网络路由选择该“9－1－1＋ESN7”，而且该“9－1－1＋ESN7”不能用于发出回叫。

发明内容

根据本发明的回叫方法对无线网内的每个交换机分配一个应急本地路由选择号码（ELRN）。在无线网内的一个交换机使应急呼叫路由选择到公用业务应答中心（PSAP）时，该交换机发送其应急本地路由选择号码作为主叫方号码（CgPN），并将移动台的标识符（MSID）送到 PSAP。如果应急呼叫中断，则 PSAP 利用所述应急路由选择号码作为被叫方号码（CdPN）进行回叫。结果，使应急呼叫从移动台路由选择到 PSAP 的交换机接收该回叫。PSAP 还将该移动台的标识符发送到该交换机。该 MSID 用于寻呼正确的移动台。在本发明的一个实施例中，PSAP 在通用地址参数中将移动台标识符发送到交换机。

在交换机接收作为被叫方号码的其应急本地路由选择号码时，该交换机识别应急回叫情况，并寻呼利用与该应急路由选择号码相关接收的移动台标识符识别的移动台。在本发明一个实施例中，在一个

ELRN 是所述 CdPN 时，交换机对处理回叫赋予的优先级比处理其他任务的优先级高。这样，PSAP 与该移动台重新连接在一起。

附图说明

根据以下对本发明所做的详细说明以及仅作为示例用的附图，可以更全面地理解本发明，其中对各附图中的相应部分指定类似的参考编号，附图包括:

图 1 至 6 是示出根据本发明的回叫方法的运行过程的通信流程图。

具体实施方式

根据本发明的回叫方法对无线通信系统内的每个交换机（例如，移动交换中心（MSC））分配唯一可路由选择的回叫号码。以下将该号码称为“应急本地路由选择号码”或 ELRN。可以认为 ELRN 与为了实现无线号码可移植性（WNP）或成千块号码汇集（TBNP）而对每个本地交换机分配的本地路由选择号码（LRN）类似。然而，ELRN 可以仅路由选择到拥有该号码的交换机，每个交换机的 ELRN 是唯一的，而且是不可移植的。

我们知道，在移动台进行应急呼叫时，提供与应急呼叫相关的移动台标识符（MSID）。例如，MSID 是移动标识号码（MIN）、用于那些不属于北美编号方案范围的 10 位数字号码的 10 位数字国际漫游移动标识号码（IRM）、或国际移动用户标识符（IMSI）。在无线系统的一个交换机接收来自移动台特别是没有 MDN 的移动台的应急呼叫（例如，9-1-1 呼叫）时，该交换机将该交换机的 ELRN 发送到服务该交换机的公用业务应答中心（PSAP）。该交换机提供 ELRN 作为主叫方号码（CgPN），而且还将移动台的 MSID 提供给 PSAP。例如，在 ISUP 通用地址参数（GAP）中发送 MSID.

如果应急呼叫中断，则 PSAP 利用 ELRN 作为被叫方号码（CdPN）进行回叫。结果，已将应急呼叫从移动台路由选择到

PSAP 的交换机接收该回叫。PSAP 还将该移动台的标识符发送到该交换机。例如，与回叫一起诸如在 ISUP 通用地址参数（GAP）中发送 MSID。

在交换机接收作为被叫方号码的其应急路由选择号码时，该交换机识别应急回叫情况，并寻呼利用与 ELRN 相关接收的 MSID 识别的移动台，然后，建立应急回叫。这种 ELRN 技术还可以在交换机中具有优先级排队，其中交换机以比其他呼叫任务高的优先级处理回叫号码。这样，即使在该交换机的业务高峰期，仍可以提高应急回叫的接通率。此外，尽管对所有应急呼叫进行了描述，但是使用该方法可以仅局限于由没有 MDN 或 MDN 不可用的移动台发出的应急呼叫。

图 1 至 6 是根据本发明的回叫方法的运行过程的通信流程图。如图 1 所示，第一移动台 MS1 发出应急呼叫，在该例中为 9－1－1，MSC 接收该应急呼叫。因此，被叫方号码是 9－1－1，而且还将第一移动台 MS1 的 MSID1 送到 MSC。然后，MSC 使该应急呼叫路由选择到在服务 PSAP。在这样做的过程中，被叫方号码保持 9－1－1，而 MSC 提供其 ELRN 作为主叫方号码。MSC 还在通用地址参数（GAP）中提供第一移动台 MS1 的 MSID1。

如果应急呼叫中断，则 PSAP 利用该 ELRN 作为被叫方号码进行回叫，因为该 ELRN 已被送到 PSAP 作为主叫方号码。结果是使回叫路由选择到 MSC，如图 2 所示。如图 2 进一步所示，与回叫一起在 ISUP GAP 中发送第一移动台的 MSID1。如图 3 所示，MSC 利用第一移动台 MS1 的 MSID1 寻呼第一移动台 MS1 并接通该回叫。

假定在正在回叫第一移动台 MS1 时，第二移动台 MS2 发出 9－1－1 应急呼叫，如图 4 所示。与第一移动台 MS1 发出应急呼叫的情况一样，第二移动台 MS2 一起发送其移动台标识符 MSID2 和应急呼叫（例如，被叫方号码为 9－1－1）。然后，MSC 使应急呼叫路由选择到 PSAP。在这样做的过程中，被叫方号码保持 9－1－1，而 MSC 提供其 ELRN 作为主叫方号码。MSC 还将第二移动台 MS2 的

MSID2 送到 PSAP。因此，图 4 示出 MSC 将同一个主叫方号码（即，ELRN）送到 PSAP 用于这两个应急呼叫。

如果第二应急呼叫中断，则 PSAP 利用 ELRN 作为被叫方号码进行回叫，因为该 ELRN 已被送到 PSAP 作为主叫方号码。结果是使第二回叫路由选择到 MSC，如图 5 所示。如图 5 进一步所示，与第二回叫一起在 ISUP GAP 中发送第二移动台的 MSID2。如图 6 所示，MSC 利用第二移动台 MS2 的 MSID2 寻呼第二移动台 MS2 并接通该回叫。

根据本发明的应急回叫方法确保连同来自移动台的每个应急呼叫将一个可路由选择的回叫号码提供给 PSAP。具体地说，ELRN 是一个用于使一个或者多个应急业务回叫路由选择到始发交换机（例如，MSC）的号码。特别是在没有可用于伴随应急呼叫的本地 MDN 时，将始发交换机的 ELRN 发送到 PSAP 作为主叫方号码（CgPN）。

在北美编号方案中，ELRN 是 10 位数字号码（NAP－NXX－XXXX），其中头 6 位数字（NAP－NXX）是为了进行路由选择而对北美地区的每个本地交换机唯一分配的。后面的 4 位数字是交换机运营商分配的。然而，所述应急回叫方法可以应用于位于世界各地的公用交换网。也就是说，ELRN 含有为了使呼叫路由选择到特定交换机而根据任何国家编号方案分配的数字。此外，可以连同任何移动业务或无线接入技术，应用应急回叫方法。

该应急回叫方法与号码可移植性和号码汇集无关。这些网络能力取决于根据与移植的或汇集的拨号号码相关的 LRN，使呼叫路由选择到在服务交换机的本地路由选择号码（LRN）方法。与之相比，ELRN 与拨号号码无关，而与交换机相关。

从某种意义上说，ELRN 在公用网内的作用类似于为本地号码可移植性要求的本地路由选择号码（LRN），例如，它们二者均可以作为使许多呼叫路由选择到特定交换机的单一号码。然而，不要求进行数据库查询以识别使呼叫路由选择到在服务 MSC 所需的 ELRN。

因此，在用作使回叫从 PSAP 路由选择到在服务 MSC 的被叫方号码（CdPN）时，ELRN 可以附带为了指出不需要进行号码可移植性数据库查询而设置的 ISUP 前向呼叫指示符（FCI）。

如上所述，ELRN 与任何特定 MDN 不相关，它用于使回叫直接路由选择到在服务交换机，而非归属系统。ELRN 使得不需要 PSAP 利用 MDN 进行应急回叫。不需要为了通过归属系统路由选择回叫，而根据现有移动通信应用部分（MAP）标准请求 MDN 或 LRN。此外，还不需要通过区外归属系统发送国际呼叫来回叫本地区内的国际漫游用户。这样就减少了信令，节省了时间而且提高了业务的可靠性。此外，不象在 TIA/EIA－41 网内那样需要临时长途号码（TLDN），或者不象在 GSM 网内那样需要移动台路由选择号码（MSRN）来使回叫从归属系统路由选择到在服务系统。这样就减少了信令，节省了时间而且不要求提供 TLDN 或 MSRN。

尽管这样对本发明进行了说明，但是显然，可以以许多方式对其进行变更。可以认为这些变更属于本发明的实质范围，而且试图使所有这些修改包括在所附权利要求所述的范围内。

图1

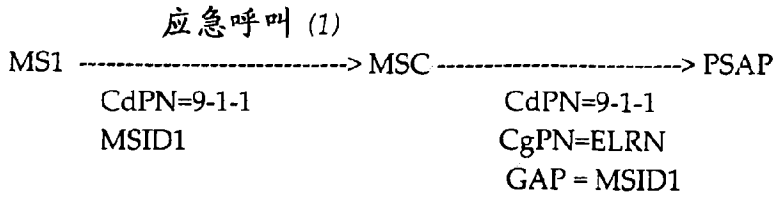


图2

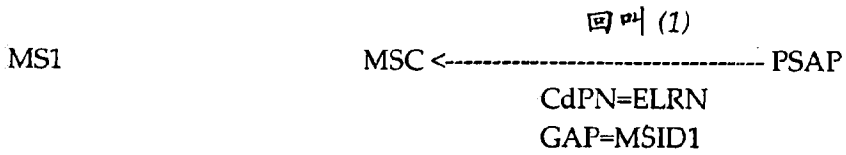


图3

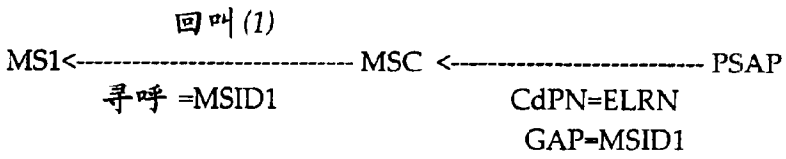


图4

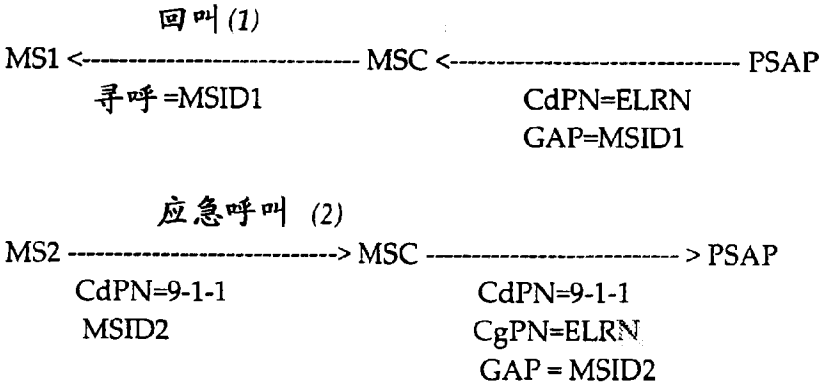


图5

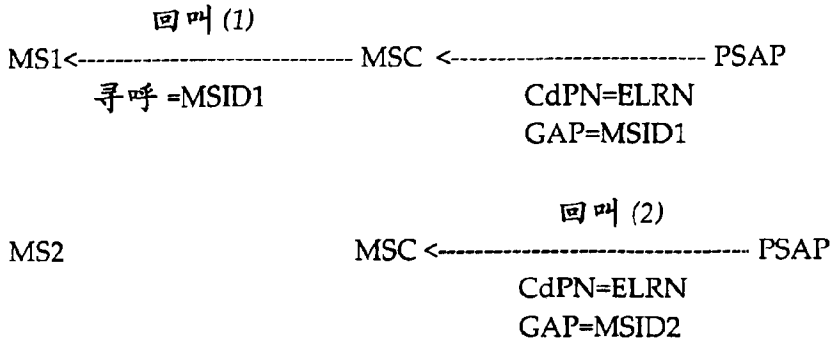
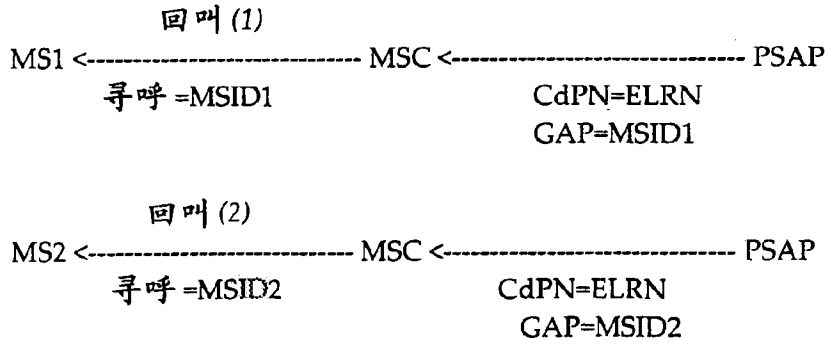


图6



Espacenet

Bibliographic data: CN1498482 (A) — 2004-05-19

Method and communication system for monitoring data flow in data network

Inventor(s): STIFTER H [DE]; PFEHLER W [DE]; KREUSCH N [DE] + (H. STIFTER, ; W. PFEHLER, ; N. KREUSCH, ; H. STIFTER,W. PFEHLER,N. KREUSCH)

Applicant(s): SIEMENS AG [DE] + (SIEMENS AG)

Classification: **- international:** ***H04L12/26; H04L29/06; H04L29/08; H04M3/22;*** (IPC1-7): H04L12/26; H04L29/06

- cooperative: **H04L12/2602**; **H04L29/06**; **H04L43/00**; **H04L63/00**; **H04L63/30**; **H04L65/103**; **H04L65/1046**; **H04L65/80**; **H04L67/2814**; **H04L67/306**; **H04M3/2281**; H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

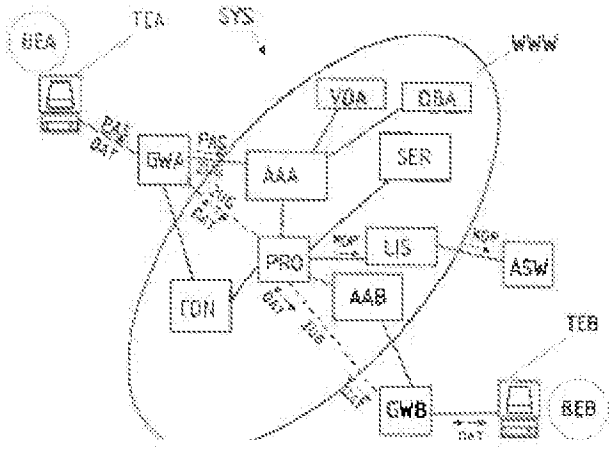
Application number: CN2002806811 20020307

Priority number(s): EP20010107063 20010321

Also published as: CN1274114 (C) EP1244250 (A1) US2004181599 (A1) US7979529 (B2) RU2003130974 (A) RU2280331 (C2) EP1371173 (A1) EP1371173 (B1) WO02082728 (A1) BR0208272 (A) less

Abstract not available for CN1498482 (A)
Abstract of corresponding document: EP1244250 (A1)

A data stream (DAT) is monitored in a data network (WWW) between two telecommunications terminals (TEA,TEB) connected to the data network via access servers (AAA,AAB), which operate during a monitoring situation to divert the data stream between the telecommunications terminals through a monitoring server (PRO) that produces a copy (KOP) of the data stream and transmits it to an analyzing unit (ASW). An independent



claim is also included for a telecommunication system for monitoring a data stream in a data network between a telecommunications terminal linked to a data network via a gateway and to a further telecommunications device.

Fig. 1

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/26
H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 02806811.4

[43] 公开日 2004 年 5 月 19 日

[11] 公开号 CN 1498482A

[22] 申请日 2002.3.7 [21] 申请号 02806811.4

[30] 优先权

[32] 2001. 3.21 [33] EP [31] 01107063.8

[86] 国际申请 PCT/EP2002/002524 2002.3.7

[87] 国际公布 WO02/082728 德 2002.10.17

[85] 进入国家阶段日期 2003.9.19

[71] 申请人 西门子公司

地址 德国慕尼黑

[72] 发明人 H·斯蒂特 W·普菲赫勒

N·克雷斯奇

[74] 专利代理机构 中国专利代理(香港)有限公司

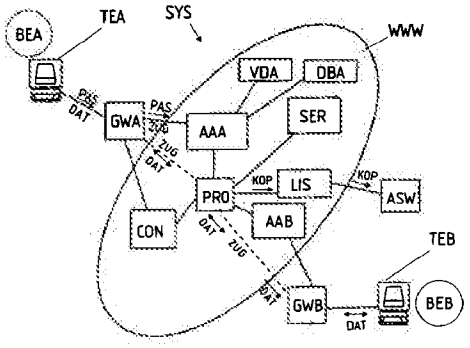
代理人 程天正 张志醒

权利要求书 4 页 说明书 9 页 附图 2 页

[54] 发明名称 用于监测数据网中数据流的方法及通信系统

[57] 摘要

本发明涉及一种用于监测位于至少两个通信终端(TEA，TEB)之间的数据网(WWW)中数据流(DAT)的方法及其通信系统(SYS)，这些终端通过至少一个接入服务器(AAA，AAB)与数据网相连。在监测的情况下，通信终端(TEA，TEB)间的数据流(DAT)自接入服务器(AAA，AAB)转由监测服务器(PRO)来传送，此监测服务器产生此数据流(DAT)的副本(KOP)，并将其传送至一个评估单元(ASW)。



ISSN1008-4274

1. 一种用于监测位于至少一个通信终端（TEA）和至少一个另外的通信设备（SER,TEB）之间的数据网（WWW）中的数据流（DAT）的方法，所述的至少一个通信终端（TEA）通过至少一个网关（GWA,GWB）与数据网（WWW）连接，其中设置至少一个鉴权服务器（AAA,AAB）以被用来对数据网（WWW）实行接入控制（ZUG），其特征在于，通过所述至少一个鉴权服务器（AAA,AAB）检测是否应监测所述至少一个通信终端（TEA）与所述至少一个另外的通信设备（SER,TEB）间的数据流（DAT），其中在监测的情况下产生此数据流（DAT）的一个副本（KOP），该副本被附上一个标识（IDK），且副本连同其上的标识（IDK）被传送到至少一个LI-服务器（LIS）和/或直接被传送到一个评估单元（ASW）。

2. 根据权利要求1中所述的方法，其特征在于，所述副本（KOP）通过所述网关（GWA,GWB）产生。

3. 根据权利要求1中所述的方法，其特征在于，所述副本通过一个专门设立的监测服务器（PRO）产生。

4. 根据权利要求1至3中之一所述的方法，其特征在于，所述LI-服务器根据标识（IDK）确定，是否应产生此副本（KOP）的至少一个二次副本（WKO），以及该副本（KOP）和/或至少一个二次副本（WKO）应被传送给谁。

5. 根据权利要求4中所述的方法，其特征在于，所述LI-服务器（LIS）产生所述副本（KOP）的至少一个二次副本（WKO）。

6. 根据权利要求1至4之一所述的方法，其特征在于，所述LI-服务器（LIS）执行与评估单元（ASW）的接口匹配。

7. 根据权利要求1至5之一所述的方法，其特征在于，所述鉴权服务器(AAA,AAB）根据分配给一个隐藏数据库（DBA,DBB）中的至少一个通信终端（TEA）的监测标识（UWD）来确定，是否存在一个监测情况。

8. 根据权利要求6所述的方法，其特征在于，所述隐藏数据库（DBA,DBB）和一个用于管理用户概况及用户鉴权数据的管理数据库（VDA,VDB）进行通信连接，并且每一个在管理数据库（VDA,VDB）中登录的用户（BEA,BEB）被分配隐藏数据库（DBA,DBB）中的一个监测标识（UWD）。

9. 根据权利要求7所述的方法，其特征在于，在清除所述管理数据库(VWA,VWB)中用户鉴权数据的情况下，所述隐藏数据库（DBA,DBB）中所分配的监测标识（UWD）也被清除。

10. 根据权利要求1至6之一所述的方法，其特征在于，作为IP承载语音的数据流来传输所述的数据流（DAT）。

11. 根据权利要求9中所述的方法，其特征在于，由一个呼叫控制器（CON）通过产生所述副本（KOP）的监测服务器（PRO）转发所述数据流（DAT）。

12. 根据权利要求3至10所述的方法，其特征在于，在监测状态下，所述鉴权服务器（AAA,AAB）通过监测服务器（PRO）转发数据流（DAT）。

13. 根据权利要求3至11之一所述的方法，其特征在于，所述数据通道（ZUG）从网关（GWA,GWB）被隧穿至监测服务器（PRO）。

14. 根据权利要求3至12之一所述的方法，其特征在于,所述数据流（DAT）的副本(KOP)被暂存在所述监测服务器（PRO）上。

15. 根据权利要求1至11之一所述的方法，其特征在于,所述数据流（DAT）的副本（KOP）被缓存在所述LI-服务器上。

16. 根据权利要求10至14之一所述的方法，其特征在于,所述控制器（CON）不仅控制所述网关（GWA,GWB），还控制所述监测服务器（PRO）。

17. 根据权利要求11至14之一所述的方法，其特征在于，由所述至少一个鉴权服务器（AAA,AAB）控制所述的监测服务器。

18. 用于监测位于至少一个通信终端（TEA）和至少一个另外配置的通信设备（SER,TEB）之间的数据网（WWW）中的数据流（DAT）的通信系统，所述的至少一个通信终端（TEA）通过至少一个网关（GWA,GWB）与数据网（WWW）连接，其中设置至少一个鉴权服务器(AAA,AAB)以被用来对数据网（WWW）实行接入控制（ZUG），其特征在于，鉴权服务器（AAA,AAB）被用来检测是否应监测所述至少一个通信终端（TEA）与所述至少一个另外的通信设备（SER,TEB）间的数据流（DAT），其中此通信系统（SYS）被配置用来在监测情况下产生所述数据流（DAT）的一个副本（KOP），并为此副本（KOP）附加一个标识（IDK），以及将此副本(KOP)连同其标识（IDK）传送至至少一个LI服务器（LIS）和/或直接传送至一个评估单元（ASW）。

19. 如权利要求17所述的通信系统,其特征在于，所述网关（GWA,GWB）被用于产生数据流（DAT）的副本（KOP）。

20. 如权利要求17所述的通信系统，其特征在于，提供一个监测服务器（PRO），其适用于产生副本（KOP）。

21. 如权利要求17至19之一所述的通信系统,其特征在于，LI-服务器被用来根据标识(IDK)确定是否应该产生副本(KOP)的至少一个二次副本(WKO)，并且此副本（KOP）和/或至少一个二次副本（WKO）应传送给谁。

22. 如权利要求21所述的通信系统，其特征在于，LI-服务器被用来产生所述副本（KOP）的至少一个二次副本（WKO）。

23. 如权利要求17至22之一所述的通信系统,其特征在于，LI-服务器被用来执行评估单元（ASW）的接口匹配。

24. 如权利要求17至23之一所述的通信系统，其特征在于，所述鉴权服务器（AAA,AAB）被用来根据隐藏数据库中至少一个通信终端（TEA）所分配的监测标识（UWD）来确定是否存在监测情况。

25. 如权利要求24所述的通信系统，其特征在于，所述隐藏数据库（DBA,DBB）和一个被分配给鉴权服务器的、用于管理用户概况和用户鉴权数据的管理数据库(VDA,VDB)被设置用来进行数据的相互交换,其中每个在管理数据库（VDA,VDB）中登录的用户（BEA,BEB）都分配有隐藏数据库（DBA,DBB）中的一个监测标识（UWD）。

26. 如权利要求25所述的通信系统，其特征在于，一旦清除管理数据库（VWA,VWB）中的用户鉴权数据，该通信系统就被用来清除其在隐藏数据库（DBA,DBB）中所分配的监测标识（UWD）。

27. 如权利要求17至26之一所述的通信系统,其特征在于，数据流（DAT）是IP承载语音的数据流。

28. 如权利要求27所述的通信系统，其特征在于,提供一个呼叫控制器(CON),其用于在监测情况下通过监测服务器（PRO）转发数据流（DAT）。

29. 如权利要求20至28之一所述的通信系统，其特征在于，所述鉴权服务器(AAA,AAB)被用来在监测情况下通过监测服务器(PRO)转发数据流(DAT)。

30. 如权利要求20至29之一所述的通信系统,其特征在于，该通信系统被用来隧穿由网关（GWA,GWB）至监测服务器（PRO）的数据通道。

31．如权利要求20至30之一所述的通信系统，其特征在于，所述监测服务器被用来中间缓存数据流（DAT）的副本(KOP)。

32．如权利要求17至31之一所述的通信系统，其特征在于，所述LI服务器被用来暂存数据流（DAT）的副本（KOP）。

33．如权利要求28至32之一所述的通信系统，其特征在于，所述呼叫控制器（CON）被用来不仅控制网关（GWA,GWB），还控制监测服务器（PRO）。

34．如权利要求29至32之一所述的通信系统，其特征在于，所述鉴权服务器（AAA,AAB）被用于控制监测服务器。

35．如权利要求20至34之一所述的通信系统，其特征在于，所述监测服务器(PRO）具有代理服务器的功能。

用于监测数据网中数据流的方法及通信系统

本发明涉及一种用于监测位于至少一个通信终端和至少一个另外的通信设备之间的数据网中的数据流的方法，所述的通信终端通过至少一个网关与数据网连接，所述的另外的通信设备可配置至少一个鉴权服务器，其目的在于执行通向数据网的接入控制。

本发明还涉及一种用于监测位于至少一个通信终端和至少一个另外配置的通信设备之间的数据网中的数据流的通信系统，所述通信终端通过至少一个网关与数据网连接，所述的另外的通信设备可配置至少一个鉴权服务器，其目的在于执行通向数据网的接入控制。

规则制定者越来越多地要求数据网的运营商提供一些功能，使得在需要时对用户的数据交换进行监测成为可能。

目前在数据网如因特网中对数据流的合法监听，即所谓“合法截听”的问题是以不同的方式解决的。

一种已知的方法是在一个要监测的局域网中配置外部取样器（分析器），它们分析总分组数据流，过滤并复制被监测者的通信，并传送给业务承运商。此方法的缺点主要是对网络的规定时限的物理干涉是不可避免的。由于被监测者的移动性增大，这种方法就不实用了。

另外一种用于电子邮件通信监听/监测的方法首先是在一个或更多电子邮件服务器上执行一种自动转发功能，它把到达和发出的电子邮件传送给业务承运商，比如官方机构。类似地可用于语音邮件等。使用这种方法所不可避免的是，必须配置所有的电子邮件服务器来识别监听/监测情况，并转发到主管官方机构，这导致高额的管理开支。

WO 0042742中描述了一种在面向分组的网如GPRS网或UMTS网中用于执行合法监听的监测方法和监测系统。为此提供了一个具有数据分组监测功能的第一网元，它通过第二网元来控制。被截获的（被监测出的）数据将通过一个网关，此网关具有一个通往有监听资格的官方机构的接口。这种方法的缺点主

要是那些不应被监听的用户的数据流也会流经所述网元，这就从根本上增加了此方法的技术和管理开支。

关于因特网中的“合法截听”例如请参见ETSI TR 101 750 V1.1.1.

非常高额的费用是不容忽视的，这些费用通常是因为网络运营商在提供前述的监听/监测功能时产生的，这主要由高额的管理开支而引起。

所以本发明的一项任务是实现一种途径，此途径通过简单且节省开支的方式实现了在一种数据网中执行监听/监测功能。

此任务由前述的方法以如下方式来解决，通过至少一个鉴权服务器来检测是否应监测在至少一个通信终端和至少一个另外的通信设备之间的数据流，其中在监测情况下产生数据流的一个副本，它被附上一个标识，此副本同标识一起被传送到至少一个LI-服务器和/或直接传送到一个评价单元。

本发明的一个好处就是设置了网络侧的监听功能，通过此可避免网络中由外部监听装置引起的干涉。另外，如果被监测者是移动的且所处位置改变，则访问该被监测者的数据流也是可能的，因为该被监测者必须通过设置所述监测措施的提供商的鉴权服务器才能拨入。

本发明的一种变型是由网关产生所述副本。

本发明的另一种变型是由特别为此所提供的监测服务器来产生所述的副本。

优选地，所述LI-服务器根据标识确定，是否应该产生所述副本的至少一个二次副本，并且确定将所述副本和/或至少一个所述二次副本应传送给谁。

有利地，由LI-服务器产生至少一个所述的二次副本，也就是说，此LI-服务器复制对应于合理数位的数量的副本。

通过LI-服务器实现对评估单元的一个接口匹配，就能得到本发明其他优点。

鉴权服务器可以根据隐藏数据库中的至少一个所述通信设备所分配的监测标识来确定，是否存在一种监测情况。

所述隐藏数据库与一个用于管理用户概况及其鉴权数据的管理数据库建立连接，其中，每个在管理数据库中登录的用户就在该隐藏数据库中分配一个监测标识。

在清除管理数据库中的用户鉴权数据的情况下，所述隐藏数据库中分配的监测标识也被清除。

本发明的另一变型是以IP承载语音的数据流的形式传输数据流，其中，呼叫控制器通过产生所述副本的监测服务器转发数据流。

另一种可能是鉴权服务器在监测状态下通过所述监测服务器转发数据流。

所述转发的变型是，提供由所述网关隧穿至所述监测服务器的数据通道。

如果不能将所述副本立即发送给业务承运商，为避免丢失数据，可以将所述数据流的副本暂存在监测服务器和/或LI-服务器上。

在本发明的一个优选实施方式中，所述控制器既控制网关也控制所述监测服务器。

本发明的另一个非常有利的实施方式在于，至少有一个鉴权服务器控制监测服务器。

上述现有技术中的通信系统尤其适合用于执行根据本发明的方法，为此在通信系统中配置了所述鉴权服务器，以便检测是否应监测处于至少一个所述通信终端与至少一个所述另外的通信设备之间的数据流，此外配置所述通信系统的目的在于，在监测的情况下产生数据流的一个副本，为此副本附加一标识，并且把此副本连同其标识传送给至少一个LI-服务器和/或直接传送给一个评估单元。

在本发明的第一个变型中所述网关被配置用来产生所述数据流副本。

在本发明的另一个变型中提供有一个监测服务器，配置此监测服务器用于产生所述副本。

此外配置所述LI-服务器的目的在于，根据标识确定是否应产生所述副本的至少一个二次副本,并且确定该副本和/或所述至少一个二次副本应传送给谁。

更有利的是配置所述的LI-服务器以产生所述的至少一个二次副本。

通过配置所述LI-服务器以便实现对所述评估单元的接口匹配，可实现其他的优点。

可以配置所述鉴权服务器以便根据在隐藏数据库中的至少一个所述通信终端所分配的监测标识，来确定是否存在一种监测情况。

配置所述隐藏数据库和一个给所述鉴权服务器分配的、用于管理用户概况及其鉴权数据的管理数据库，以便彼此交换数据，其中，把所述隐藏数据库中的一个监测标识分配给每一个在所述管理数据库中登录的用户。

可以配置该通信系统，以便在清除所述管理数据库中的用户鉴权数据的情况下，清除所述隐藏数据库中所分配的监测标识。

在本发明的一个有利的变型中，数据流是IP承载语音的数据流，其中提供了一个呼叫控制器，其配置用于在监测的情况下通过所述监测服务器转发数据流。

另一个有利的变型在于，配置所述鉴权服务器，以便在监测的情况下通过所述监测服务器转发数据流。

通过配置所述通信系统能得到其他好处，其目的在于，隧穿从网关到监测服务器的数据通道。

为了防止数据丢失，可以配置所述监测服务器和/或所述LI-服务器，以便暂存所述数据流的副本。

此外可以配置所述呼叫控制器，以便既控制所述网关又控制所述监测服务器。

在另一种变型中，配置了鉴权服务器来控制监测服务器。

有利地，所述监测服务器具有代理服务器的功能。

在下文中，借助附图中非限制性的实施例描述本发明及其他的优点，图中示出了：

图1：根据本发明的通信系统，

图2 a：带有一个标识的一个数据流的副本，

图2 b：图2 a中的标识的细节，和

图3：根据本发明方法的示例性的流程图。

按照图1，本发明通信系统SYS的每一个想要通过自己的通信终端TEA或通信装置TEB接入一个数据网WWW、例如接入因特网的用户BEA，BEB，必须通过一个网关GWA，GWB拨入或者注册到一个接入服务器AAA。在本申请中，一个通信装置被理解为任何一种通信终端，例如一个与数据网连接的PC或者某些能在数据网WWW中存在的服务器。

接入服务器AAA，AAB可以构成为AAA-服务器或者远程鉴权拨入用户业务的服务器，简称RADIUS服务器。为了得到一个接入数据网WWW的数据通道ZUG，对于一个用户来说，鉴权是必不可少的。

在此情况下，一个用户BEA，BEB的鉴权可以通过输入一个口令PAS或输

入一个用户标识，例如用户的名字加以实现。

根据识别结果，接入服务器AAA，AAB决定一个通往数据网WWW的数据通道ZUG是否被允许或者被拒绝。

用户BEA，BEB的鉴权可以由接入服务器AAA侧借助于向一个管理数据库VDA的询问加以实现，在此管理数据库中实现对用户数据的管理。

如果存在一个正面的鉴权结果，就可以向一个隐藏数据库提问，在此数据库中一个监测标识UWD被分配给每一个在这个管理数据库中登录的用户。如果监测标识UWD说明处于用户BEA的通信终端TEA和另一个通信终端之间的一个数据流DAT应该被引导通过，那么就产生数据流DAT的一个副本KOP。

原始数据流DAT的副本KOP，例如可以由被分配给通信终端TEA的网关GWA，或者由一个特意为此提供的监测服务器PRO产生。

如果监测服务器PRO产生原始数据流DAT的副本的话，则通过监测服务器PRO转发数据流DAT。这个服务器优选地具有代理功能。监测服务器PRO与一种代理服务器的区别仅仅在于，配置监测服务器PRO是为了执行通过它运行的(被转发的)数据流DAT的副本KOP，给该副本设立一个一起被提供的标识IDK(图2)，例如IP-地址或即将被监听的用户的一个用密码书写的标识，并且传送给一个“合法截听”服务器或者，简而言之，传送给一个LI-服务器LIS，在此情况下原来的数据流被继续传送给通过用户确定的目标地址。

如果由网关GWA产生副本KOP，那么上述副本的和向LI-服务器继续传送副本KOP的功能或者根据用户所确定的目标地址传送原来的数据流DAT的功能，将在网关GWA中得以实现。

在监测的情况下，一个通向数据网WWW的数据通道ZUG，对于即将被监测的用户BEA来说，可以直接通过网关和监测服务器PRO得以实现。

转发通往监测服务器PRO的数据流DAT可以借助于隧道，例如按照在RFC 2661中详细说明的L2T-协议得以实现。

通过监测服务器PRO转发数据流DAT的另一种可能性在于，把数据网中的一个地址分配给监测服务器PRO，如果是因特网的话，则把一个IP-地址分配给监测服务器PRO。这个地址可以被存放在接入服务器AAA，AAB的一个存储装置中，与此同时在监测的情况下，数据流DAT例如按照TCP／IP-协议继续向监测服务PRO的地址传送。

正如上文所述，监测服务器PRO产生通过它被转发的数据流DAT的副本KOP，并且把这一副本KOP传送到一LI-服务器，此服务器根据附在其上的标识IDK决定对这样的副本KOP应该怎样处置，例如是否应该产生其他的副本，即该副本的二次副本WKO，或者应该将这样的副本传送至哪种评估单元。

然后在评估单元ASW中，例如在一个官方机构为此而配置的PC中，完成副本KOP的进一步的处理和分析。

LI-服务器LIS通常是若干工作站的一种配置。正如上面所述,其任务在于，接收数据流DAT的副本KOP，分析由监测服务器附在副本KOP上的标识IDK，如有可能则产生副本KOP的其他的副本WKO，并且将其送交业务承运商。

配置LI-服务器以用于对业务承运商的各种不同的评估单元实施接口匹配。因此，例如对于监测来说，向执行监测的官方机构的已知时分复用（简称TDM）-切换-接口建立两个H-323通信连接可能是必要的。另一种可能性在于，通过一个IP-切换-接口向进行监测的官方机构送交这个副本。

LI-服务器LIS为了向业务承运商或者评估单元ASW进一步传送这个副本所需要的信息，能够由业务承运商一方在一个数据库LID中存放。

另一个可能性在于，由监测服务器PRO或者网关GWA直接向评估单元ASW传送此副本KOP连同标识IDK。

在产生数据流DAT的副本KOP之后，由监测服务器PRO以传统方式，例如根据TCP / IP-协议，将原始数据流DAT进一步路由给第二个用户BEB或者通信装置TEB，SER。

按照图2a，把一个标识IDK作为起始写在数据流DAT的副本KOP的前面。此标识至少可具有一个IP-头IPH，例如被监测的用户BEA的IP-地址。此外还可以提供一个特别的LI-头LIH(图2b)，此LI-头包含关于进一步数据传送的信息。于是，例如第一行可以含有消息的类型TYP，例如是否涉及一种语音消息或者一个“被监听的”电子邮件。下一行可以含有头长LEN，而在第三行可以含有按照标准ETSI ES 201671的一个操作员ID即OID。一个呼叫标识码CIN可用于对一个“被监听的”用户BEA的识别；而官方机构标识LID则用于标识副本KOP应被传送到的哪一个业务承运商。需要时，其他的信息SUP可以附加给上述已知的标识。

按照图3，在语音传输的情况下，根据IP承载语音协议，一个相应的应用

程序APP在呼叫方BEA的通信终端TEA上被启动，这个通信终端于是通过第一网关GWA建立与第一接入服务器AAA的连接。该接入服务器AAA检测，哪一个用户打算需要语音传输服务，并检测其是否有权要求这样的服务。为此目的建立了网关GWA与接入服务器AAA之间的H. 323或RADIUS-通讯。

如果呼叫用户BEA有权使用语音服务，那么接入服务器AAA根据用户BEA的鉴权检查，是否应该检测呼叫方与被呼叫方间的数据交换。

在成功地进行接入检查之后，呼叫控制器CON通过与第二接入服务器AAB的通信，查明被叫的通信终端TEB的IP-地址，并且通过另一个网关GWB促使与这个通信终端TEB的信令通信。

如果这时要对呼叫方进行监测，那么控制器CON并不直接建立网关GWA与被呼叫的通信终端TEB的连接，正如通常的情况那样，而是引入监测服务器PRO。也就是说第一个通信终端TEA与第二个通信终端TEB的连接被拆成两段，即被拆成从第一个通信终端TEA到监测服务器PRO的一段和从监测服务器PRO到第二个通信终端TEB的一段。

在正常情况下，控制器CON控制第一个网关GWA。然而由于监测的缘故，接通数据网WWW的通道被延长至所述监测服务器PRO，并且在那里本来只开始为用户BEA的数据流DAT进行正常路由，所以配置所述控制器CON以实现从网关到所述监测服务器的“切换”。这就是说，通过第一个接入服务器AAA通知所述控制器CON存在一种监测情况，以及被监测的通信终端TEA的数据通道ZUG隧穿监测服务器PRO。所述控制器从这时起把所述监测服务器PRO视为“新的”第一网关GWA，并像控制网关GWA一样来控制该服务器。因此在监测的情况下，所述呼叫控制器CON就将所述监测服务器PRO视为网关GWA一样，这种情况既适用于呼叫方又适用于被叫方。

正如上文所述，所述监测服务器PRO接下来产生所述两个通信终端TEA和TEB之间的数据流DAT的副本KOP。为产生此副本KOP，初始的数据流DAT在所述监测服务器PRO中被加倍。所述初始数据流DAT在加倍之后由所述监测服务器PRO向第二个通信终端TEB继续路由，而所述数据流DAT的副本KOP如前所述被转发到LI-服务器或者评估单元ASW。

所述监测服务器PRO也可配置作为LI-服务器LIS，用于暂存所述副本KOP以在向评估单元ASW的直接传送不可能的情况下，避免数据丢失。

为了在对初始数据流DAT的质量和速度无显著损失的情况下实现监听，位于监测服务器PRO与网关GWA之间的那段应该很短，因此如果在所述数据网WWW中安排大量的监测服务器PRO则是有利的。

如果被呼叫的用户BEB应被监测，则基本上通过如上所述的方法实现；其中，第二个接入服务器AAB可以根据被呼叫方BEB的IP-地址实现鉴权，并通过所述监测服务器PRO转发数据流DAT。

为了实现根据被呼叫方BEB的IP-地址对其鉴权的目的，第二个接入服务器AAB可以包括一个数据库DAB，该数据库含有所述被叫方的IP-地址和被叫方是否被监听的记录。

对用户BEA进行监测的命令由一个有权监测的官方机构发出，并将其记录在隐藏数据库DBA中。

如果被监测的用户BEA在其通信终端上启动一个在数据网WWW中进行数据传输的应用程序，如上文所述，那么实现用户鉴权并确定是否存在一种监测情况。

在监测的情况下，例如在其上已存放一主页或其他数据的一个服务器向A方传送所述监测服务器PRO的地址，而不转发被叫方BEB的地址或通信装置TEB SER的地址。B方的网关GWB从鉴权服务器AAA或呼叫控制器CON获得监测服务器PRO的网络地址，而不是呼叫方BEA的网络地址。

由所述鉴权服务器AAA或呼叫控制器CON通知监测服务器PRO是否应进行监测。所有用于监测和连接的必要信息，例如“把A方与B方连接”的信息及类似信息，可以通过H．248传输而由所述鉴权服务器AAA或呼叫控制器CON传送至所述监测服务器PRO。

如上文所述，位于A方与B方用户或服务器之间的数据流DAT在所述监测服务器中被加倍，其中被加倍的数据被附上一个标识IDK，这样产生的副本KOP在以后被传送所述给LI-服务器。

对于原始数据流，监测服务器具有与代理服务器一样的功能，并且只连接A方与B方。

本发明的另一个变型在于，A方从鉴权服务器AAA或呼叫控制器CON那里收到B方端的网络地址；在此情况下，借助于H．248传送而请求A方的网关把源于用户BEA的所有数据业务都隧道传送给监测服务器。与此同时，由呼叫

控制器把监测服务PRO的地址而不是A方的网络地址传送给其网络地址已知的B方。

所述监测服务器PRO从所述呼叫控制器那里得到隧道传送的相应信息，并且将A和B方连接起来。

隧道的优点在于，对于被监测的用户BEA来说，通过监测服务器PRO转发数据流所必要的地址改变是不明显的。

如果鉴权服务器AAA，AAB或者呼叫控制器通过H．248通信而通知监测服务器PRO：一个数据流DAT被转发，那么监测服务器就能够把一个启动消息传送给LI-服务器，以至于这个LI服务器从LI-数据库中询问必要的数据，并在副本KOP到达时可使用这些数据。

如果被监测的数据交换结束,那么呼叫控制器CON就通知监测服务器PRO,其应该中断与LI-服务器的关于该具体监测的通讯。在收到一个源于监测服务器PRO的一条结束消息之后，LI-服务器能够重新清除来自LI-数据库的数据，并且停止与业务承运商的通信。

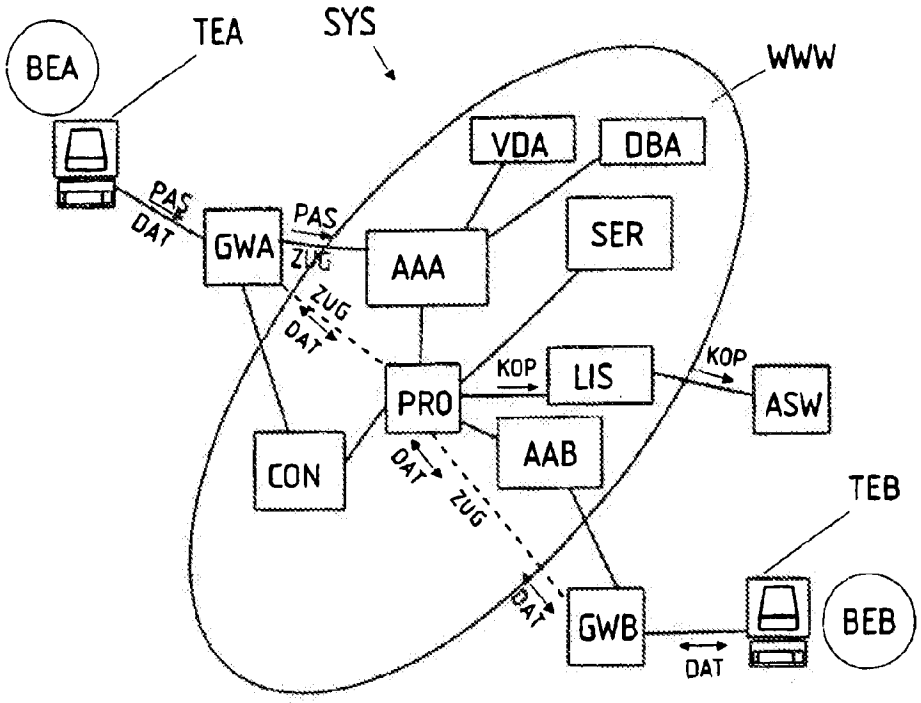


图 1

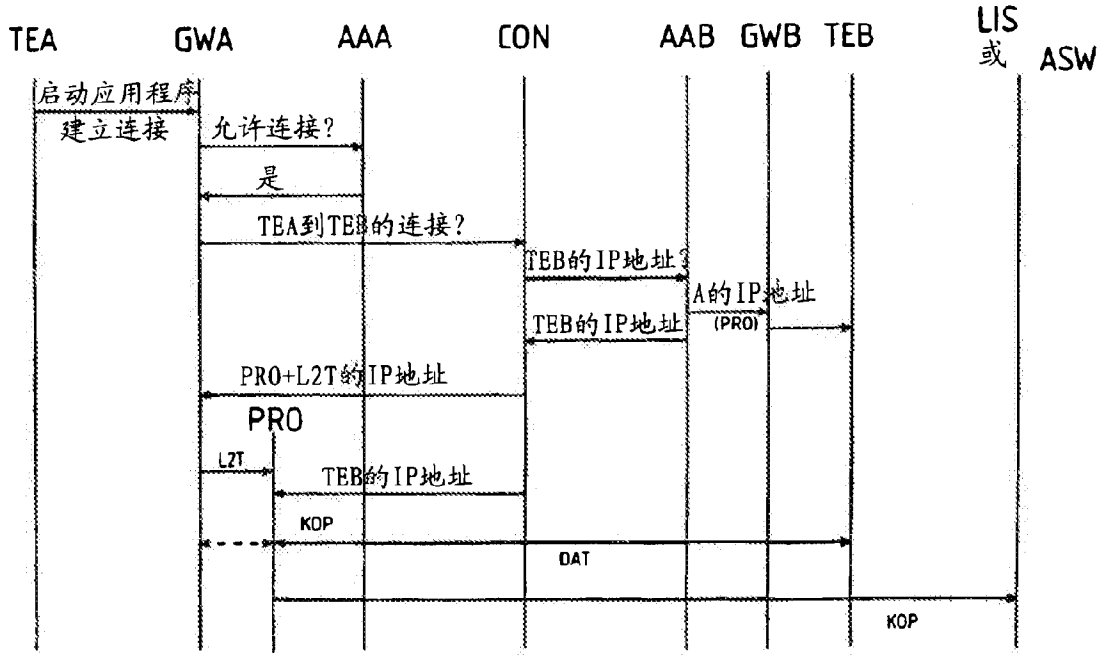


图 3

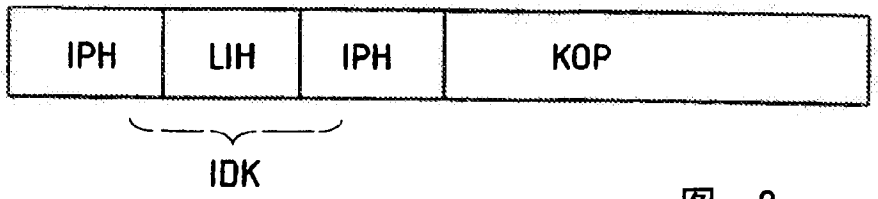


图 2a

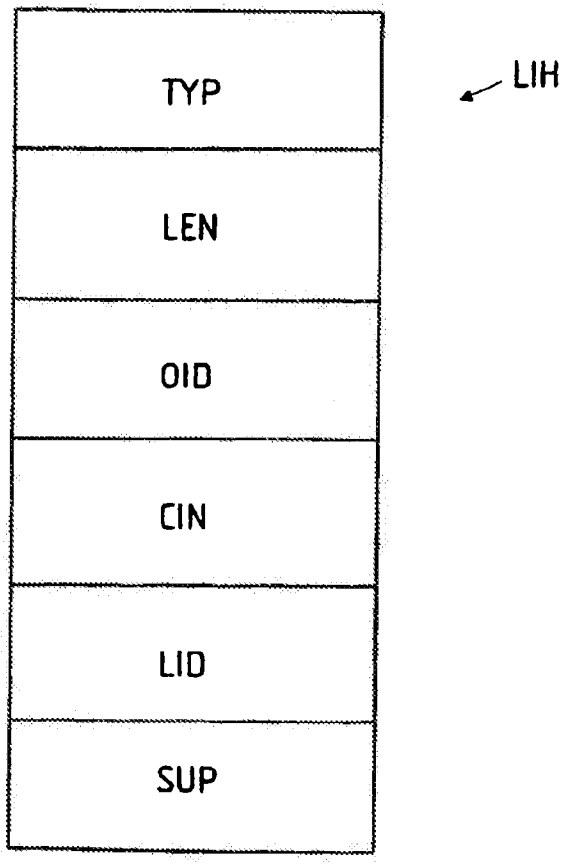


图 2b

Espacenet

Bibliographic data: CN1668137 (A) — 2005-09-14

A method of associating call back data to a call center

Inventor(s): ROLLENDER DOUGLAS H [US] ± (ROLLENDER DOUGLAS H)

Applicant(s): LUCENT TECHNOLOGIES INC [US] ± (LUCENT TECHNOLOGIES INC)

Classification: **- international:*H04M3/58; H04W4/22;*** (IPC1-7): H04M3/51; H04Q7/38
- cooperative: H04W4/22; H04W76/007

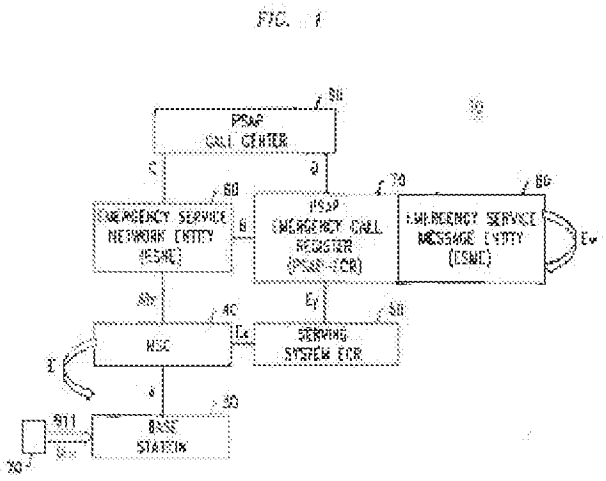
Application number: CN2005154422 20050310

Priority number (s): US20040798629 20040311

Also published as: EP1575327 (A1) US2005202799 (A1) US7702308 (B2) KR20060043407 (A) KR101160472 (B1) JP2005260971 (A) JP4875310 (B2) less

Abstract not available for CN1668137 (A)
Abstract of corresponding document: EP1575327 (A1)

A method of communication to at least one wireless unit originating an emergency call. The method includes the step of receiving at least one tag identifier in response to the emergency call originating from the at least one wireless unit. Once the tag identifier is received, a wireless call back number corresponding with the at least one tag identifier may be transmitted. A public service answering point emergency call register ("PSAP-ECR") may receive the at least one tag identifier and transmits the wireless call back number over a D interface.



[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04M 3/51

[12] 发明专利申请公开说明书

[21] 申请号 200510054422.8

[43] 公开日 2005 年 9 月 14 日

[11] 公开号 CN 1668137A

[22] 申请日 2005.3.10
[21] 申请号 200510054422.8
[30] 优先权
[32] 2004. 3.11 [33] US [31] 10/798,629
[71] 申请人 朗迅科技公司
地址 美国新泽西州
[72] 发明人 道格拉斯·H.·罗兰德尔

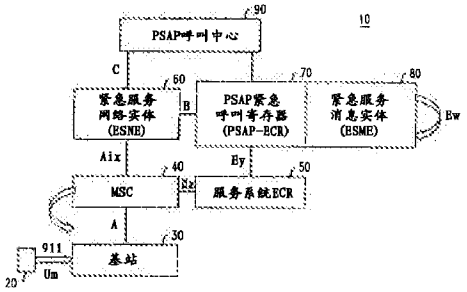
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 康建峰

权利要求书 2 页 说明书 13 页 附图 4 页

[54] 发明名称 将呼叫数据与呼叫中心相关联的方法

[57] 摘要

本发明公开一种与至少一个发起紧急呼叫的无线单元通信的方法。所述方法包括，作为对来自至少一个无线单元发起的紧急呼叫的响应，接收至少一个特征标识符的步骤。一旦接收了所述特征标识符，将发送相应于该至少一个特征标识符的无线回叫号码。公共服务应答点紧急呼叫寄存器(“PSAP-ECR”)将接收该至少一个特征标识符并通过一个 D 接口发送该无线呼叫号码。



ISSN1008-4274

1. 一种与至少一个发起紧急呼叫的无线单元通信的方法，所述方法包括:

作为对来自至少一个无线单元的紧急呼叫的响应，接收至少一个特征标识符;

相应于该至少一个特征标识符，发送一个无线回叫号码。

2. 如权利要求 1 所述的方法，其中发送无线回叫号码的步骤包括:

发送与至少一个无线单元相关联的位置信息，该位置信息相应于所述至少一个特征标识符。

3. 一种在具有紧急呼叫寄存器的通信系统中建立由至少一个无线单元发起的紧急呼叫的方法，所述方法包括:

作为对来自至少一个无线单元的紧急呼叫的响应，从与至少一个无线单元相关联的移动交换中心发送至少一个特征标识符。

4. 一种在具有紧急呼叫寄存器的通信系统中建立由至少一个无线单元发起的紧急回叫的方法，所述方法包括:

从紧急呼叫寄存器发送至少一个特征标识符;

将所述至少一个特征标识符输入紧急服务消息实体; 以及

相应于输入的至少一个所接收的特征标识符，请求紧急回叫。

5. 一种在具有紧急呼叫寄存器的通信系统中建立由至少一个无线单元发起的紧急呼叫的方法，所述方法包括:

接收来自紧急呼叫寄存器的至少一个特征标识符;

将所述至少一个特征标识符输入紧急服务消息实体; 以及

相应于输入的至少一个所输入的特征标识符，请求紧急呼叫。

6. 一种建立由与移动交换中心相关联的至少一个无线单元发起的紧急呼叫的方法，所述方法包括:

作为对来自至少一个无线单元的紧急呼叫的响应，从与至少一个无线单元相关联的移动交换中心向一个紧急服务实体发送至少一个特征标识符。

7. 如权利要求 6 所示的方法，包括:

发送与至少一个无线单元相关联的回叫和位置信息，所述回叫和位置信息相应于至少一个特征标识符。

8. 如权利要求 1 或 2 或 3 或 4 或 5 或 6 或 7 所述的方法，其中至少一个特征标识符包括数据库的一个参考关键字。

9. 如权利要求 8 所述的方法，其中所述数据库包括至少一个紧急呼叫寄存器以及一个紧急服务消息实体。

10. 如权利要求 8 所述的方法，其中所述至少一个特征标识符相应于紧急服务路由关键字、本地公共安全号码、传呼身份以及移动设备标识号码中的至少一个。

将呼叫数据与呼叫中心相关联的方法

技术领域

本发明涉及电信领域，特别的，涉及无线通信。

背景技术

在美国，紧急服务呼叫通过拨打“9-1-1”实现。世界其它地区可能使用其他简短的拨号串，举例来说，墨西哥用“6-1-1”。这些简短的拨号串都是出于使用容易记忆的号码简化求助呼叫的目的。这些呼叫都被路由到一个本地公共服务应答点呼叫中心（“PSAP-CC”）上以便在呼叫者正在通话的同时启动紧急响应（举例来说，警察局、消防局、公路维修、和/或救护车）。然而，如果在紧急事件被完整的报告或者响应者到达之前，呼叫不知因为什么原因断开连接或者落线了，PSAP-CC 就需要回叫发起者。

应该注意，通过有线网络发起的“9-1-1”呼叫的记录可能包括自动线路识别（“ALI”）或者呼叫发起的接入线路的电话号码。而无线用户的目录号码（“DN”）或者电话号码不与物理线路或者无线单元相关联。而是，与移动 DN（“MDN”）相反，通过移动基站识别（“MSID”）的方式将对漫游的无线用户的呼叫路由到该无线单元。相应的，执行对无线单元的回叫引发了例如与陆线设备不交融的障碍。

特别的，MSID 的特征在于它即可以是一个 10 位的移动标识号码（“MIN”）也可以是一个 15 位的国际移动用户标识符（“IMSI”）。IMSI 可以由无线单元用户所加入的服务协议的服务提供商编程到一个无线单元或者用户标识模块（“SIM”）卡中。相应的，MSID 也可以是不可拨号的号码。

无线单元的 DN 是一个可拨号号码，DN 由呼叫者拨出并被用来通过网络将呼叫路由到无线用户的主系统。在用户主系统中，主位置寄存器

（“HLR”）包含与用户 DN 相关联的 MSID。MSID 与 DN 不同，可以被用来通过网络将呼叫路由到服务无线系统上以及用来传呼用户。用户的 DN 可以通过无线单元从 SIM 卡提供给服务系统或者由主系统在一个独立的称为用户配置文件的数据文件中提供给服务系统。

采用独立的 DN 和 MSID 号码的系统的首次公开最近才出现在一些无线系统中。其他的系统从一开始就使用这一技术。曾经，在实施基于本地路由号码（“LRN”）方法和国际漫游（“IR”）的无线号码的可移植性（“WNP”）或者千组号码池（“TBNP”）之前，无线单元的移动标识号码与一些系统的 DN 一致，特别是在由 TIA/EIA-41 标准支持的系统中。然而，对于 WNP 和 TBNP，MDN 变为从一个服务提供者到另一个服务提供者“可移植的”或者“可入池的”。由于 MSID 可以不是可移植或可入池的，接收的服务提供者就可以以入口（ported-in）或池中的 MDN 为用户分配一个新的 MSID。

国际漫游也迫使 MSID 和 MDN 分离开来。在北美编号方案的 10 位 MDN 之后，MIN 也变为 10 位号码，采用不同目录编号方案的其他国家的通信公司可能不同意其用户的 DN 等于国际识别的 MIN 格式。另一个标准的 MSID 是 IMSI。其可以在全球的 TIA/EIA-41 和 GSM 系统中使用。IMSI 是一个基于 ITU-T 建议书 E.212 的 15 位的非可拨号号码，因此不能作为 10 位的 MDN。

曾经，当 MDN 和 MIN 相同的时候，可以向 PSAP-CC 传送 MIN 并且其可以被用作回叫号码。如上所述，随着 MIN 和 MDN 的分离，必需向 PSAP-CC 传送 MDN 作为独立的呼叫号码，以及传送呼叫者的 MSID。这就存在一个问题，与这一解决方案的实施有关。一个方面是服务系统可以没有呼叫者的 MDN，而仅有 MSID 来随着呼叫提供给 PSAP-CC。这一原因，根据标准，与分离的 MSID-MDN 的实施方式有关。另一原因在于用于向 PSAP-CC 传递呼叫的网络接口不具有一起发送 DN 和 MSID 或者，在一些情况下，甚至是完整的 DN 的容量。

一个老的服务 TIA/EIA-41 系统可能不支持 WNP、TBNP 或者 IR。这意味着老的服务系统希望 MIN 和 MDN 是一样的。老的系统甚至不知

道如何在用户服务配置文件中寻找分离的 MDN（举例来说，键入 MIN 而不是 MDN）。由于这一限制，不允许这些用户使用基础服务，但是必须允许他们进行紧急服务的呼叫。结果，当在一个旧的系统中时，拨打"9-1-1"呼叫的漫游者随着呼叫把 MSID 而不是 MDN 传递到 PSAP-CC 中。相应的，不可能进行回叫。

一个更新的服务系统是 WNP 和 IR，其可能不能向 PSAP-CC 传送 MDN。这一情况将发生，如果呼叫的无线单元没有在任何服务提供者处登记（举例来说，有仅用于紧急呼叫的移动电话）。这些无线单元可以称为非用户启动（"NSI"）的电话。也有可能在 HLR 用包含 DN 的用户服务配置文件响应服务系统之前，用户已经拨打了紧急呼叫。即使向 PSAP-CC 提供了回叫用的实用 DN，如果用户对于所有入局呼叫都有呼叫转递服务或者如果用户有一个限制性的、预付费服务并且没有剩余的开支可用于支付来自 PSAP-CC 的入局回叫，对于该 DN 的回叫将不会产生。此外，如果回叫号码是对一个正在观光的国际漫游者，PSAP-CC 将需要拨打一个国际电话。一些 PSAP-CC 可能不具备回叫一个国际号码的能力。此外，在完成国际呼叫的过程中还有网络拥塞或者延迟的风险，这对以及时的方式处理紧急事件是十分不利的。一些 PSAP-CC 甚至被配置不允许通过独立的、出局管理线路拨打任何出局呼叫。

国际漫游者的回叫 DN 将需要 PSAP-CC 拨打一个国际呼叫来接通在其本地紧急服务地带（"ESZ"）的用户。这对于通常不拨打国际电话的 PSAP-CC 和出于紧急目的要求立即回叫信息的应用而言不是实际的、及时且充分可靠解决方案。此外，如果 PSAP-CC 仅支持 10 位，整个国际 MDN（包括国家码在内达 15 位）可以不提供给 PSAP-CC 用于回叫。

也有可能正在进行呼叫的无线单元并为登记到任何服务提供者。结果，可能没有与无线单元相关联的 DN 或者编码到无线单元中的永久 MSID-这样的无线单元被称为 NSI 移动电话，举例来说。这可能是因为（a）NSI 电话从来未曾登记（有仅用于紧急呼叫的电话），（b）电话是新的并且还未由服务提供者初始化，（c）定购已经过期并且 NSI 电话不再与服务提供者登记，或者（d）有意无意的导致 SIM 卡丢失、被盗或

者仅仅未曾插入或者已被移除。

一些无线单元也支持包含在 MSID 和 DN 中的可移除的用户标识模块（“R-UIM”）或者用户标识模块（“SIM”）。如果 R-UIM 或者 SIM 不在电话当中，其也可被用来拨出一个紧急呼叫。然而，不为 PSAP-CC 提供电话或者服务系统知道的 DN 或者 MSID 作为回叫号码。

每个 MS 包括一个由制造商编码在电话中的唯一的移动设备标识号码（“MEIN”）。MEIN 可以是，举例来说，在 ANSI/TIA/EIA-41 系统中使用的电子序列号码（“ESN”），或者在 GSM 系统中使用的国际移动设备身份（“IMEI”）。MEIN 独立于 MSID 和 DN。随着发起呼叫的意图，MEIN 从空中在无线单元和无线系统的基站之间传送或随后传送。举例来说，如果没有发起呼叫的意图，MEIN 可以由服务系统请求。

当分配给无线用户的目录号码不可用时，无线紧急服务的当前标准请求向 PSAP-CC 传送“9-1-1+MEIN 的最后 7 位”作为回叫号码的形式。虽然这能够有助于提示 PSAP-CC 随着该呼叫没有可用的实用回叫号码，这一“9-1-1+MEIN 的最后 7 位（MEIN7）”不能唯一标识呼叫（举例来说，许多紧急呼叫可以通过相同的“9-1-1+ MEIN7”来标识）并且不能通过网络路由。这是由于“9-1-1+MEID 的最后 7 位”不包含完整的 MEID，并且因此不是唯一的。

虽然上面的方法为 PSAP-CC 提供了一些执行对无线单元的紧急回叫的方法，但仍然存在一些障碍。举例来说，在特定环境下，无线单元的回叫号码可以仅仅是一个带有用户位置数据的伪号码。相应的，需要一种确保能够确保为发起“9-1-1”呼叫的无线单元提供实际回叫号码的方法和体系结构。

发明内容

本发明提供了一种能够确保为发起“9-1-1”呼叫的无线单元提供实际回叫号码的方法和体系结构。更具体来说，本发明能够基于至少一个特征标识符(tag identifier)，使得诸如本地公共服务应答点呼叫中心（“PSAP-CC”）的呼叫中心能够启动回叫，不论发端的“9-1-1”呼叫者是

通过无线还是有线通信设施拨打的。为了达到上述目的，特征标识符可以对应于姓名或与不同源的信令唯一关联的标签，诸如举例来说声音的关联，具有与通过不同信道或者在独立的消息中发送关联的数据。相应的，特征标识符可以包括对数据库的一个或者多个参考关键字，诸如紧急呼叫寄存器或者紧急服务消息实体，举例来说。因此，所述特征标识符可以对应于紧急服务路由关键字、本地公共安全号码、传呼身份和/或移动设备标识号码，举例来说。

在本发明的一个实施例中，为发起紧急呼叫的至少一个无线单元提供了通信的方法。所述方法包括作为对来自至少一个无线单元的紧急呼叫的响应，接收至少一个特征标识符的步骤。一旦接收了所述特征标识符，发送与相应于该至少一个特征标识符的无线回叫号码。应该注意公共服务应答点紧急呼叫寄存器可以接收所述特征标识符并且通过 **D** 接口发送无线回叫号码。

在本发明的另一实施例中，提供了一种在具有紧急呼叫寄存器的通信系统中，建立由至少一个无线单元发起的紧急呼叫的方法。所述方法包括例如作为对来自至少一个无线单元的紧急呼叫的响应，通过 E_x 接口，从与至少一个无线单元相关联的移动交换中心发送至少一个特征标识符。对于在前面所述的具体实施例，特征标识符可以包括紧急呼叫寄存器的参考关键字。此外，特征标识符可以相应于紧急服务路由关键字、本地公共服务号码、传呼身份以及移动设备标识号码中的至少一个。此后，发送的特征标识符将进入紧急呼叫寄存器（举例来说，服务系统紧急呼叫寄存器或者公共服务应答点紧急呼叫寄存器）。

在本发明的另一具体实施例中，提供了一种在具有紧急呼叫寄存器的通信系统中，建立由至少一个无线单元发起的紧急回叫的方法。所述方法包括通过 B_e 接口从紧急呼叫寄存器发送至少一个特征标识符。接收所述特征标识符并且将其输入数据库，诸如紧急服务消息实体。此后相应于输入的特征标识符，请求紧急回叫。

在本发明的又一具体实施例中，提供了一种在具有紧急消息服务实体的通信系统中，建立由至少一个无线单元发起的紧急回叫的方法。所

述方法包括通过B_e接口接收来自紧急呼叫寄存器的至少一个特征标识符并将其输入紧急服务消息实体。此后相应于输入的至少一个所输入的特征标识符，请求紧急回叫。

在本发明的再一具体实施例中，提供了一种建立由与移动交换中心相关联的至少一个无线单元发起的紧急呼叫的方法。所述方法包括作为对来自至少一个无线单元的紧急呼叫的响应，从与至少一个无线单元相关联的移动交换中心向一个紧急服务实体发送至少一个特征标识符。该方法包括通过D接口从紧急服务消息实体发送与至少一个无线单元相关联的回叫和位置信息，所述回叫和位置信息相应于至少一个特征标识符。

通过阅读下面的具体说明并结合附随的权利要求数和附图，这些和其他的具体实施例对于本领于的普通技术人员而言将是清楚明白、易于理解的。

附图说明

通过参考附图以及阅读下文中非限定性的具体实施例的描述能够更好的理解本发明，其中：

图1和2示出了本发明一个具体实施例的体系结构和流程图；以及

图3和4示出了本发明另一具体实施例的体系结构和流程图。

应该强调的是，本申请的附图不是按比例的而仅仅是图解表示，因此并不刻意表示本发明的特定规格，这些通过对本公开文件的浏览，能够由本领域的普通技术人员清楚的确定。

具体实施方式

本发明提供了一种能够确保为发起“9-1-1”呼叫的无线单元提供实际回叫号码的方法和体系结构。更具体来说，本发明能够基于至少一个特征标识符，使得诸如本地公共服务应答点呼叫中心（“PSAP-CC”）的呼叫中心能够启动回叫，不论发端的“9-1-1”呼叫者是通过无线还是有线通信设施拨出的。为了达到上述目的，特征标识符可以对应于姓名或与不同源的信令唯一关联的标签，诸如，举例来说，声音的关联。相应的，

特征标识符可以包括对数据库的一个或者多个参考关键字，诸如，紧急呼叫寄存器或者紧急服务消息实体，举例来说。因此，所述特征标识符可以对应于紧急服务路由关键字、本地公共安全号码、传呼(paging)身份和/或移动设备标识号码，举例来说。

参考图 1 和 2，示出了本发明的一组实施例。对于图 1 而言，示出了支持移动紧急服务的网络参考模型（"NRM"）的体系结构 10，而图 2 示出了相应于图 1 的 NRM 的消息流程图 100。更具体而言，图 1 和图 2 的实施例与非呼叫相关信令（"NCAS"）技术有关，所述 NCAS 技术用于通过指定的接口向呼叫中心传送呼叫，而不需要通过该指定接口处理特定呼叫所需的数据。

如图 1 所示，示出了用于向体系结构 10 进行"9-1-1"呼叫通信的无线单元 20。为了本发明所公开的目的，"9-1-1"呼叫是对应于一个紧急呼叫和/或紧急服务的请求（举例来说，警察局、消防局、公路维修、和/或救护车）。通信，当由无线单元 20 发起时，通过空中接口 U_m，经由一个基站 30 传送到移动交换中心 40（"MSC"）。向体系结构 10 进行"9-1-1"呼叫通信的步骤对应于图 2 所示的图解 100 中的消息流 110。

一旦 MSC 40 接收了"9-1-1"呼叫，与无线单元 20 相关联的标识信息将传送到服务系统 50 的紧急呼叫寄存器（"ECR-SS"）中。向 ECR-SS 50 传送信息的步骤对应于图 2 的消息流 120。更具体来说，与无线单元 20 相关联的信息包括，举例来说，移动设备标识号码（"MEIN"）。向 ECR-SS 50 传送 MEIN 将由 MSC 40 通过第一 NRM 接口 E_x 来执行。应该注意，MEIN，当向 ECR-SS 50 传送时，可以通过国际移动设备身份（"IMEI"）、电子序列号码（"ESN"）、伪 ESN（"pESN"）和/或移动设备身份（"MEID"）来实现。

随着 MEIN 的传送，MSC 40 也可以向 ECR-SS 50 传送传呼身份（"PGID"）作为消息流 120 的一部分。在来自无线单元 20 的"9-1-1"呼叫从基站 30 和 MSC 40 落线或者断开与其的连接的情况下，PGID 可以用来传呼无线单元 20。为了在呼叫落线或者断开连接的情况下传呼无线单元 20，需要 MSC 40 的本地公共安全号码（"LPN"）来唯一标识服务

于“9-1-1”呼叫者（举例来说，无线单元 20）的交换机。LPN 可以通过来自于分配给 MSC 40 的本机或者非便携号码组块的可拨号号码来实现。LPN 可以有助于标识 ECR-SS 50 以及当呼叫在体系结构 10 中落线或断开连接时向“9-1-1”呼叫者发起回叫。

此外对于 LPN，紧急服务路由关键字（“ESRK”）也可以被用来唯一标识“9-1-1”呼叫者，其作为图 2 的消息流 120 的一部分。当与“9-1-1”呼叫相关联时，ESRK 可以支持无线单元 20 的本地信息的通信。参与提供 ESRK 的网络单元和接口可以，在一个实施例中，使用现有的通信标准来实现。

如上所述，PGID 可以是许多基于通信标准的标识符中的一个，如果“9-1-1”呼叫落线或者断开连接，所述标识符支持传呼无线单元 20 来传送一个入站呼叫。对于基于 GSM 的系统而言，无线单元 20 可以通过由无线单元 20 提供的国际移动基站身份（“IMSI”），与 IMSI 相关联的临时移动基站身份（“TMSI”）和/或来自无线单元 20 的 IMEI 来传呼。在 CDMA 2000 系统中，这一传呼步骤可以使用移动标识号码（“MIN”）、IMSI、来自非用户启动（“NSI”）的无线单元的缺省移动基站身份（“dMSID”）、来自无线单元 20 的 ESN 和/或由无线单元 20 中的 MEID 生成的 pESN 来实现。

对于与无线单元20相关联的从MSC 40接收的标识信息，SS-ECR 50 可以通过网络接口 E_y 将该信息重定向到与公共服务应答点 70（“PSAP”）相关联的另一个紧急呼叫寄存器（“ECR”）。这一活动对应于图 2 的消息流 130。相应的，MEIN、LPN、dMSID 和/或 ESRK 可以从 SS-ECR 55 再次发送到 ECR-PSAP 70。应该注意，所示 PSAP-ECR 数据库与紧急服务消息实体 80（“ESME”）相关联。然而，在 ESME 80 中的其他相关数据库可以键入 ESRK、MEIN、移动基站身份（举例来说 MIN 或 IMSI）和/或呼叫者的目录号码。

此后，ESRK 可以随着“9-1-1”呼叫从 MSC 40 传送到紧急服务网络单元 60（“ESNE”）。这一传输可以通过另一网络接口 A_{ix} 执行。这一活动相应于图 2 的消息流 140。

一旦传递到 ESNE60，ESRK 就被重新发送到公共安全访问点呼叫中心 90（“PSAP-CC”）。ESRK 的进一步传输可以通过另一网络接口 C 来执行。这一活动相应于图 2 的消息流 150。

接着，PSAP-CC 90 可以利用 ESRK 来询问 ESME 80“9-1-1”呼叫是从哪个无线单元 20 发起的。应该明白，ESME 80 应该包括从接口 E_y 到 ECR-PSAP 70 先前重新定向的信息。这一 ESME 80 询问可以通过另一网络接口 D 来执行。该活动对应于图 2 的消息流 160。

作为对来自 PSAP-CC 90 的询问的响应，ESME 80 可以提供一个回叫号码（“CBN”），以及蜂窝站点（cell site）位置和/或无线单元位置，服务系统的 LPN 以及无线单元 20 到 PSAP-CC 90 的 MEIN。这一信息可以通过 D 接口传送到 PSAP-CC 90。该活动对应于图 2 的消息流 170。应该注意，传送到 PSAP-CC 90 的 CBN，在本发明的一个实施例中，可以不是无线单元的目录号码或者在现有 NSI 电话标准中限定的非可拨号号码。反之，这里，回叫号码可以包括服务于无线单元 20 的 MSC 40 的 LPN 以及无线单元 20 的 MEIN。

对于正在处理的 CBN，PSAP-CC 90 可以进一步使用作为数据库关键字的 ESRK 通过 D 接口向 PSAP-ECR 70 和 ESME 80 发送信号。如果“9-1-1”的发起呼叫落线或者断开连接，能够执行该信号发送步骤通过 MSC 40 请求回叫。通过 MSC 40 的回叫允许任何 PSAP-CC 不需要立即进行出局呼叫来使用 D 接口作为另一个可选方式使 ESME 中的 PSAP-CC 发送信号以请求 MSC 40 发起一个在移动电话和 PSAP-CC 之间的新的“9-1-1”呼叫。此处，回叫请求可以通过 E_y 接口从 PSAP-ECR 70 向 SS-ECR 50 中继。此后，SS-ECR 50 可以经由 E_x 接口通过 MSC 40 请求回叫。这一活动相应于图 2 的消息流 180 到 200。

在另一实施例中，如果 PSAP-CC 90 安装了适合的线路和设备，在 PSAP-CC 90 中的传呼者可以使用 LPN 和/或 MEIN 来发起一个直接指向服务于无线单元 20 的 MSC 40 的回叫。这里，MEIN 可以插入到一个与全局地址参数（“GAP”）有关的 ISDN 使用者部分（“ISUP”）。应该注意，PSAP-CC 90 也可以使用 ESRK 来通过 D 接口发送请求 ESME 80 来请

求 ESNE 60。这一请求意在使用 LPN 和 MEIN 启动一个从 PSAP-CC 90 到 MSC 40 的回叫。这一活动对应于图 2 的消息流 210 到 220。

应该注意，MEIN 可能识别由 MSC 40 伺候的无线单元 20 来完成回叫。PSAP-CC 90 的目录号码可以包含在呼叫起始消息的呼叫方字段中。这一号码可以通过 MSC 40 而获得并且在呼叫方字段中被检测以确保授权呼叫者享有紧急呼叫服务。

参考图 3 和 4，示出了本发明的另一组具体实施例。关于图 3，示出了支持移动紧急服务的网络参考模型（"NRM"）的体系结构 300，而图 4 示出了对应于图 3 的 NRM 的消息流程图 400。更具体而言，图 3 和图 4 的实施例与用于通过呼叫中心建立呼叫的另一技术有关。

如图 3 所示，示出了用于向体系结构 300 进行"9-1-1"呼叫通信的无线单元 320。通信，当由无线单元 320 发起时，通过空中接口 U_m，经由一个基站 330，传送到 MSC 340。向体系结构 300 进行"9-1-1"呼叫通信的步骤对应于图 4 所示的图解 400 中的消息流 410。

一旦 MSC 340 接收了"9-1-1"呼叫，与无线单元 320 相关联的标识信息将传送到 ECR-SS 350 中。向 ECR-SS 350 传送信息的步骤对应于图 4 的消息流 420。更具体来说，与无线单元 320 相关联的信息包括，举例来说，MEIN。向 ECR-SS 350 传送 MEIN 将由 MSC 40 通过第一 NRM 接口 E_x 来执行。应该注意，MEIN，当向 ECR-SS 350 传送时，可以通过 IMEI、ESN、pESN 和/或 MEID 来实现。

随着 MEIN 的传送，MSC 340 也可以向 ECR-SS 350 传送 PGID 作为消息流 420 的一部分。在来自无线单元 320 的"9-1-1"呼叫从基站 330 和 MSC 340 落线或者断开与其的连接的情况下，PGID 可以用来传呼无线单元 320。为了在呼叫落线或者断开连接的情况下传呼无线单元 320，需要 MSC 340 的 LPN 来唯一标识服务于"9-1-1"呼叫者（举例来说，无线单元 320）的特定交换机或终端局。LPN 可以通过来自于分配给 MSC 340 的本机或者非便携号码组块的可拨号号码来实现。LPN 可以有助于标识 ECR-SS 350 以及当呼叫在体系结构 300 当中落线或断开连接时向"9-1-1"呼叫者发起回叫。

此外，对于 LPN，ESRK 也可以被用来唯一标识“9-1-1”呼叫者（举例来说，无线单元 320），其作为图 4 的消息流 420 的一部分。当与“9-1-1”呼叫相关联时，ESRK 可以支持无线单元 320 的本地信息的通信。参与提供 ESRK 的网络单元和接口可以，在一个实施例中，使用现有的通信标准来实现。

如上所述，PGID 可以是许多基于通信标准的标识符中的一个，如果“9-1-1”呼叫落线或者断开连接，所述标识符支持传呼无线单元 320。对于基于 GSM 的系统而言，无线单元 320 可以通过由无线单元 320 提供的 IMSI，与 IMSI 相关联的 TMSI 和/或来自无线单元 320 的 IMEI 来传呼。在 CDMA 2000 系统中，这一传呼步骤可以使用 MIN、IMSI、来自 NSI 无线单元的 dMSID、来自无线单元 320 的 ESN 和/或由无线单元 320 中的 MEID 生成的 pESN 来实现。

对比图 1 和 2 的实施例的方法，体系结构 300 和消息流程图 400 示出了呼叫相关的信令（“CAS”）和非呼叫相关的信令（“NCAS”）的组合。更具体来说，CAS 技术可以与 ESNE 360 相关联而 NCAS 方法，基于从 ESME 380 分离出 PSAP-ECR 370，与 PSAP-CC 390 相关联。相应的，这一技术可以称为移动紧急服务的 CAS 和 NCAS 混合模式。

体系结构 300 在 SS-ECR 350 和 PSAP-ECR 370 之间使用网络接口 E_y。此外，除了在 MSC 340 和 ESME 380 之间添加网络接口 E 之外，网络接口 B 也可以置于 ESNE 360 和不含 PSAP-ECR 370 的 ESME 380 之间。相应的，ESNE 360 和 PSAP-ECR 370 之间的直接接口并未示出。此外，附加的网络接口也 B_e 也包含在 PSAP-ECR 370 和 ESME 380 之间。网络接口 D 可以置于 ESME 380 和 PSAP-CC 390 之间。最后，单独的附加网络接口 D_e 包含在 PSAP-ECR 370 和 PSAP-CC 390 之间。

对于与无线单元 320 相关联的从 MSC 340 接收的标识信息，与图 1 和 2 所示的实施例不同，SS-ECR 350 可以通过 E_y 接口将关于新的紧急呼叫的信息传送到 PSAP-ECR 370。这一活动对应于图 4 的消息流 430。应该注意，PSAP-ECR 370 是与 ESME 380 逻辑上分立的。相应的，LPN、MEIN 和 ESRK 可以通过 B_e 接口从 PSAP-ECR 370 传送到 ESME 380。

此后，ESRK 可以随着呼叫（举例来说，作为呼叫相关信令）经由 A_{ix} 接口与 LPN 和 MEIN 一起通过 MSC 40 传送到 ENSE 360。这一活动相应于图 4 的消息流 440。应该注意，ESRK 可以通过 C 接口从 ESNE 360 发送到 PSAP-CC 390，而 LPN 和 MEIN 可以通过 B 接口从 ESNE 360 发送到 ESME 380，此相应于消息流 450。

一旦 ESRK 随着呼叫传送并且通过 C 接口被发送，PSAP-CC 390 可以使用 ESRK 来询问 ESME 380。这一询问意在向 PSAP-CC 390 提供与无线单元 320 相关的回叫号码（举例来说，LPN 和 MEIN）。这一活动相应于图 4 的消息流 460。

接着，ESME 380 可以响应 PSAP-CC 390。更具体来说，ESME 380 可以提供回叫号码、无线单元位置以及 PSAP-CC 390 处理紧急呼叫所需的其他有关信息。这一活动相应于图 4 的消息流 470。

如果“9-1-1”呼叫落线或者断开连接，PSAP-CC 390 可以使用 ESRK 通过 D 接口向 ESME 380 发送信号。这样做，就可以通过 MSC 340 请求回叫。这一活动相应于图 4 的消息流 480。此后，ESME 380 可以使用在其数据库中与 ESRK 相关联的 MEIN 通过 MSC 340 向 PSAP-ECR 370 请求回叫，此相应于消息流 490。作为选择，PSAP-ECR 370 可以使用 MEIN 向 PSAP-CC 390 发送信号指示其可以使用该 MEIN 向 PSAP-ECR 370 发送信号以指示其直接经由 D_e 接口通过 MSC 340 请求回叫，其相应于消息流 495。

接着，PSAP-ECR 370 可以使用 EMIN 通过 MSC 服务器请求回叫。此处，随着来自 PSAP-ECR 370 通过 SS-ECR 350 传送的请求，MSC 340 发起回叫。这一活动相应于图 4 的消息流 500。最后，SS-ECR 350 可以向 MSC 340 提供 PGID 并通过 MSC 340 请求一个向无线单元 320 和 PSAP-CC 390 的回叫。

虽然本特定发明已参考所示的具体实施例被描述，但是这些描述不具有限定性的意义。应该理解，虽然已经描述了本发明，参考这些说明，所示实施例以及本发明额外的实施例的各种变化对于本领域的普通技术人员而言是显而易见的，且不背离由附加的权利要求所述的本发明的精

髓。相应的，方法、系统及其各部分和所述方法和系统可以在不同的地点实施，诸如无线单元、基站、基站控制器和/或移动交换中心，举例来说。此外，实施和使用所述系统的处理电路可以由专用集成电路、软件驱动处理电路、固件、可编程逻辑设备、硬件、具体的组件或者上述组件的排列来实现，本领域的普通技术人员可以很容易的理解。本领域的普通技术人员将容易的认识到本发明可以具有不严格符合在此实例申请中所述的这些和各种其他的改变、安排和方法，但其不背离本发明的精髓和范围。附加的权利要求书将覆盖这些落入本发明实际范围内的改变或实施例。

图1

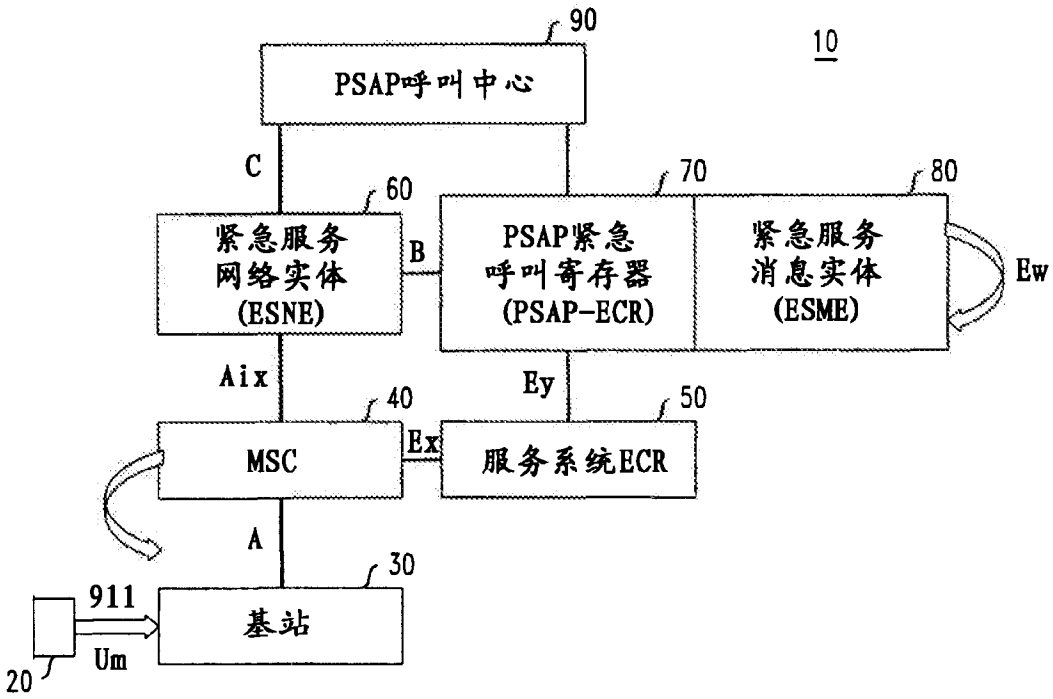


图 2

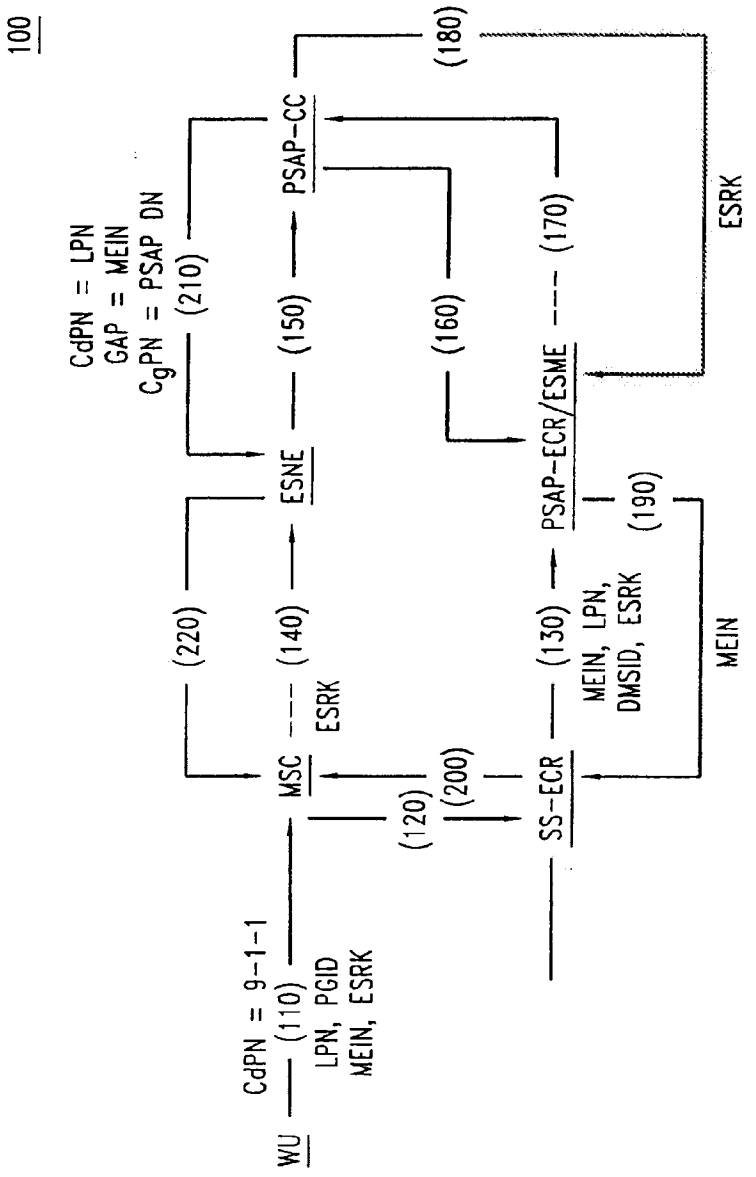


图3

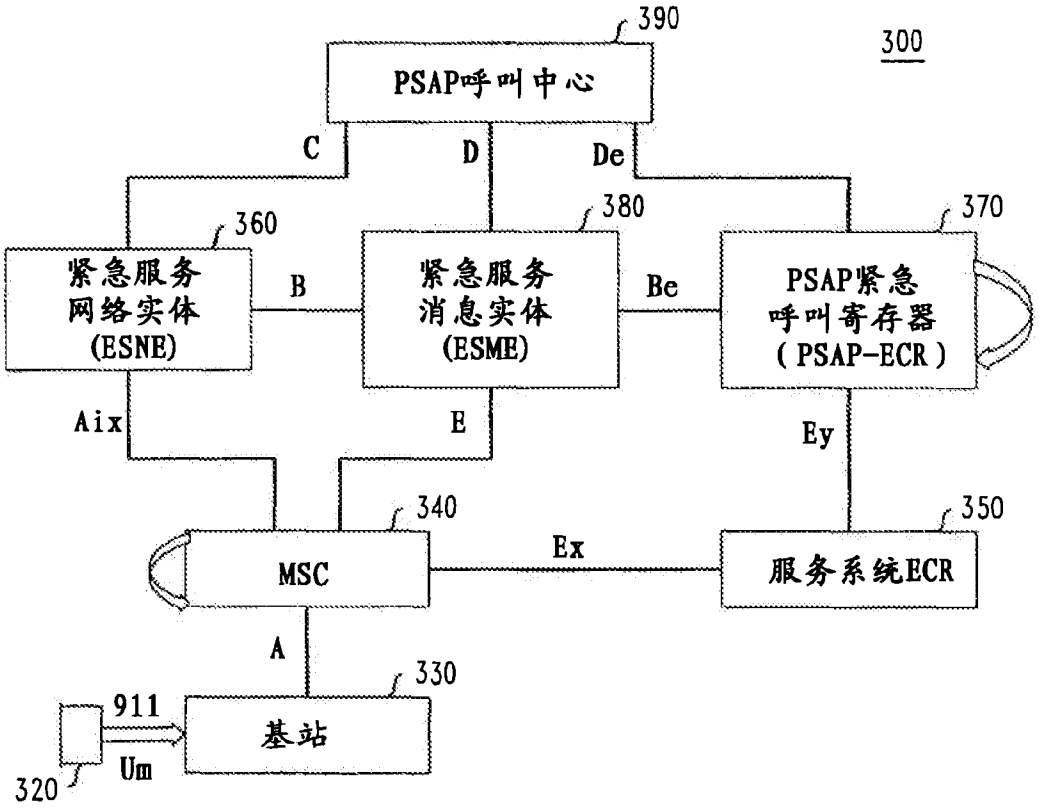
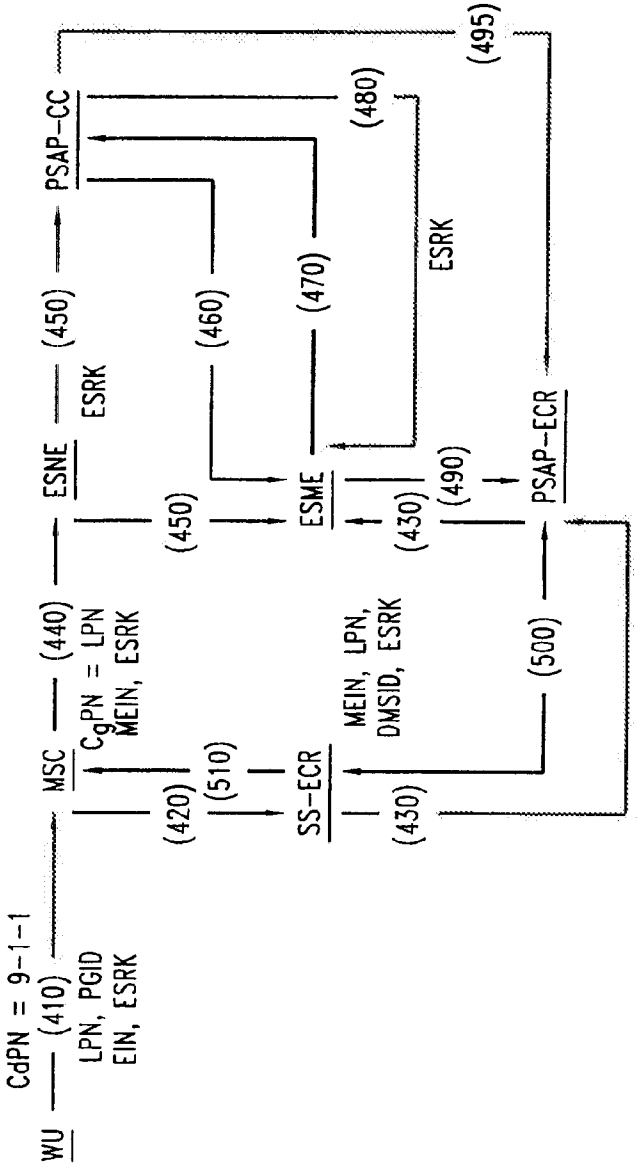


图 4



Espacenet

Bibliographic data: CN1274114 (C) — 2006-09-06

Method and communication system for monitoring data flow in data network

Inventor(s): KREUSCH H STIFTER W PFEHLER N [DE] + (H. STIFTER, ; W. PFEHLER, ; N. KREUSCH, ; H. STIFTER,W. PFEHLER,N. KREUSCH)

Applicant(s): SIEMENS AG [DE] + (SIEMENS AG)

Classification: - international:***H04L12/26; H04L29/06; H04L29/08; H04M3/22***
- cooperative: **H04L12/2602**; **H04L29/06**; **H04L43/00**; **H04L63/00**; **H04L63/30**; **H04L65/103**; **H04L65/1046**; **H04L65/80**; **H04L67/2814**; **H04L67/306**; **H04M3/2281**; H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

Application number: CN2002806811 20020307

Priority number(s): EP20010107063 20010321

Also published as: CN1498482 (A) EP1244250 (A1) US2004181599 (A1) US7979529 (B2) RU2003130974 (A) RU2280331 (C2) EP1371173 (A1) EP1371173 (B1) WO02082728 (A1) BR0208272 (A) less

Abstract not available for CN1274114 (C)
Abstract of corresponding document: EP1244250 (A1)

A data stream (DAT) is monitored in a data network (WWW) between two telecommunications terminals (TEA,TEB) connected to the data network via access servers (AAA,AAB), which operate during a monitoring situation to divert the data stream between the telecommunications terminals through a monitoring server (PRO) that produces a copy (KOP) of the data stream and transmits it to an analyzing unit (ASW). An independent claim is also included for a

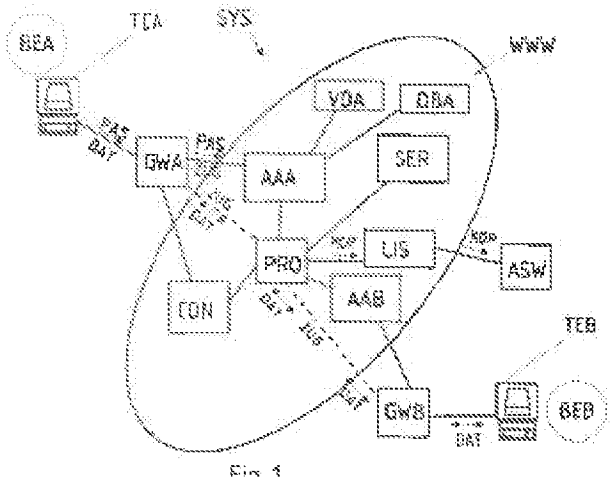


Fig. 1

PETITIONER APPLE INC. EX. 1004-322

telecommunication system for monitoring
a data stream in a data network between a telecommunications terminal linked to a data network via a gateway and to a further telecommunications device.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利说明书

专利号 ZL 02806811.4

[45] 授权公告日 2006 年 9 月 6 日

[11] 授权公告号 CN 1274114C

[22] 申请日 2002.3.7 [21] 申请号 02806811.4
[30] 优先权
[32] 2001.3.21 [33] EP [31] 01107063.8
[86] 国际申请 PCT/EP2002/002524 2002.3.7
[87] 国际公布 WO2002/082728 德 2002.10.17
[85] 进入国家阶段日期 2003.9.19
[71] 专利权人 西门子公司
地址 德国慕尼黑
[72] 发明人 H·斯蒂特 W·普菲赫勒
N·克雷斯奇
审查员 刘欣科

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 张志醒

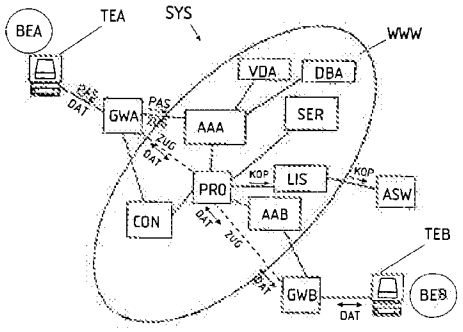
权利要求书 4 页 说明书 10 页 附图 2 页

[54] 发明名称

用于监测数据网中数据流的方法及通信系统

[57] 摘要

本发明涉及一种用于监测位于至少两个通信终端(TEA，TEB)之间的数据网(WWW)中数据流(DAT)的方法及其通信系统(SYS)，这些终端通过至少一个接入服务器(AAA，AAB)与数据网相连。在监测的情况下，通信终端(TEA，TEB)间的数据流(DAT)自接入服务器(AAA，AAB)转由监测服务器(PRO)来传送，此监测服务器产生此数据流(DAT)的副本(KOP)，并将其传送至一个评估单元(ASW)。



1. 一种用于监测位于至少一个通信终端（TEA）和至少一个另外的通信设备（SER,TEB）之间的数据网（WWW）中的数据流（DAT）的方法，所述的至少一个通信终端（TEA）通过至少一个网关（GWA,GWB）与数据网（WWW）连接，其中设置至少一个鉴权服务器（AAA,AAB）以被用来对数据网（WWW）实行接入控制（ZUG），其特征在于，通过所述至少一个鉴权服务器（AAA,AAB）检测是否应监测所述至少一个通信终端（TEA）与所述至少一个另外的通信设备（SER,TEB）间的数据流（DAT），其中在监测的情况下产生此数据流（DAT）的一个副本（KOP），该副本被附上一个标识（IDK），且副本连同其上的标识（IDK）被传送到至少一个LI-服务器（LIS）和/或直接被传送到一个评估单元（ASW）。

2. 根据权利要求1中所述的方法，其特征在于，所述副本（KOP）通过所述网关（GWA,GWB）产生。

3. 根据权利要求1中所述的方法，其特征在于，所述副本通过一个专门设立的监测服务器（PRO）产生。

4. 根据权利要求1至3中之一所述的方法，其特征在于，所述LI-服务器根据标识（IDK）确定，是否应产生此副本（KOP）的至少一个二次副本（WKO），以及该副本（KOP）和/或至少一个二次副本（WKO）应被传送给谁。

5. 根据权利要求4中所述的方法，其特征在于，所述LI-服务器（LIS）产生所述副本（KOP）的至少一个二次副本（WKO）。

6. 根据权利要求1至3之一所述的方法，其特征在于，所述LI-服务器（LIS）执行与评估单元（ASW）的接口匹配。

7. 根据权利要求1至3之一所述的方法，其特征在于，所述鉴权服务器(AAA,AAB）根据分配给一个隐藏数据库（DBA,DBB）中的至少一个通信终端（TEA）的监测标识（UWD）来确定，是否存在一个监测情况。

8. 根据权利要求7所述的方法，其特征在于，所述隐藏数据库（DBA,DBB）和一个用于管理用户概况及用户鉴权数据的管理数据库（VDA,VDB）进行通信连接，并且每一个在管理数据库（VDA,VDB）中登录的用户（BEA,BEB）被分配隐藏数据库（DBA,DBB）中的一个监测标识（UWD）。

9. 根据权利要求8所述的方法，其特征在于，在清除所述管理数据库(VWA,VWB)中用户鉴权数据的情况下，所述隐藏数据库（DBA,DBB）中所分配的监测标识（UWD）也被清除。

10. 根据权利要求1所述的方法，其特征在于，作为IP承载语音的数据流来传输所述的数据流（DAT）。

11. 根据权利要求3中所述的方法，其特征在于，由一个呼叫控制器（CON）通过产生所述副本（KOP）的监测服务器（PRO）转发所述数据流（DAT）。

12. 根据权利要求3所述的方法，其特征在于，在监测状态下，所述鉴权服务器（AAA,AAB）通过监测服务器（PRO）转发数据流（DAT）。

13. 根据权利要求3所述的方法，其特征在于，所述数据通道（ZUG）从网关（GWA,GWB）被隧穿至监测服务器（PRO）。

14. 根据权利要求3所述的方法，其特征在于,所述数据流（DAT）的副本(KOP)被暂存在所述监测服务器（PRO）上。

15. 根据权利要求1至3之一所述的方法，其特征在于,所述数据流（DAT）的副本（KOP）被缓存在所述LI-服务器上。

16. 根据权利要求10至14之一所述的方法，其特征在于,所述控制器（CON）不仅控制所述网关（GWA,GWB），还控制所述监测服务器（PRO）。

17. 根据权利要求11至14之一所述的方法，其特征在于，由所述至少一个鉴权服务器（AAA,AAB）控制所述的监测服务器。

18. 用于监测位于至少一个通信终端（TEA）和至少一个另外配置的通信设备（SER,TEB）之间的数据网（WWW）中的数据流（DAT）的通信系统，所述的至少一个通信终端（TEA）通过至少一个网关（GWA,GWB）与数据网（WWW）连接，其中设置至少一个鉴权服务器(AAA,AAB)以被用来对数据网（WWW）实行接入控制（ZUG），其特征在于，鉴权服务器（AAA,AAB）被用来检测是否应监测所述至少一个通信终端（TEA）与所述至少一个另外的通信设备（SER,TEB）间的数据流（DAT），其中此通信系统（SYS）被配置用来在监测情况下产生所述数据流（DAT）的一个副本（KOP），并为此副本（KOP）附加一个标识（IDK），以及将此副本(KOP)连同其标识（IDK）传送至至少一个LI服务器（LIS）和/或直接传送至一个评估单元（ASW）。

19. 如权利要求18所述的通信系统,其特征在于，所述网关（GWA,GWB）被用于产生数据流（DAT）的副本（KOP）。

20. 如权利要求18所述的通信系统，其特征在于，提供一个监测服务器（PRO），其适用于产生副本（KOP）。

21. 如权利要求18至20之一所述的通信系统,其特征在于，LI-服务器被用来根据标识(IDK)确定是否应该产生副本(KOP)的至少一个二次副本(WKO)，并且此副本（KOP）和/或至少一个二次副本（WKO）应传送给谁。

22. 如权利要求21所述的通信系统，其特征在于，LI-服务器被用来产生所述副本（KOP）的至少一个二次副本（WKO）。

23. 如权利要求18至20之一所述的通信系统,其特征在于，LI-服务器被用来执行评估单元（ASW）的接口匹配。

24. 如权利要求18至20之一所述的通信系统，其特征在于，所述鉴权服务器（AAA,AAB）被用来根据隐藏数据库中至少一个通信终端（TEA）所分配的监测标识（UWD）来确定是否存在监测情况。

25. 如权利要求24所述的通信系统，其特征在于，所述隐藏数据库（DBA,DBB）和一个被分配给鉴权服务器的、用于管理用户概况和用户鉴权数据的管理数据库(VDA,VDB)被设置用来进行数据的相互交换,其中每个在管理数据库（VDA,VDB）中登录的用户（BEA,BEB）都分配有隐藏数据库（DBA,DBB）中的一个监测标识（UWD）。

26. 如权利要求25所述的通信系统，其特征在于，一旦清除管理数据库（VWA,VWB）中的用户鉴权数据，该通信系统就被用来清除其在隐藏数据库（DBA,DBB）中所分配的监测标识（UWD）。

27. 如权利要求18所述的通信系统,其特征在于，数据流（DAT）是IP承载语音的数据流。

28. 如权利要求20所述的通信系统，其特征在于,提供一个呼叫控制器(CON),其用于在监测情况下通过监测服务器（PRO）转发数据流（DAT）。

29. 如权利要求20所述的通信系统，其特征在于，所述鉴权服务器（AAA,AAB）被用来在监测情况下通过监测服务器（PRO）转发数据流（DAT）。

30. 如权利要求20所述的通信系统,其特征在于，该通信系统被用来隧穿由网关（GWA,GWB）至监测服务器（PRO）的数据通道。

31. 如权利要求20所述的通信系统，其特征在于，所述监测服务器被用来中间缓存数据流（DAT）的副本(KOP)。

32. 如权利要求18所述的通信系统，其特征在于，所述LI服务器被用来暂存数据流（DAT）的副本（KOP）。

33. 如权利要求28至32之一所述的通信系统，其特征在于，所述呼叫控制器（CON）被用来不仅控制网关（GWA,GWB），还控制监测服务器（PRO）。

34. 如权利要求29至32之一所述的通信系统，其特征在于，所述鉴权服务器（AAA,AAB）被用于控制监测服务器。

35. 如权利要求20所述的通信系统，其特征在于，所述监测服务器(PRO)具有代理服务器的功能。

用于监测数据网中数据流的方法及通信系统

技术领域

本发明涉及一种用于监测位于至少一个通信终端和至少一个另外的通信设备之间的数据网中的数据流的方法，所述的通信终端通过至少一个网关与数据网连接，所述的另外的通信设备可配置至少一个鉴权服务器，其目的在于执行通向数据网的接入控制。

本发明还涉及一种用于监测位于至少一个通信终端和至少一个另外配置的通信设备之间的数据网中的数据流的通信系统，所述通信终端通过至少一个网关与数据网连接，所述的另外的通信设备可配置至少一个鉴权服务器，其目的在于执行通向数据网的接入控制。

背景技术

规则制定者越来越多地要求数据网的运营商提供一些功能，使得在需要时对用户的数据交换进行监测成为可能。

目前在数据网如因特网中对数据流的合法监听，即所谓“合法截听”的问题是以不同的方式解决的。

一种已知的方法是在一个要监测的局域网中配置外部取样器（分析器），它们分析总分组数据流，过滤并复制被监测者的通信，并传送给业务承运商。此方法的缺点主要是对网络的规定时限的物理干涉是不可避免的。由于被监测者的移动性增大，这种方法就不实用了。

另外一种用于电子邮件通信监听/监测的方法首先是在一个或更多电子邮件服务器上执行一种自动转发功能，它把到达和发出的电子邮件传送给业务承运商，比如官方机构。类似地可用于语音邮件等。使用这种方法所不可避免的是，必须配置所有的电子邮件服务器来识别监听/监测情况，并转发到主管官方机构，这导致高额的管理开支。

WO 0042742中描述了一种在面向分组的网如GPRS网或UMTS网中用于执行合法监听的监测方法和监测系统。为此提供了一个具有数据分组监测功能的

第一网元，它通过第二网元来控制。被截获的（被监测出的）数据将通过一个网关，此网关具有一个通往有监听资格的官方机构的接口。这种方法的缺点主要是那些不应被监听的用户的数据流也会流经所述网元，这就从根本上增加了此方法的技术和管理开支。

关于因特网中的“合法截听”例如请参见ETSI TR 101 750 V1.1.1.

非常高额的费用是不容忽视的，这些费用通常是因为网络运营商在提供前述的监听/监测功能时产生的，这主要由高额的管理开支而引起。

发明内容

所以本发明的一项任务是实现一种途径，此途径通过简单且节省开支的方式实现了在一种数据网中执行监听/监测功能。

此任务由前述的方法以如下方式来解决，通过至少一个鉴权服务器来检测是否应监测在至少一个通信终端和至少一个另外的通信设备之间的数据流，其中在监测情况下产生数据流的一个副本，它被附上一个标识，此副本同标识一起被传送到至少一个LI-服务器和/或直接传送到一个评价单元。

据此，根据本发明的用于监测位于至少一个通信终端和至少一个另外的通信设备之间的数据网中的数据流的方法，所述的至少一个通信终端通过至少一个网关与数据网连接，其中设置至少一个鉴权服务器以被用来对数据网实行接入控制，通过所述至少一个鉴权服务器检测是否应监测所述至少一个通信终端与所述至少一个另外的通信设备间的数据流，其中在监测的情况下产生此数据流的一个副本，该副本被附上一个标识，且副本连同其上的标识被传送到至少一个LI-服务器和/或直接被传送到一个评估单元。

本发明的一个好处就是设置了网络侧的监听功能，通过此可避免网络中由外部监听装置引起的干涉。另外，如果被监测者是移动的且所处位置改变，则访问该被监测者的数据流也是可能的，因为该被监测者必须通过设置所述监测措施的提供商的鉴权服务器才能拨入。

本发明的一种变型是由网关产生所述副本。

本发明的另一种变型是由特别为此所提供的监测服务器来产生所述的副本。

优选地，所述LI-服务器根据标识确定，是否应该产生所述副本的至少一个二次副本，并且确定将所述副本和/或至少一个所述二次副本应传送给谁。

有利地，由LI-服务器产生至少一个所述的二次副本，也就是说，此LI-服务器复制对应于合理数位的数量的副本。

通过LI-服务器实现对评估单元的一个接口匹配，就能得到本发明其他优点。

鉴权服务器可以根据隐藏数据库中的至少一个所述通信设备所分配的监测标识来确定，是否存在一种监测情况。

所述隐藏数据库与一个用于管理用户概况及其鉴权数据的管理数据库建立连接，其中，每个在管理数据库中登录的用户就在该隐藏数据库中分配一个监测标识。

在清除管理数据库中的用户鉴权数据的情况下，所述隐藏数据库中分配的监测标识也被清除。

本发明的另一变型是以IP承载语音的数据流的形式传输数据流，其中，呼叫控制器通过产生所述副本的监测服务器转发数据流。

另一种可能是鉴权服务器在监测状态下通过所述监测服务器转发数据流。

所述转发的变型是，提供由所述网关隧穿至所述监测服务器的数据通道。

如果不能将所述副本立即发送给业务承运商，为避免丢失数据，可以将所述数据流的副本暂存在监测服务器和/或LI-服务器上。

在本发明的一个优选实施方式中，所述控制器既控制网关也控制所述监测服务器。

本发明的另一个非常有利的实施方式在于，至少有一个鉴权服务器控制监测服务器。

上述现有技术中的通信系统尤其适合用于执行根据本发明的方法，为此在通信系统中配置了所述鉴权服务器，以便检测是否应监测处于至少一个所述通信终端与至少一个所述另外的通信设备之间的数据流，此外配置所述通信系统的目的在于，在监测的情况下产生数据流的一个副本，为此副本附加一标识，并且把此副本连同其标识传送给至少一个LI-服务器和/或直接传送给一个评估单元。

据此，根据本发明的用于监测位于至少一个通信终端和至少一个另外配置的通信设备之间的数据网中的数据流的通信系统，所述的至少一个通信终端通过至少一个网关与数据网连接，其中设置至少一个鉴权服务器以被用来对数据网实行接入控制，鉴权服务器被用来检测是否应监测所述至少一个通信终端

与所述至少一个另外的通信设备间的数据流，其中此通信系统被配置用来在监测情况下产生所述数据流的一个副本，并为此副本附加一个标识，以及将此副本连同其标识传送至至少一个LI服务器和/或直接传送至一个评估单元。

在本发明的第一个变型中所述网关被配置用来产生所述数据流副本。

在本发明的另一个变型中提供有一个监测服务器，配置此监测服务器用于产生所述副本。

此外配置所述LI-服务器的目的在于，根据标识确定是否应产生所述副本的至少一个二次副本,并且确定该副本和/或所述至少一个二次副本应传送给谁。

更有利的是配置所述的LI-服务器以产生所述的至少一个二次副本。

通过配置所述LI-服务器以便实现对所述评估单元的接口匹配，可实现其他的优点。

可以配置所述鉴权服务器以便根据在隐藏数据库中的至少一个所述通信终端所分配的监测标识，来确定是否存在一种监测情况。

配置所述隐藏数据库和一个给所述鉴权服务器分配的、用于管理用户概况及其鉴权数据的管理数据库，以便彼此交换数据，其中，把所述隐藏数据库中的一个监测标识分配给每一个在所述管理数据库中登录的用户。

可以配置该通信系统，以便在清除所述管理数据库中的用户鉴权数据的情况下，清除所述隐藏数据库中所分配的监测标识。

在本发明的一个有利的变型中，数据流是IP承载语音的数据流，其中提供了一个呼叫控制器，其配置用于在监测的情况下通过所述监测服务器转发数据流。

另一个有利的变型在于，配置所述鉴权服务器，以便在监测的情况下通过所述监测服务器转发数据流。

通过配置所述通信系统能得到其他好处，其目的在于，隧穿从网关到监测服务器的数据通道。

为了防止数据丢失，可以配置所述监测服务器和/或所述LI-服务器，以便暂存所述数据流的副本。

此外可以配置所述呼叫控制器，以便既控制所述网关又控制所述监测服务器。

在另一种变型中，配置了鉴权服务器来控制监测服务器。

有利地，所述监测服务器具有代理服务器的功能。

附图说明

在下文中，借助附图中非限制性的实施例描述本发明及其他的优点，图中示出了：

图1：根据本发明的通信系统，

图2 a：带有一个标识的一个数据流的副本，

图2 b：图2 a中的标识的细节，和

图3：根据本发明方法的示例性的流程图。

具体实施方式

按照图1，本发明通信系统SYS的每一个想要通过自己的通信终端TEA或通信装置TEB接入一个数据网WWW、例如接入因特网的用户BEA，BEB，必须通过一个网关GWA，GWB拨入或者注册到一个接入服务器AAA。在本申请中，一个通信装置被理解为任何一种通信终端，例如一个与数据网连接的PC或者某些能在数据网WWW中存在的服务器。

接入服务器AAA，AAB可以构成为AAA-服务器或者远程鉴权拨入用户业务的服务器，简称RADIUS服务器。为了得到一个接入数据网WWW的数据通道ZUG，对于一个用户来说，鉴权是必不可少的。

在此情况下，一个用户BEA，BEB的鉴权可以通过输入一个口令PAS或输

入一个用户标识，例如用户的名字加以实现。

根据识别结果，接入服务器AAA，AAB决定一个通往数据网WWW的数据通道ZUG是否被允许或者被拒绝。

用户BEA，BEB的鉴权可以由接入服务器AAA侧借助于向一个管理数据库VDA的询问加以实现，在此管理数据库中实现对用户数据的管理。

如果存在一个正面的鉴权结果，就可以向一个隐藏数据库提问，在此数据库中一个监测标识UWD被分配给每一个在这个管理数据库中登录的用户。如果监测标识UWD说明处于用户BEA的通信终端TEA和另一个通信终端之间的一个数据流DAT应该被引导通过，那么就产生数据流DAT的一个副本KOP。

原始数据流DAT的副本KOP，例如可以由被分配给通信终端TEA的网关GWA，或者由一个特意为此提供的监测服务器PRO产生。

如果监测服务器PRO产生原始数据流DAT的副本的话，则通过监测服务器PRO转发数据流DAT。这个服务器优选地具有代理功能。监测服务器PRO与一种代理服务器的区别仅仅在于，配置监测服务器PRO是为了执行通过它运行的(被转发的)数据流DAT的副本KOP，给该副本设立一个一起被提供的标识IDK(图2)，例如IP-地址或即将被监听的用户的一个用密码书写的标识，并且传送给一个“合法截听”服务器或者，简而言之，传送给一个LI-服务器LIS，在此情况下原来的数据流被继续传送给通过用户确定的目标地址。

如果由网关GWA产生副本KOP，那么上述副本的和向LI-服务器继续传送副本KOP的功能或者根据用户所确定的目标地址传送原来的数据流DAT的功能，将在网关GWA中得以实现。

在监测的情况下，一个通向数据网WWW的数据通道ZUG，对于即将被监测的用户BEA来说，可以直接通过网关和监测服务器PRO得以实现。

转发通往监测服务器PRO的数据流DAT可以借助于隧道，例如按照在RFC 2661中详细说明的L2T-协议得以实现。

通过监测服务器PRO转发数据流DAT的另一种可能性在于，把数据网中的一个地址分配给监测服务器PRO，如果是因特网的话，则把一个IP-地址分配给监测服务器PRO。这个地址可以被存放在接入服务器AAA，AAB的一个存储装置中，与此同时在监测的情况下，数据流DAT例如按照TCP / IP-协议继续向监测服务PRO的地址传送。

正如上文所述，监测服务器PRO产生通过它被转发的数据流DAT的副本KOP，并且把这一副本KOP传送到一LI-服务器，此服务器根据附在其上的标识IDK决定对这样的副本KOP应该怎样处置，例如是否应该产生其他的副本，即该副本的二次副本WKO，或者应该将这样的副本传送至哪种评估单元。

然后在评估单元ASW中，例如在一个官方机构为此而配置的PC中，完成副本KOP的进一步的处理和分析。

LI-服务器LIS通常是若干工作站的一种配置。正如上面所述,其任务在于，接收数据流DAT的副本KOP，分析由监测服务器附在副本KOP上的标识IDK，如有可能则产生副本KOP的其他的副本WKO，并且将其送交业务承运商。

配置LI-服务器以用于对业务承运商的各种不同的评估单元实施接口匹配。因此，例如对于监测来说，向执行监测的官方机构的已知时分复用（简称TDM）-切换-接口建立两个H-323通信连接可能是必要的。另一种可能性在于，通过一个IP-切换-接口向进行监测的官方机构送交这个副本。

LI-服务器LIS为了向业务承运商或者评估单元ASW进一步传送这个副本所需要的信息，能够由业务承运商一方在一个数据库LID中存放。

另一个可能性在于，由监测服务器PRO或者网关GWA直接向评估单元ASW传送此副本KOP连同标识IDK。

在产生数据流DAT的副本KOP之后，由监测服务器PRO以传统方式，例如根据TCP / IP-协议，将原始数据流DAT进一步路由给第二个用户BEB或者通信装置TEB，SER。

按照图2a，把一个标识IDK作为起始写在数据流DAT的副本KOP的前面。此标识至少可具有一个IP-头IPH，例如被监测的用户BEA的IP-地址。此外还可以提供一个特别的LI-头LIH(图2b)，此LI-头包含关于进一步数据传送的信息。于是，例如第一行可以含有消息的类型TYP，例如是否涉及一种语音消息或者一个“被监听的”电子邮件。下一行可以含有头长LEN，而在第三行可以含有按照标准ETSI ES 201671的一个操作员ID即OID。一个呼叫标识码CIN可用于对一个“被监听的”用户BEA的识别；而官方机构标识LID则用于标识副本KOP应被传送到的哪一个业务承运商。需要时，其他的信息SUP可以附加给上述已知的标识。

按照图3，在语音传输的情况下，根据IP承载语音协议，一个相应的应用

程序APP在呼叫方BEA的通信终端TEA上被启动，这个通信终端于是通过第一网关GWA建立与第一接入服务器AAA的连接。该接入服务器AAA检测，哪一个用户打算需要语音传输服务，并检测其是否有权要求这样的服务。为此目的建立了网关GWA与接入服务器AAA之间的H．323或RADIUS-通讯。

如果呼叫用户BEA有权使用语音服务，那么接入服务器AAA根据用户BEA的鉴权检查，是否应该检测呼叫方与被呼叫方间的数据交换。

在成功地进行接入检查之后，呼叫控制器CON通过与第二接入服务器AAB的通信，查明被叫的通信终端TEB的IP-地址，并且通过另一个网关GWB促使与这个通信终端TEB的信令通信。

如果这时要对呼叫方进行监测，那么控制器CON并不直接建立网关GWA与被呼叫的通信终端TEB的连接，正如通常的情况那样，而是引入监测服务器PRO。也就是说第一个通信终端TEA与第二个通信终端TEB的连接被拆成两段，即被拆成从第一个通信终端TEA到监测服务器PRO的一段和从监测服务器PRO到第二个通信终端TEB的一段。

在正常情况下，控制器CON控制第一个网关GWA。然而由于监测的缘故，接通数据网WWW的通道被延长至所述监测服务器PRO，并且在那里本来只开始为用户BEA的数据流DAT进行正常路由，所以配置所述控制器CON以实现从网关到所述监测服务器的“切换”。这就是说，通过第一个接入服务器AAA通知所述控制器CON存在一种监测情况，以及被监测的通信终端TEA的数据通道ZUG隧穿监测服务器PRO。所述控制器从这时起把所述监测服务器PRO视为“新的”第一网关GWA，并像控制网关GWA一样来控制该服务器。因此在监测的情况下，所述呼叫控制器CON就将所述监测服务器PRO视为网关GWA一样，这种情况既适用于呼叫方又适用于被叫方。

正如上文所述，所述监测服务器PRO接下来产生所述两个通信终端TEA和TEB之间的数据流DAT的副本KOP。为产生此副本KOP，初始的数据流DAT在所述监测服务器PRO中被加倍。所述初始数据流DAT在加倍之后由所述监测服务器PRO向第二个通信终端TEB继续路由，而所述数据流DAT的副本KOP如前所述被转发到LI-服务器或者评估单元ASW。

所述监测服务器PRO也可配置作为LI-服务器LIS，用于暂存所述副本KOP以在向评估单元ASW的直接传送不可能的情况下，避免数据丢失。

为了在对初始数据流DAT的质量和速度无显著损失的情况下实现监听，位于监测服务器PRO与网关GWA之间的那段应该很短，因此如果在所述数据网WWW中安排大量的监测服务器PRO则是有利的。

如果被呼叫的用户BEB应被监测，则基本上通过如上所述的方法实现；其中，第二个接入服务器AAB可以根据被呼叫方BEB的IP-地址实现鉴权，并通过所述监测服务器PRO转发数据流DAT。

为了实现根据被呼叫方BEB的IP-地址对其鉴权的目的，第二个接入服务器AAB可以包括一个数据库DAB，该数据库含有所述被叫方的IP-地址和被叫方是否被监听的记录。

对用户BEA进行监测的命令由一个有权监测的官方机构发出，并将其记录在隐藏数据库DBA中。

如果被监测的用户BEA在其通信终端上启动一个在数据网WWW中进行数据传输的应用程序，如上文所述，那么实现用户鉴权并确定是否存在一种监测情况。

在监测的情况下，例如在其上已存放一主页或其他数据的一个服务器向A方传送所述监测服务器PRO的地址，而不转发被叫方BEB的地址或通信装置TEB SER的地址。B方的网关GWB从鉴权服务器AAA或呼叫控制器CON获得监测服务器PRO的网络地址，而不是呼叫方BEA的网络地址。

由所述鉴权服务器AAA或呼叫控制器CON通知监测服务器PRO是否应进行监测。所有用于监测和连接的必要信息，例如“把A方与B方连接”的信息及类似信息，可以通过H．248传输而由所述鉴权服务器AAA或呼叫控制器CON传送至所述监测服务器PRO。

如上文所述，位于A方与B方用户或服务器之间的数据流DAT在所述监测服务器中被加倍，其中被加倍的数据被附上一个标识IDK，这样产生的副本KOP在以后被传送所述给LI-服务器。

对于原始数据流，监测服务器具有与代理服务器一样的功能，并且只连接A方与B方。

本发明的另一个变型在于，A方从鉴权服务器AAA或呼叫控制器CON那里收到B方端的网络地址；在此情况下，借助于H．248传送而请求A方的网关把源于用户BEA的所有数据业务都隧道传送给监测服务器。与此同时，由呼叫

控制器把监测服务PRO的地址而不是A方的网络地址传送给其网络地址已知的B方。

所述监测服务器PRO从所述呼叫控制器那里得到隧道传送的相应信息，并且将A和B方连接起来。

隧道的优点在于，对于被监测的用户BEA来说，通过监测服务器PRO转发数据流所必要的地址改变是不明显的。

如果鉴权服务器AAA，AAB或者呼叫控制器通过H．248通信而通知监测服务器PRO：一个数据流DAT被转发，那么监测服务器就能够把一个启动消息传送给LI-服务器，以至于这个LI服务器从LI-数据库中询问必要的数据，并在副本KOP到达时可使用这些数据。

如果被监测的数据交换结束,那么呼叫控制器CON就通知监测服务器PRO,其应该中断与LI-服务器的关于该具体监测的通讯。在收到一个源于监测服务器PRO的一条结束消息之后，LI-服务器能够重新清除来自LI-数据库的数据，并且停止与业务承运商的通信。

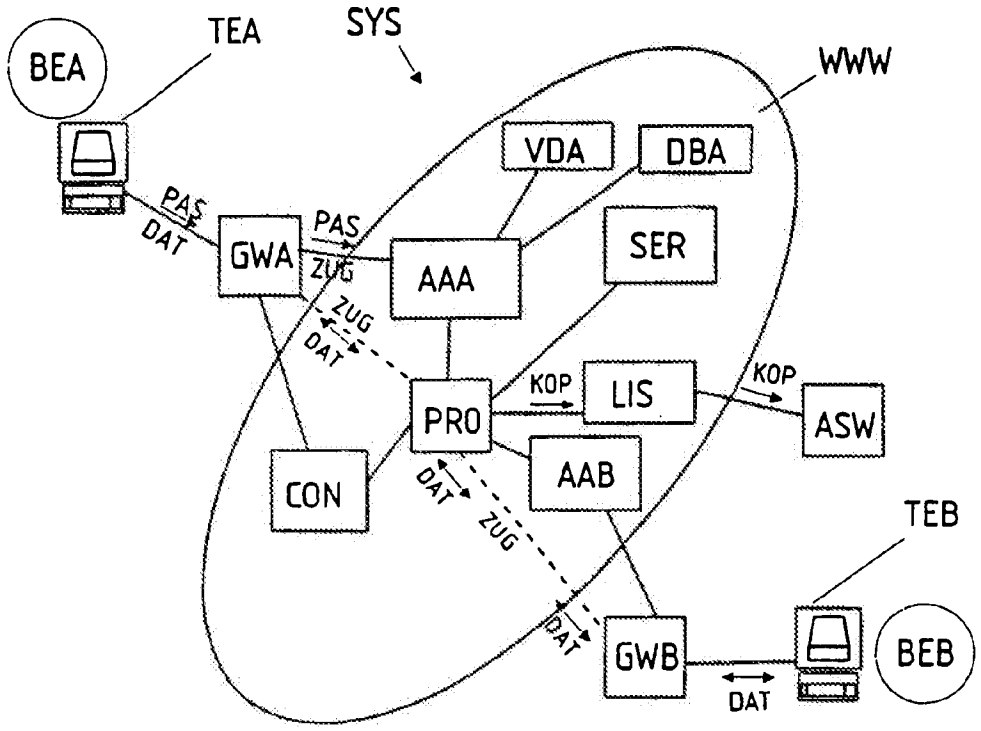


图 1

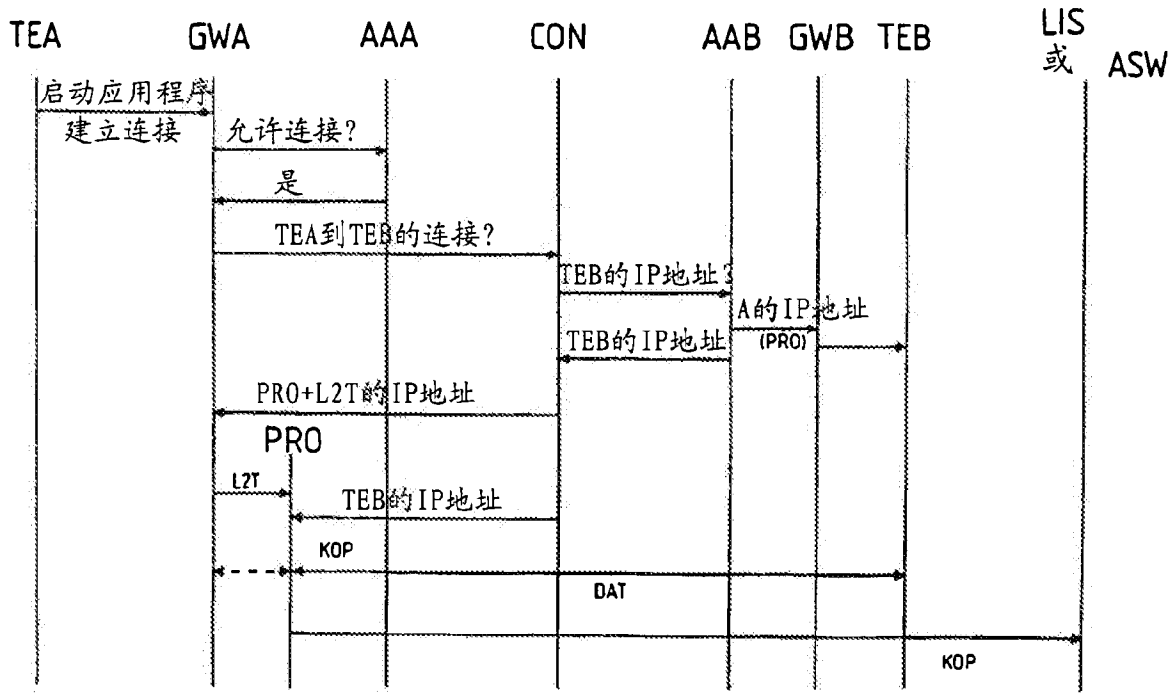


图 3

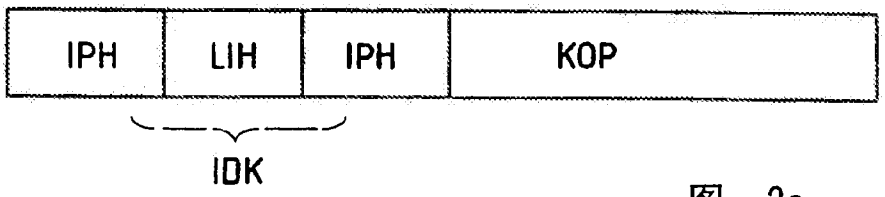


图 2a

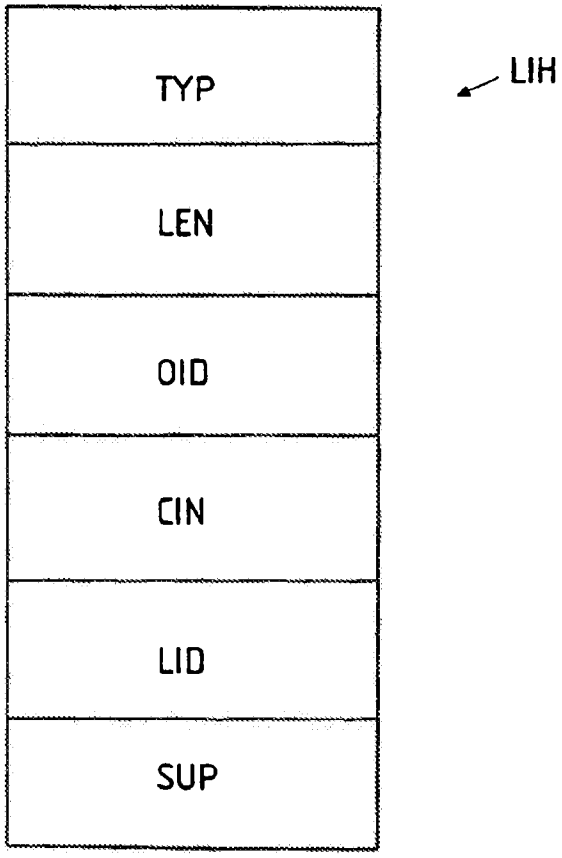


图 2b

Espacenet

Bibliographic data: CN101005503 (A) — 2007-07-25

Method and data processing system for intercepting communication between a client and a service

Inventor(s): THOMAS ANDRESS JIRI HEINE STEF [US] ± (ANDRESS JIRI,HEINE STEFAN,VON KULESSA THOMAS, ; ANDRESS JIRI, ; VON KULESSA THOMAS, ; HEINE STEFAN)

Applicant(s): IBM [US] ± (IBM)

Classification: **- international:** ***H04L29/06; H04L9/00***
- cooperative: **H04L63/08; H04L63/0884**

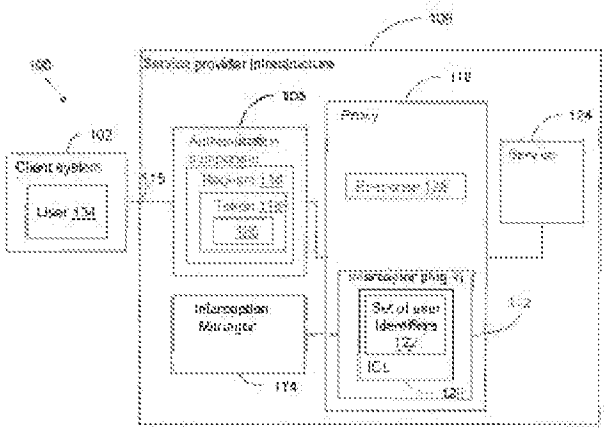
Application number: CN2007101788 20070116

Priority number (s): EP20060100369 20060116

Also published as: CN101005503 (B) US2007174469 (A1) US8024785 (B2)

Abstract of CN101005503 (A)

A method of monitoring communication between client-side and serveice, wherein the method includes a step of performancing user certification of the client-side user and a step of receiving requests from the client-side user via the service. The requests contains user special marks including unique user identifier. The user special marks can be allocated to the user requests thanks to user certification. If the unique user identifier equals to one user identifier of a group of unique user identifiers, the user requests are stored, wherein using the unique user identifier as key. The service sends answers relative to the requests, if the unique user identifier of the request is included in the group of unique user identifiers, storing copy thereof.



[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 9/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710001788.8

[43] 公开日 2007 年 7 月 25 日

[11] 公开号 CN 101005503A

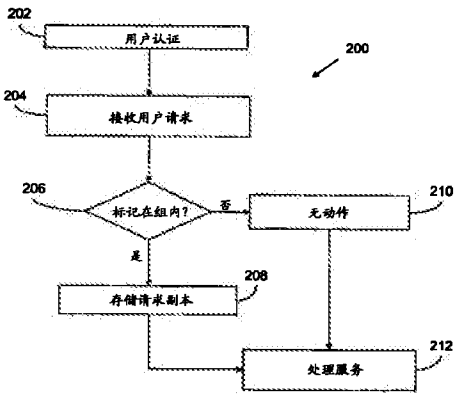
[22] 申请日 2007.1.16
[21] 申请号 200710001788.8
[30] 优先权
[32] 2006. 1.16 [33] EP [31] 06100369.5
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 托马斯·冯库莱萨 斯蒂芬·海因吉里·安德烈斯
[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森
权利要求书 4 页 说明书 13 页 附图 7 页

[54] 发明名称

用于侦听客户端和服务之间的通信的方法和数据处理系统

[57] 摘要

提供了一种侦听客户端和服务之间的通信的方法，其中该方法包括执行所述客户端的用户的用户认证的步骤以及由所述服务从所述客户端的用户接收请求的步骤。 所述请求包括用户特有标记，并且该用户特有标记包括唯一的用户标识符。 该用户特有标记由于所述用户认证而能够被分配给所述用户的请求。 如果所述唯一用户标识符等于一组唯一用户标识符的一个用户标识符，则存储所述请求的副本，其中，将所述唯一用户标识符用作密钥。 所述服务发送与所述请求有关的响应，如果所述响应涉及的请求的唯一用户标识符被包括在这组唯一用户标识符中，则存储其副本。



1. 一种侦听客户端(102)和服务(124)之间的通信的方法，所述方法包括：

执行所述客户端(102)的用户(104)的用户认证；

在所述服务(124)处从所述客户端(102)的所述用户(104)接收请求(116)，所述请求(116)包括用户特有标记(118)，所述用户特有标记(118)包括唯一的用户标识符(126)，所述用户特有标记(118)由于所述用户认证而能够被分配给所述用户的所述请求(116)；

如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述请求(116)的副本。

2. 如权利要求 1 所述的方法，所述方法还包括：

从所述服务(124)向所述客户端(102)发送响应(128)，所述响应(128)与包括所述用户特有标记(118)的所述请求(116)有关，其中所述用户特有标记(118)包括所述唯一用户标识符(126)；

如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符，则使用所述唯一用户标识符(126)作为密钥来存储所述响应(128)的副本。

3. 如权利要求 1 或 2 所述的方法，其中，由认证组件(108)来执行所述用户认证，其中，所述认证组件(108)将所述用户特有标记(118)添加到所述请求(116)中，其中，侦听器插件(112)将所述唯一用户标识符(126)与所述一组唯一用户标识符(122)进行比较，其中，所述侦听器插件(112)被插入代理服务器(110)，所述代理服务器(110)位于所述服务(124)和所述客户端(102)之间，其中，所述侦听器插件(112)包括侦听控制列表(120)，所述侦听控制列表(120)包含所述一组唯一用户标识符(122)，其中，所述侦听器插件(112)链接到侦听管理器(114)，其中，所述请求(116)和所述响应(128)被存储在所述侦听管理器(114)上。

4. 如权利要求 3 所述的方法，其中，所述请求(116)和所述响应(128)被存储在消息队列(402)上，其中，所述消息队列(402)被包括在所述侦听器插件中，或者其中，所述请求(116)和所述响应(128)被存储在所述侦听器插件(112、332)上，由此，所述请求(116)和所述响应(128)通过加密的端到端通信(338)而

被所述消息队列(402)或者从所述侦听器插件(112、332)传递到所述侦听管理器(114、334)。

5. 如权利要求 3 或 4 所述的方法，其中，将所述侦听控制列表(120)永久存储在所述侦听管理器(114、506)上，并且其中，所述方法还包括:

在所述代理服务器(502)的启动之后，将所述侦听器插件(504)加载到所述代理服务器(502)中;

在所述代理服务器(502)的所述启动之后，将所述侦听控制列表从所述侦听管理器(506)加载到所述侦听器插件(504)中。

6. 如权利要求 3、4 或 5 所述的方法，所述方法包括:

利用更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表;

将所述更新的侦听控制列表加载到所述侦听插件中。

7. 如权利要求 2 至 6 中的任一项所述的方法，其中，从所述服务(124)或从所述代理服务器(110)的高速缓冲存储器接收所述响应(128)。

8. 如权利要求 1 至 7 中的任一项所述的方法，其中，以加密的方式将所述请求(116)和所述响应(128)与对应的唯一用户标识符(126)一起存储。

9. 如权利要求 3 至 8 中的任一项所述的方法，其中，在所述侦听插件(332)和所述侦听管理器(334)之间的所述连接(338)是加密的端到端通信。

10. 如权利要求 3 至 9 中的任一项所述的方法，其中，所述认证组件(314)、所述代理服务器(316)、所述侦听器插件(332)、所述侦听管理器(334)以及所述服务(306)是网络宿主环境的组件或服务提供商基础设施(302)的组件。

11. 如权利要求 3 至 10 中的任一项所述的方法，其中，所述侦听管理器和所述侦听器插件采用加密方法来存储所述侦听控制列表。

12. 如权利要求 3 至 11 中的任一项所述的方法，其中，所述侦听管理器(334)通过安全线路(342)链接到执法机构的网络，其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务提供商的所选择的职员访问所述侦听控制列表。

13. 一种计算机程序产品，包括用于执行根据前述权利要求中的任一项的方法的计算机可执行指令。

14. 一种侦听客户端(102)和服务(124)之间的通信的数据处理系统，所述

数据处理系统包括:

用于执行所述客户端(102)的用户(104)的用户认证的部件;

用于在所述服务(124)处从所述客户端(102)的所述用户(104)接收请求(116)的部件,所述请求(116)包括用户特有标记(118),所述用户特有标记(118)包括唯一的用户标识符(126),所述用户特有标记(118)由于所述用户认证而能够被分配给所述用户的所述请求(116);

用于如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符,则使用所述唯一用户标识符(126)作为密钥来存储所述请求(116)的副本的部件。

15. 如权利要求 14 所述的数据处理系统,所述数据处理系统还包括:

用于从所述服务(124)向所述客户端(102)发送响应(128)的部件,所述响应(128)与包括所述用户特有标记(118)的所述请求(116)有关,所述用户特有标记(118)包括所述唯一用户标识符(126);

用于如果所述唯一用户标识符(126)等于一组唯一用户标识符(122)的一个用户标识符,则使用所述唯一用户标识符(126)作为密钥来存储所述响应(128)的副本的部件。

16. 如权利要求 14 或 15 所述的数据处理系统,其中,由认证组件(108)来执行所述用户认证,其中,所述认证组件(108)将所述用户特有标记(118)添加到所述请求(116)中,其中,侦听器插件(112)将所述唯一用户标识符(126)与所述一组唯一用户标识符(122)进行比较,其中,所述侦听器插件(112)被插入代理服务器(110),所述代理服务器(110)位于所述服务(124)和所述客户端系统(102)之间,其中,所述侦听器插件(112)包括侦听控制列表(120),所述侦听控制列表(120)包含所述一组唯一用户标识符(122),其中,所述侦听器插件(112)链接到侦听管理器(114),其中,所述请求(116)和所述响应(128)被存储在所述侦听管理器(114)上。

17. 如权利要求 16 所述的数据处理系统,其中,所述请求(116)和所述响应(128)被存储在消息队列(402)上,其中,所述消息队列(402)被包括在所述侦听器插件(112、332)中,或者其中,所述请求(116)和所述响应(128)被存储在所述侦听管理器(114、334)上,由此,将所述请求(116)和所述响应(128)通过加密的端到端通信(338)而从所述消息队列(402)传递到所述侦听管理器(114、334)。

18. 如权利要求 16 或 17 所述的数据处理系统，其中，所述侦听管理器(114、506)包括用于存储所述侦听控制列表(120)的部件，并且其中，所述数据处理系统还包括:

用于在所述代理服务器(502)的启动之后将所述侦听器插件(504)加载到所述代理服务器(502)中的部件;

用于在所述代理服务器(502)的所述启动之后将所述侦听控制列表(120)从所述侦听管理器(506)加载到所述侦听器插件(504)中的部件。

19. 如权利要求 16 至 18 中的任一项所述的数据处理系统，所述数据处理系统包括:

用于通过更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表的部件;

用于将所述更新的侦听控制列表加载到所述侦听插件中的部件。

20. 如权利要求 16 至 19 中的任一项所述的数据处理系统，其中，所述侦听管理器包括用于建立到执法机构的网络的安全网络连接的部件，并且其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务提供商的所选择的职员访问所述侦听控制列表。

用于侦听客户端和服务之间的通信的方法和数据处理系统

技术领域

本发明一般地涉及一种用于侦听客户端和服务之间的通信的方法和数据处理系统，并且具体涉及一种用于侦听客户端和服务之间的嫌疑人的通信的方法和数据处理系统。

背景技术

在大多数国家中，法律强制通信或服务提供商使得能够为象特务机关、刑事调查部门以及国家和国际犯罪打击和犯罪防范组织的执法机构侦听顾客的通信。因此，电信服务提供商必须提供电信和IT基础设施，以便使执法部门能够侦听语音和数据流量。基本上，必须确保以下主要原则：

1. 该侦听对于其通信被侦听的人来说必须是不可见的和不可识别的。
2. 该侦听对于服务提供商的职员来说必须是不可见的和不可识别的。
3. 仅仅允许侦听合法确定的嫌疑人的通信。

然而，传统的语音通信基于电路交换网络技术，并且在接入点处，侦听相当容易实现，基于分组交换技术的IP数据流量暴露了关于上述原则的障碍。通常使用的用于侦听数据流量的方法是在特定的侦听点记录若干用户会话的所有IP流量，随后进行过滤器分析，以便重新产生完整的用户会话。三个原因主要地说明这一实践的低效：需要存储、管理和分析巨量数据。此外，记录数据流量不一定记录到所有通信数据，因为分组交换网络可以使用不可预测的路由和节点。侦听不是实时的，并且可能影响法律问题，原因是存储比所需的更多的用户数据。

因此，在互连交换机中，诸如公共交换电话网和公共陆地移动网络的电话网络中进行侦听。所述交换机被互连到与执法机构相连接的传达设备。交换机使用电话号码(ISDN/MSISDN)作为侦听依据。在交换机处侦听对于某个电话号码的呼入或呼出通话。该交换机复制通信内容。除了呼叫者和被叫者之间的传输之外，经由传达设备将数据传递给执法机构。

在基于 TCP/IP 的网络中，侦听与电话网络非常相似。交换机与连接到执法机构的传达设备相连接。使用 IP 地址的源地址字段、IP 地址的目的地地址字段或者二者取代电话号码作为侦听依据。通常的实践是记录来自或去往给定 IP 地址的所有连接数据(但不一定是全部内容)。存在若干种类型的信息源，从该信息源中，例如从 IP 路由器日志文件、从 HTTP 服务器日志文件、从网络协议分析器或从动态流量过滤，可以提取通信数据记录。

已经知道一些专利，其描述用于合法侦听分组无线网络的侦听方法和系统。那些仅适用于网络运营商，原因是他们需要与其核心网络的交换基础设施进行深入交互。最接近的 5 个专利列出如下:

美国专利申请 US220/0049913A1 和 US220/0051457A1——侦听系统和方法——涉及一种用于在诸如通用分组无线服务(GPRS)或通用移动通信系统(UMTS)的分组网络中进行合法侦听的侦听系统和方法。

名称为侦听方法和系统的美国专利申请 US2002/0078384A1 涉及一种侦听方法和系统，用于在诸如通用分组无线服务(GPRS)或通用移动通信系统(UMTS)的分组网络中进行合法侦听的侦听系统和方法。

美国专利申请 US2002/0068582A1——用于向执法机构报告信息的方法、系统和传达设备——涉及蜂窝对电信网络用户通信的监控，并且特别涉及一种用于向执法机构报告所监控的信息的方法、系统和传达设备。

在名称为——用于使用基于实时内容的网络监控来检测和报告在线活动的系统和方法的美国专利申请 2002/0128925 中描述了关于监控的更普通的方法。其一般地涉及通过诸如因特网、万维网或公司局域网(LAN)的公共或专用网络报告在线活动的系统。该专利仅适用于基于 URL 的过滤，并且不进行整个用户会话。它明确排除了对诸如图像的特定内容类型的侦听，因此不适用于合法侦听。

基于 IP 的侦听使用定义的 IP 地址来侦听来自或去往特定 IP 地址的通信。然而，如果用户不具有诸如由例如因特网接入提供商的第三方提供的动态分配的 IP 地址的公知/固定 IP 地址，则基于 IP 地址的侦听并不够。要利用这样的 IP 地址侦听的用户建立的应用程序会话将不会被记录到。基于 IP 的侦听可以记录特定应用程序或整个基础设施的所有通信。然而，对于大量应用程序/网站来说，将记录的数据量是巨大的。这些数据的管理和处理需要大量的努力和例如以大量数据存储设备形式的资源。由于在此情况中将侦听所有应

用程序会话，因此隐私问题确实存在，并且法律方面确实适用。为了从所记录的数据中获得所感兴趣的应用程序会话的内容，必须进行过滤。由于这涉及大量数据，因此所述过滤是耗时和耗费资源的。

此外，可以使用传输层安全协议(TLS)或安全套接字层(SSL)来加密通过IP地址侦听所记录的数据。对诸如HTTP网络服务器日志或应用程序日志的标准应用程序和基础设施日志的分析不包含通信的全部内容。为了获得全部应用程序会话内容，需要修改应用程序以实现所需的日志记录。

因此，确实存在对于用于侦听数据流量的改进的方法和数据处理系统的需要。

发明内容

根据本发明的实施例，提供了一种侦听客户端和服务之间的通信的方法，其中，该方法包括执行所述客户端的用户的用户认证的步骤，以及由所述服务从所述客户端的用户接收请求的步骤。所述请求包括用户特有标记(token)，并且该用户特有标记包括唯一的用户标识符。由于所述用户认证，可以将该用户特有标识符分配给用户的请求。如果该唯一用户标识符与一组唯一用户标识符中的一个用户标识符相等，则存储该请求的副本，其中，将该唯一用户标识符用作密钥。

将用户特有标记添加到从客户端发送给服务的所有请求。用户特有标记包括唯一的用户标识符。通过使用该用户特有标记，可以识别该用户。检查所述唯一的用户标识符是否等于包括在一组唯一用户标识符中的一个用户标识符。如果是这种情况，则记录请求的副本，从而将用户标识符用作密钥以便识别该用户。因此，通过将包括在标记中的用户标识符和一组唯一用户标识符进行比较来窃听客户端和服务之间的通信。在这组唯一用户标识符中，包含可疑的并且将被窃听的所有用户的用户标识符。

根据本发明的实施例，所述方法还包括将来自服务的响应发送给客户端的步骤，其中，所述响应与包括用户特有标记的请求有关，所述用户特有标记包括唯一的用户标识符。如果该唯一用户标识符等于一组唯一用户标识符中的一个用户标识符，则在所述方法的另一步骤中，将所述响应的副本与作为密钥的唯一用户标识符一起存储。

因此，不仅仅侦听从客户端发送到服务的请求。从服务发送给客户端的

响应也被侦听。如果响应与包括标记的请求有关、其中所述标记具有也包括在该组唯一用户标识符中的唯一用户标识符，则存储该响应的副本。

当仅仅对于在该组唯一用户标识符中存储了其用户标识符的用户的请求和响应进行侦听时，所述方法尤其有利。所有其它用户不受根据本发明的方法影响。因此，根据本发明的方法满足仅仅允许侦听合法确定的人的通信的法律要求。此外，被侦听的人不会觉察到他或她已经被侦听。

根据本发明的实施例，通过认证组件来执行用户认证，其中，认证组件将用户特有标记添加到所述请求中，其中，侦听器插件将唯一的用户标识符与一组唯一用户标识符进行比较，其中，该侦听器插件被插入代理服务器，其中，该代理服务器位于服务和客户端之间，其中，侦听器插件包括侦听控制列表，其中，侦听控制列表包含该组唯一用户标识符，其中，侦听器插件连接到侦听管理器，其中，将所述请求和响应存储在侦听管理器上。

典型为服务提供商的基础设施的第一组件并且从客户端接收消息的认证组件对用户进行认证，并且将用户特有标记添加到所述请求中。如上所述，用户特有标记包括唯一的用户标识符。所述请求还被传递给位于服务和客户端之间的代理服务器。侦听器插件被插入包括侦听控制列表的代理服务器。侦听控制列表保存该组唯一用户标识符。针对该组唯一用户标识符检查被包括在消息的标记中的用户标识符。如果唯一用户标识符被包括在该组唯一用户标识符中，则将响应副本存储在侦听管理器上。因为可以简单地将侦听器插件插入代理服务器，所以使用侦听器插件识别是否从应该被侦听的用户发送请求特别有利。然而，这要求服务提供商的基础设施包括代理服务器。还有可能在另一组件中使用侦听器插件。例如，可以将侦听器插件集成到认证组件中，此外，使用容留该侦听器插件的分离组件也是可行的。然后，将把这一组件布置在认证组件和服务之间。

根据本发明的实施例，将所述请求和响应存储在消息队列中，其中，在侦听器插件中比较该消息队列，或者其中，将所述请求和响应存储在侦听器插件中，由此通过加密的端到端通信将所述请求和响应从消息队列或从侦听器插件传递到侦听管理器。

根据本发明的实施例，将侦听控制列表永久存储在侦听管理器上，并且在代理服务器启动之后将侦听器插件加载到代理服务器中，并且在该代理服务器启动之后，将侦听控制列表从侦听管理器加载到侦听器插件中。

根据本发明的实施例，利用被加载到侦听器插件中的更新的侦听控制列表来更新侦听控制列表，从而刷新所存储的侦听控制列表。

根据本发明的实施例，从服务或从代理服务器的高速缓冲存储器接收所述响应。

根据本发明的实施例，以加密的方式将所述请求和响应与对应的唯一用户标识符一起存储。这确保了将不会向未被授权访问被侦听的响应和请求的任何人授予访问权。

根据本发明的实施例，侦听器插件和侦听管理器之间的连接是加密的端到端通信。当将被侦听的响应和请求从侦听插件传递到侦听管理器时，这阻止未被授权访问被侦听的请求和响应的任何人。

根据本发明的实施例，认证组件、代理服务器、侦听器插件、侦听管理器和服务本身是网络宿主环境的组件或服务提供商的基础设施的组件。例如但不唯一的是，所述服务与提供服务的服务器或者设备盒有关。

根据本发明的实施例，侦听管理器和侦听器插件采用加密方法来存储侦听控制列表。以加密的方式存储被侦听的请求和响应以及侦听控制列表的优点在于防止未被授权访问这些敏感数据中的任一个的任何人这么做。当法律要求未被授权的任何人都不能访问这些敏感数据中的任一个时，这特别有利。因此，根据本发明的方法满足法律所要求的必要条件。

根据本发明的实施例，侦听管理器通过安全线路连接到执法机构的网络，其中，仅仅执法机构的职员被特许访问存储在侦听管理器上的侦听控制列表以及被侦听的响应和请求，并且其中，仅仅准许服务提供商的被选中的职员访问侦听控制列表。

在另一方面，本发明涉及一种计算机程序产品，其包括用于执行根据本发明的方法的计算机可执行指令。

在另一方面，本发明涉及一种侦听客户端和服务之间的通信的数据处理系统，其中，所述数据处理系统包括用于执行客户端的用户的用户认证的部件和用于在服务处从客户端的用户接收请求的部件，其中，所述请求包括用户特有标记，其中该用户特有标记包括唯一的用户标识符，其中，由于所述用户认证，可以将该用户特有标记分配给该用户。该数据处理系统还包括用于如果所述唯一的用户标识符与一组唯一用户标识符中的一个用户标识符相等则使用所述唯一的用户标识符作为密钥来存储所述请求和相关响应的副

本。

附图说明

下面，将仅仅参考附图、作为示例来更详细地描述本发明的优选实施例，在附图中：

图 1 示出了连接到被适配为侦听通信的服务提供商的基础设施的客户端系统的方框图，

图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图，

图 3 在方框图中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端和服务之间的数据流量，

图 4 示出了侦听设施的可扩充(scalable)设置的方框图，

图 5 是示出在侦听器插件启动期间由各个组件处理的步骤的顺序图，

图 6 是图示当侦听通信时各个组件的交互的顺序图，以及

图 7 示出了图示当更新侦听控制列表时执行的步骤的顺序图。

具体实施方式

图 1 示出了连接到被适配为侦听通信的服务提供商 106 的基础设施的客户端系统 102 的方框图 100。服务提供商基础设施 106 包括认证组件 108、代理服务器 110、侦听管理器 114 和服务 124。用户 104 登录到客户端系统 102 中。客户端系统 102 例如是诸如 PC、移动电话或 PDA 的、运行浏览器应用程序的设备，其连接到服务提供商基础设施 106。服务提供商知晓用户 104，因此服务提供商准许用户 104 访问服务提供商基础设施 106。

认证组件 108 从客户端 102 接收请求 116。在那里，将带有用户标识符 126 的标记 118 添加到请求 116 中。可以通过用户标识符 126 来识别用户 104。请求 116 被发送给服务 124。代理服务器 110 位于认证组件 108 和服务 124 之间，使得请求 116 在它到达服务 124 之间通过代理服务器 110。代理服务器 110 包括侦听器插件 112。在此示例中，侦听器插件 112 是被插入代理服务器 110 中的插件。侦听器插件 112 保存列出一组用户标识符 122 的侦听控制列表(ICL)120。侦听器插件 112 从请求 116 读取用户标识符 126。如果用户标识符 126 被包括在侦听控制列表 120 中，则将请求 116 的副本与用户标识符 126 一起发送到侦听管理器 114，在那里，将请求 116 的副本与用户标识符 126

一起存储。

服务 124 接收请求 116。服务 124 将响应 128 发送回客户端。当响应 128 通过代理服务器 110 时，侦听器插件 112 检查该响应是否与被侦听的请求有关。如果是这样，则将响应 128 的副本与用户标识符 126 一起存储在侦听管理器 114 中。响应 128 被进一步发送给客户端系统 102，使得用户最终接收到根据其请求 116 的响应 128。由此，用户不知道他可能已被侦听。

图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图 200。在步骤 202 中，执行客户端系统的用户的用户认证。在步骤 204 中，在侦听器插件处从客户端的用户接收请求，其中，该请求包括含有唯一用户标识符的用户特定标记，其中，由于所述用户认证，可以将用户特有标记分配给该用户的请求。在步骤 206 中，检查该唯一用户标识符是否被包括在一组唯一用户标识符中。如果是这种情况，则根据本发明的方法继续进行步骤 208，其中，存储所述请求的副本。否则，根据本发明的方法继续进行步骤 210，其中，不进一步考虑动作。在步骤 208 或 210 的处理之后，在步骤 212 中，将所述请求传递到所述服务，在那里它被处理。

图 3 在方框图 300 中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端 312 和服务提供商基础设施 302 之间的数据流量。概念服务提供商基础设施是非常笼统的术语，并且它应当被理解为：在此文档的语境中，它指的是在最广泛的意义上向用户提供通信服务的服务提供商的基础设施。如先前所述，服务提供商只需要通过使用认证组件来识别该用户的方式。下面，将专注于与通信服务提供商所提供的基础设施不同的服务提供商的基础设施。通常，通信服务提供商通过使用分配给客户端的动态 IP 地址来授权用户的访问，并且允许到 IP 网络的通信。另一方面，服务提供商具有固定 IP 地址以及被用来获得服务的公知域名，所述服务例如可以是在线银行服务或者在更广的意义上为相同 IP 网络上的网络服务。

客户端 312 可以是具有浏览器应用程序的设备，所述设备经由网络 310 连接到也被称为服务提供商所在地(premise)的服务提供商基础设施 302。客户端 312 也可以是使用包括语音浏览器(例如 VoiceXML 浏览器)的交互式语音响应(IVR)系统的电话，其中，通过服务提供商基础设施 302 通过网络 310 向其提供服务。语音浏览器应用网络技术，以便使用户能够经由言语和双音多频(DTMF)的组合而从电话访问服务。

网络 310 可以是由通信服务提供商提供的所有类型访问信道的代表实体。如上所述，服务提供商和通信服务提供商通常不是相同的。这意味着服务提供商不知道除了客户端的 IP 地址以外的用户细节。服务提供商不能在没有通信服务提供商的帮助的情况下识别或认证用户。由于这一事实，诸如在线银行的由服务提供商所提供的大多数网络应用要求用户在访问所述服务时认证他们自己。

服务提供商基础设施302通常由3个组件组成，它们是HTTP服务器304、应用程序服务器 306 和目录服务 308。此外，服务提供商基础设施通常包括所谓的边缘组件 313，其包括认证组件 314 和代理服务器 316。

客户端 312 经由连接 318 和 320，通过网络 310 而连接到服务提供商基础设施 302。在认证组件 314 处接收来自客户端 312 的请求。认证组件 314 经由连接 330，针对目录服务 308 验证证书。认证组件 314 仅仅将可被证实的请求经由连接 322、324 和 326 转发到代理服务器 316、HTTP 服务器 304 或应用程序服务器 306。

认证组件 314 还将用户特有标记添加到请求中。该用户特有标记包括可用以唯一地识别用户的唯一的用户标识符。

将所述请求继续传递到代理服务器 316。代理服务器 316 包括侦听器插件 332，其分析所述标记，并且针对在侦听控制列表中列出的一组用户标识符来检查用户标识符。如果在侦听控制列表中列出了所述用户标识符，则将该请求的副本存储在例如侦听器插件的高速缓冲存储器中。

所述请求被进一步传递给 HTTP 服务器 304 和应用程序服务器 306，由此，将与目录服务 308 的连接 328 用于授权的目的和用户细节。从应用程序服务器 326 产生响应，所述响应随后经由 HTTP 服务器 304 和边缘组件 313 而被发送回客户端系统 312。如果以前请求过所述请求，那么也可以直接由代理服务器 316 部分或全部地产生所述请求。

代理服务器 316 的侦听器插件 332 还分析所述响应是否与带有标记的用户标识符的请求有关，其中所述用户标识符也被包括在侦听控制列表中列出的一组用户标识符中。如果在侦听控制列表中列出了所述用户标识符，则将所述响应的副本存储在例如侦听器插件的存储器中。

通常，以加密的方式将被侦听的请求和响应存储在侦听器插件的存储器中，使得服务提供商的未被授权的服务职员不能访问所述请求和响应。此外，

出于相同的原因，以加密的方式存储该侦听控制列表。

侦听管理器 334 经由连接 338 连接到代理服务器 316，并且可以直接与侦听器插件 332 通信。可以使用连接 338 来在侦听器插件 332 和侦听管理器 334 之间建立加密的端到端通信。例如，可以周期性地建立连接 338，然后，可以将存储在侦听器插件 332 的存储器中的请求和响应从侦听器插件 332 传递到侦听管理器 334。

或者，可以永久地建立连接 338，并且可以将被侦听的响应和请求从侦听器插件 332 直接传送到侦听管理器 334，在侦听管理器 334 中，它们将以加密的方式而被永久存储。侦听控制列表也以加密的方式被存储在那里。

此外，在侦听器插件和侦听管理器组件之间可以使用消息队列，以便提高可用性和适用性。在这么做的时候，实现了侦听器插件 332 和侦听管理器 334 之间的有保证的传送，并且在服务中断的情况下避免了数据丢失。

侦听管理器 334 经由连接 342 与网络 340 通信。连接 342 最好也是永久或临时建立的加密的端到端连接。网络 340 由执法机构控制。可以将被侦听地响应和请求从侦听管理器传递到网络 340，以便由执法机构的授权职员作进一步分析。

如之前已经提到的那样，将用户特有标记添加到从客户端接收的所有请求中，在该客户端上该用户特定标记所涉及的用户访问服务提供商所在地。利用被包括在该侦听控制列表中的用户标识符来检查该用户特有标记。服务提供商知道该用户标识符。因此，执法机构必须向帮助建立侦听控制列表的服务提供商的职员中的几个人授权，因为这些人必须提供用户特有标识符。

图 4 示出了侦听设施的可扩充设置的方框图 400。该设置基本上与如图 3 所述的相同，并且根据本发明的用于侦听用户请求和响应的方法也是相同的。将水平扩充(scaling)技术应用于认证组件 314、代理服务器 316 和对应的侦听器插件 332。消息队列 402 被置于侦听器插件 332 和侦听管理器 334 之间。在侦听器插件 332 和侦听管理器组件 334 之间使用消息队列 402，以便如上所述提高可用性和适用性。

图 5 是示出在侦听器插件 504 启动期间由各个组件(即代理服务器 502、侦听器插件 504 和侦听管理器 506)处理的步骤的顺序图 500。在步骤 508 中，启动代理服务器 502。侦听器插件 504 被加载到代理服务器中。它被插入代理服务器 502。在步骤 510 中，侦听器插件将它自己初始化。它从侦听管理

器 506 请求侦听控制列表，所述侦听控制列表被加载到侦听器插件 504 的存储器中。侦听器插件 504 将“准备工作”信号发送回代理服务器 502。在步骤 512 中，完成代理服务器 502 的启动，并且该代理服务器将其状态设置为“准备工作”。

图 6 是图示当侦听嫌疑用户的通信时各个组件(即客户端系统 602、认证组件 604、代理服务器 606、服务 608、侦听器插件 610、侦听管理器 612 和执法机构(LEA)614)的交互的顺序图 600。

在步骤 630 中，客户端 602 将请求发送给认证组件 604。认证组件 604 在步骤 616 中对用户进行认证，将带有用户标识符的用户特有标记添加到该请求中，并且在步骤 632 中将该请求发送给代理服务器 606。在步骤 634 中，调用侦听器插件 610。针对侦听控制列表检查用户标识符，并且如果它被保存在侦听控制列表中，则在步骤 618 中侦听该请求。在步骤 636 中，将该请求的副本发送到侦听器管理器 612，所述侦听器管理器 612 在步骤 620 中存储该请求。在步骤 638 中，它被进一步发送给执法机构 614，或者更准确地说，它被进一步发送给该机构的网络。在步骤 640 中，代理服务器 606 还将所述请求转发给服务 608，在那里，在步骤 622 中，执行该服务自身。在步骤 642 中，将与所述请求有关的响应发送回代理服务器 606。该代理服务器在步骤 644 中调用侦听器插件。在步骤 624 中，如果所述响应与被侦听的请求有关，那么它也被侦听。所述响应的副本被发送给侦听管理器 612，在那里，在步骤 628 中将其存储。在步骤 648 中，它被进一步发送给执法机构 614。代理服务器 606 还在步骤 650 中将所述响应转发到认证组件 604，在步骤 652 中，将所述响应发送给客户端。用户在不知道他可能已经被侦听的情况下接收到该响应。

图 7 示出了图示被执行以便更新侦听控制列表(ICL)的步骤的顺序图 700。在步骤 710 中，授权的管理员 702 维护和更新存储在侦听管理器 704 上的侦听控制列表(ICL)。在步骤 712 中，分发更新的侦听控制列表。在步骤 718 中将该侦听控制列表发送到侦听器插件 706。在步骤 714 中，更新的侦听控制列表刷新所存储的侦听控制列表。在步骤 720 中，将向侦听管理器 704 通知已经成功地进行了该更新的消息从侦听器插件 706 发送到侦听管理器 704。在步骤 716 中，将更新信息发送给执法机构(LEA)708。在步骤 722 中，向 LEA 708 通知允许对侦听控制列表(ICL)的改变。

参考标号列表

100	方框图
102	客户端系统
104	用户
106	服务提供商基础设施
108	认证组件
110	代理服务器
112	侦听器插件
114	侦听管理器
116	请求
118	标记
120	侦听控制列表
122	一组用户标识符
124	服务
126	用户标识符
128	响应
200	流程图
202	用户认证
204	在侦听器插件处接收用户的请求
206	检查是否设置了标记
208	存储请求的副本
210	无动作
212	处理服务
300	方框图
302	服务提供商基础设施
304	HTTP 服务器
306	应用程序服务器
308	目录服务
310	网络
312	客户端

313	边缘组件
314	认证组件
316	代理服务器
318	连接
320	连接
322	连接
324	连接
326	连接
328	连接
330	连接
332	侦听器插件
334	侦听管理器
336	连接
338	连接
340	网络
342	连接
400	方框图
402	消息队列
500	顺序图
502	代理服务器
504	侦听器插件
506	侦听管理器
600	顺序图
602	客户端系统
604	认证组件
606	代理服务器
608	服务
610	侦听器插件
612	侦听管理器
614	执法机构

700	顺序图
702	管理员
704	侦听管理器
706	侦听器插件
708	执法机构

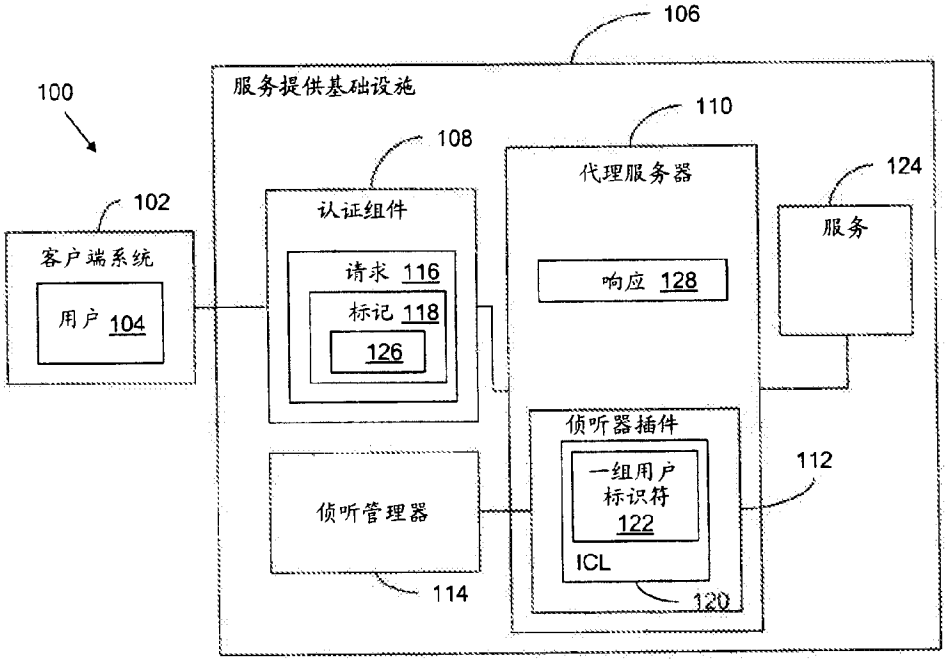


图 1

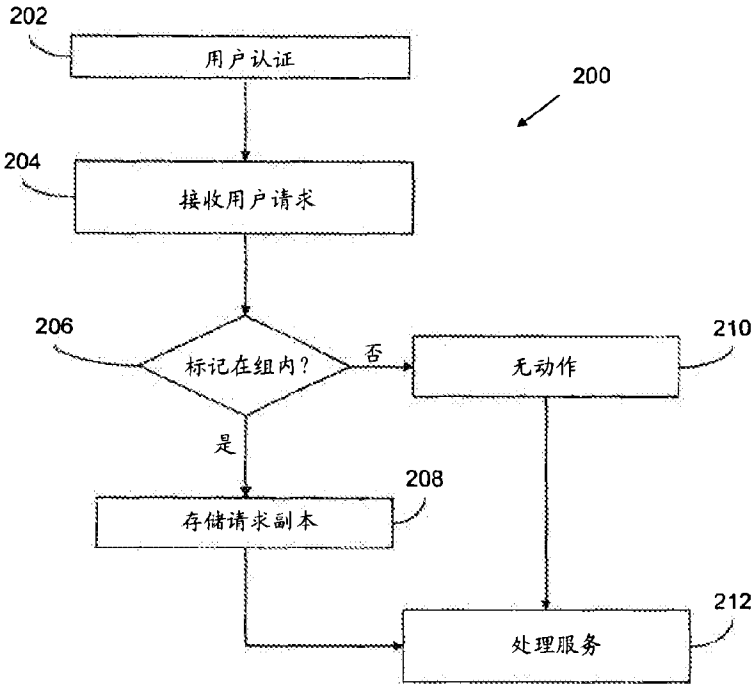


图 2

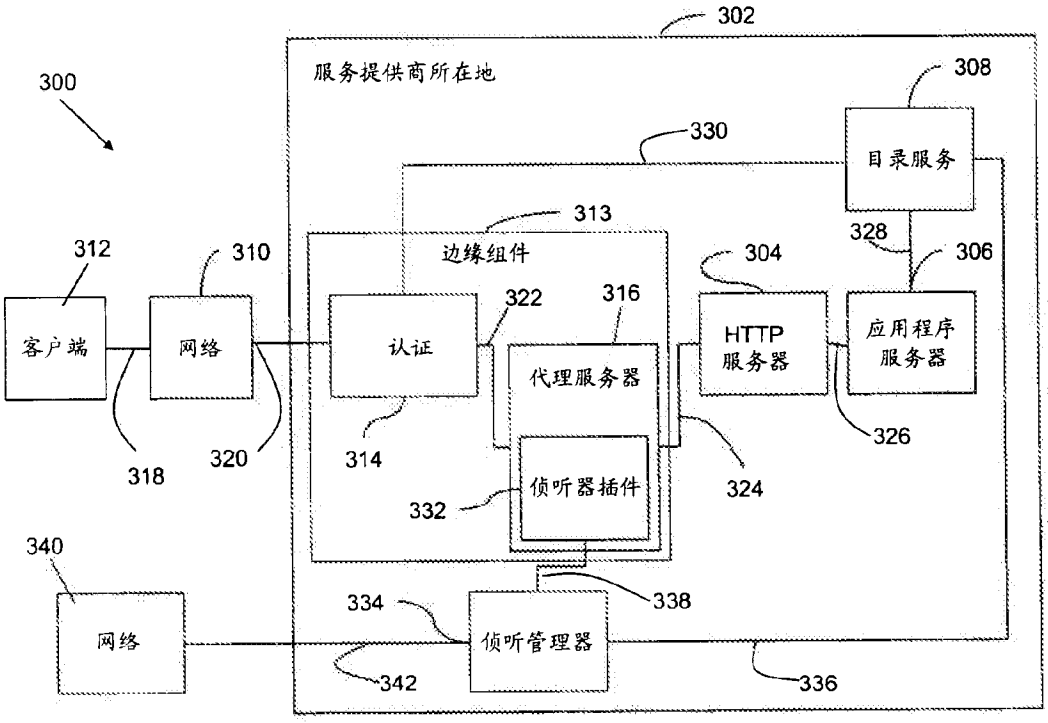


图 3

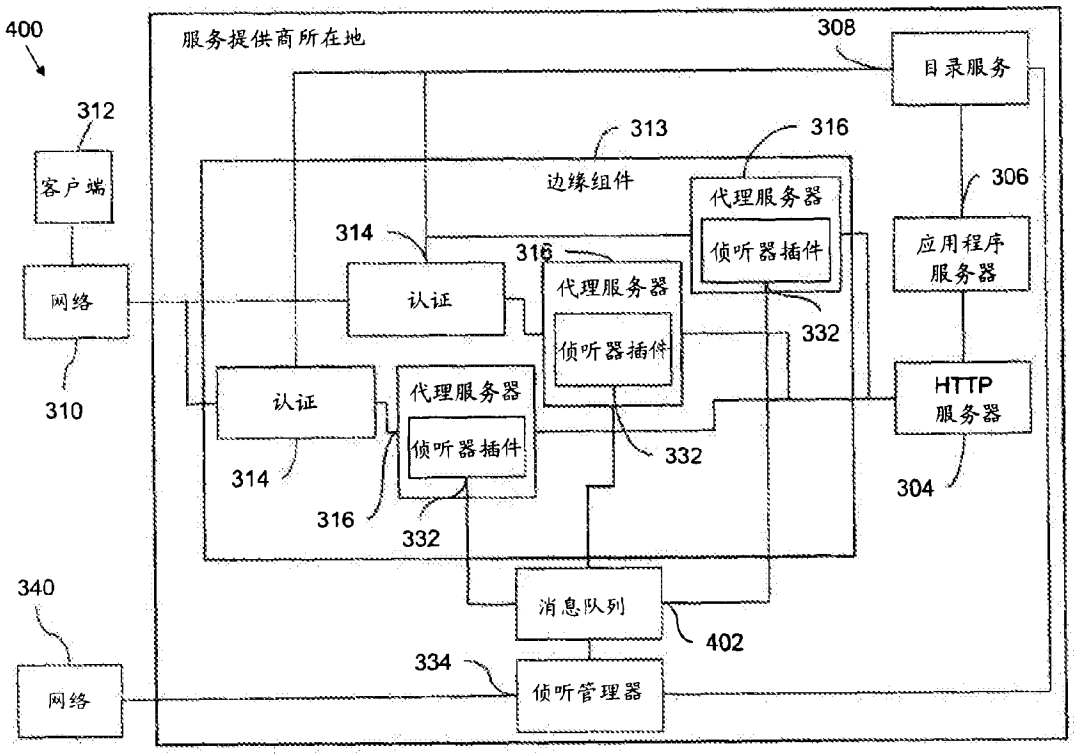


图 4

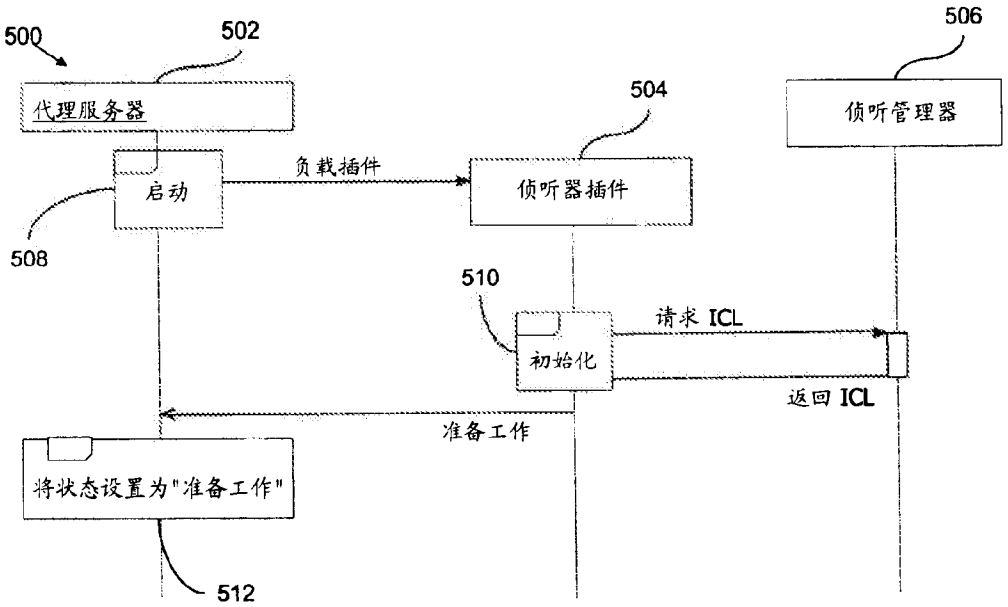


图 5

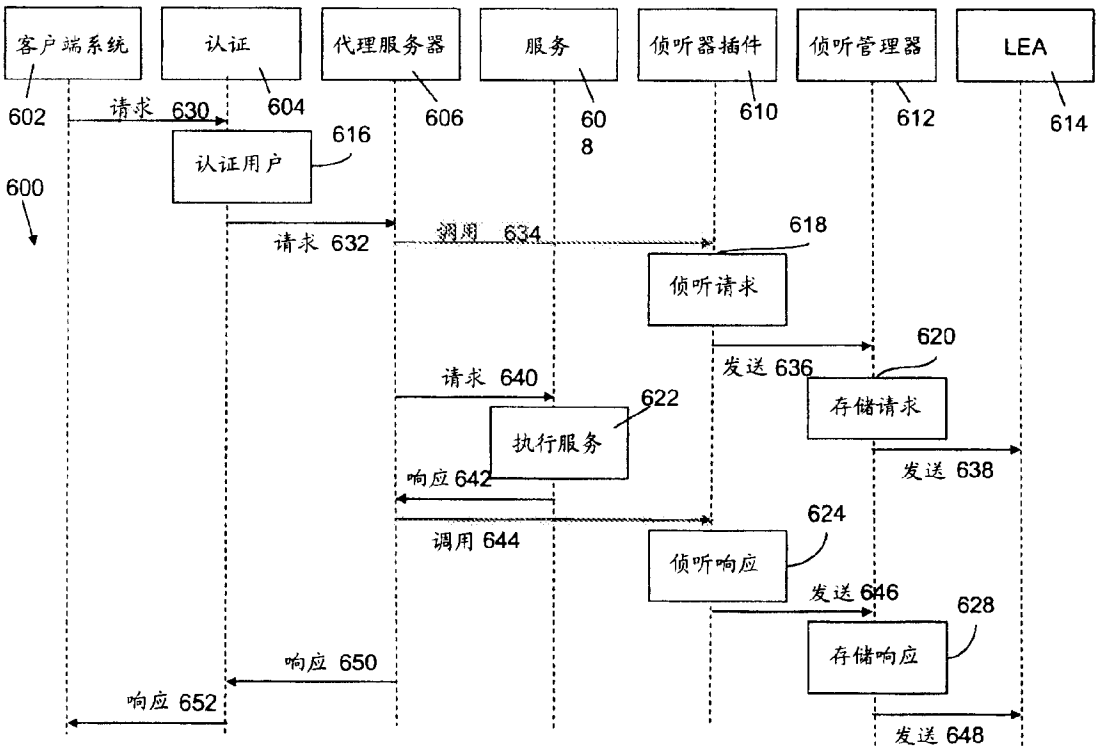


图 6

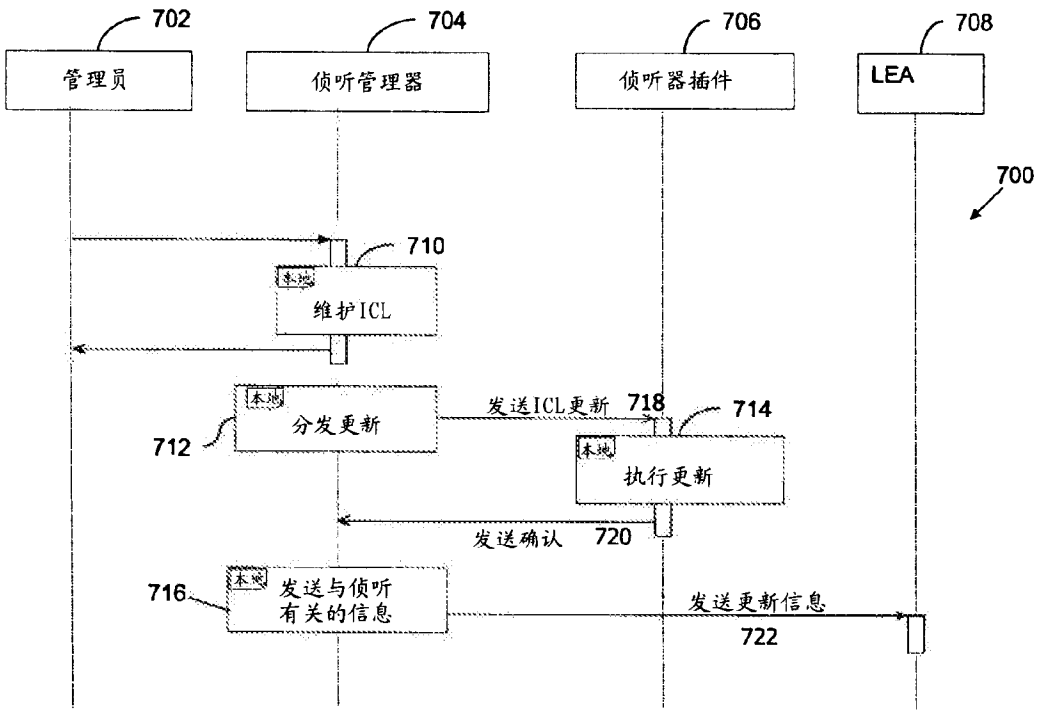


图 7

Espacenet

Bibliographic data: CN101069390 (A) — 2007-11-07

Method for the routing of communications to a voice over internet protocol terminal in a mobile communication system

Inventor(s): JUHA KALLIO [FI] + (KALLIO JUHA)

Applicant(s): NOKIA CORP [FI] + (NOKIA CORP)

Classification: - international: ***H04L12/28; H04L12/56; H04W76/02;*** *H04W8/26;* ***H04L***
- cooperative: **H04W76/021**; **H04W8/10**; H04W8/26

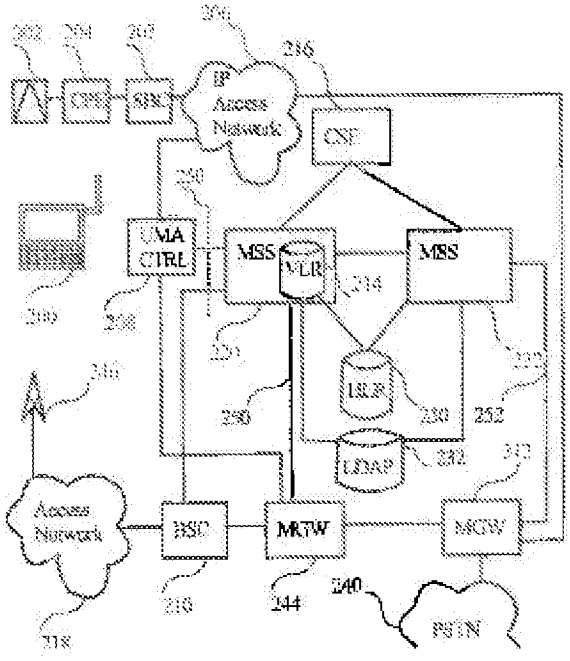
Application number: CN2005841159 20051220

Priority number (s): FI20040001659 20041223 ; WO2005FI00540 20051220

Also published as: CN101069390 (B) WO2006067269 (A1) US2006142011 (A1) US7400881 (B2) KR20070097526 (A) KR100886165 (B1) EP1829300 (A1) EP1829300 (A4) EP1829300 (B1) less

Abstract of CN101069390 (A)

The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile



PETITIONER APPLE INC. EX. 1004-367

station. The call control node translates the called party number to the logical name using the directory.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/56 (2006.01)
H04L 12/28 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580041159.7

[43] 公开日 2007 年 11 月 7 日

[11] 公开号 CN 101069390A

[22] 申请日 2005.12.20
[21] 申请号 200580041159.7
[30] 优先权
[32] 2004.12.23 [33] FI [31] 20041659
[86] 国际申请 PCT/FI2005/000540 2005.12.20
[87] 国际公布 WO2006/067269 英 2006.6.29
[85] 进入国家阶段日期 2007.5.30
[71] 申请人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 J·卡利奥
[74] 专利代理机构 北京市金杜律师事务所
代理人 冯 谱

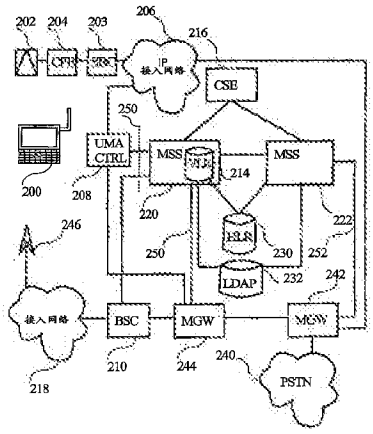
权利要求书 4 页 说明书 17 页 附图 6 页

[54] 发明名称

用于在移动通信系统中将通信路由到基于网际协议的语音终端的方法

[57] 摘要

本发明涉及一种用于在通信系统中对呼叫和消息进行路由的方法。 在该方法中移动台使用逻辑名来注册到呼叫控制节点。 逻辑名在目录中映射为国际移动订户标识。 呼叫控制节点使用国际移动订户标识来执行位置更新到归属位置寄存器。 使用被叫方号码来联系移动台。 当收到去往核心网络的终止呼叫或者消息时，为移动台分配漫游号码，而将该呼叫或者消息路由到当前服务于移动台的呼叫控制实体。 呼叫控制节点使用目录将被叫方号码转译成逻辑名。



1. 一种用于在至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的通信系统中对呼叫进行路由的方法，所述方法包括:

从移动台接收去往第一呼叫控制节点的注册消息，所述注册消息包括针对所述移动台的逻辑名;

在所述第一呼叫控制节点的请求下在目录中将所述逻辑名映射为针对所述移动台的国际移动订户标识;

在所述第一呼叫控制节点的请求下更新所述移动台的位置到归属位置寄存器，所述第一呼叫控制节点的所述请求包括所述国际移动订户标识;

在第二呼叫控制节点中接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码;

从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码;

在所述归属位置寄存器的请求下从所述第一呼叫控制节点分配漫游号码;

从所述归属位置寄存器发送至少包括所述漫游号码的查问响应消息到所述第二呼叫控制节点;

从所述第二呼叫控制节点发送所述呼叫建立请求消息到所述第一呼叫控制节点; 以及

在所述第一呼叫控制节点的第二请求下在所述目录中将所述被叫方号码映射为针对所述移动台的所述逻辑名。

2. 根据权利要求 1 所述的方法，所述方法还包括:

在所述第二呼叫控制节点中获得主叫方号码;

在所述第一呼叫控制节点中确定所述主叫方号码是否包括指示了所述主叫方号码可以转译成第二逻辑名的前缀; 以及

在所述第一呼叫控制节点的第三请求下在所述目录中将所述主

叫方号码映射为针对主叫方的所述第二逻辑名。

3. 根据权利要求 1 所述的方法，所述方法还包括:

在所述移动台确定无线局域网的可用性;

建立从所述移动台到连接至所述无线局域网的接入路由器的连接; 以及

经由所述接入路由器获得所述第一呼叫控制节点的标识。

4. 根据权利要求 1 所述的方法，其中所述通信系统包括无线局域网。

5. 根据权利要求 1 所述的方法，其中所述移动通信系统包括全球移动通信系统网络和通用移动电话系统网络中的至少一个。

6. 根据权利要求 5 所述的方法，其中所述第一呼叫控制节点和所述第二呼叫控制节点是移动服务交换中心服务器。

7. 根据权利要求 1 所述的方法，其中所述移动台包括会话发起协议用户代理。

8. 根据权利要求 7 所述的方法，其中所述注册消息是会话发起协议注册消息。

9. 根据权利要求 1 所述的方法，其中所述呼叫建立请求消息是 ISDN 用户部分呼叫建立请求消息。

10. 根据权利要求 1 所述的方法，其中所述目录是轻型目录访问协议目录。

11. 一种至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的系统，所述系统还包括:

在所述第一呼叫控制节点中的移动性实体，配置用以: 从所述移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名; 请求从所述目录将所述逻辑名映射为针对所述移动台的国际移动订户标识; 以及通过指明所述国际移动订户标识来请求从所述归属位置寄存器更新所述移动台的位置;

在所述第二呼叫控制节点中的呼叫控制实体，配置用以: 接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码; 从

所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到所述第一呼叫控制节点；以及

在所述第一呼叫控制节点中的呼叫控制实体，配置用以请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

12，根据权利要求 11 所述的系统，其中在所述第一呼叫控制节点中的所述呼叫控制实体被配置用以：确定主叫方号码是否包括指示了所述主叫方号码可以转译成第二逻辑名的前缀；以及请求从所述目录中将所述主叫方号码映射为针对主叫方的所述第二逻辑名。

13. 根据权利要求 11 所述的系统，所述系统还包括：

在所述移动台中的通信实体，配置用以：确定无线局域网的可用性；建立从所述移动台到连接至所述无线局域网的接入路由器的连接；以及经由所述接入路由器获得所述第一呼叫控制节点的标识。

14. 根据权利要求 11 所述的系统，其中所述系统包括无线局域网。

15. 根据权利要求 11 所述的系统，其中所述系统包括全球移动通信系统网络和通用移动电话系统网络中的至少一个。

16. 根据权利要求 15 所述的系统，其中所述第一呼叫控制节点和所述第二呼叫控制节点是移动服务交换中心服务器。

17. 根据权利要求 11 所述的系统，其中所述移动台包括会话发起协议用户代理。

18. 根据权利要求 17 所述的系统，其中所述注册消息是会话发起协议注册消息。

19. 根据权利要求 11 所述的系统，其中所述呼叫建立请求消息是 ISDN 用户部分呼叫建立请求消息。

20. 根据权利要求 11 所述的系统，其中所述目录是轻型目录访问协议目录。

21. 一种呼叫控制节点，包括：

移动性实体，配置用以：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识；以及通过指明所述国际移动订户标识来请求从归属位置寄存器更新所述移动台的位置；

呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到第二呼叫控制节点；以及请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

22. 一种具体体现在计算机可读介质内的计算机程序，所述计算机程序被配置用以执行以下步骤：

从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；

请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识；

请求从归属位置寄存器更新所述移动台的位置，所述请求包括所述国际移动订户标识；

接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；

发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；

从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；

发送呼叫建立请求消息到另一呼叫控制节点；以及

请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

23. 根据权利要求 22 所述的计算机程序，其中所述计算机可读介质是可移动存储卡。

24. 根据权利要求 22 所述的计算机程序，其中所述计算机可读介质是磁盘或者光盘。

用于在移动通信系统中将通信路由到基于网际协议的语音终端的方法

技术领域

本发明涉及在移动通信系统中进行路由。具体而言，本发明涉及在移动通信系统中将通信路由到基于 IP 的语音（VoIP）终端。

背景技术

近来无线局域网（WLAN）在移动通信中已经变得重要。WLAN 相较于比如通用移动电信系统（UMTS）和全球移动通信系统（GSM）这样的许可频带蜂窝通信系统而言的优点在于它们使用非许可频带并且小区大小小得多的事实。这些事实使得有可能构建由小型公司实体和个人用户运营的专用 WLAN。无线通信在这些 WLAN 中的成本比在许可频带蜂窝系统中要低廉得多。WLAN 已经主要用于因特网络接入，但是通过 WLAN 提供语音通信的想法近来已经赢得契机。为了针对基于 WLAN 技术的语音而获得广阔的市场份额以及为终端用户提供可靠的服务体验，有必要能够提供支持基于 WLAN 和基于许可频带的无线接入的双系统终端。换言之，对于用户来说必须有可能在 WLAN 和许可频带蜂窝系统中漫游。通常，WLAN 无线接入在存在有 WLAN 基础设施的市区中使用，而许可频带蜂窝系统在 WLAN 覆盖以外的区域中使用。

3G 伙伴项目已经将 IP 多媒体子系统(IMS)标准化以便迎合 VoIP 和其它基于 IP 的多媒体服务之需。通常，UMTS 无线接入网络用来接入支持 IMS 的核心网络。然而，包括移动交换中心（MSC）、归属位置寄存器（HLR）、访问位置中心（VLR）、CAMEL 服务实体（CSE）和服务控制点（SCP）的现有电路交换核心网络基础设施提供范围广阔的服务。当运营商希望向双系统终端提供 WLAN 和许可频带无线接

入能力时，如果运营商具有通过两种无线接入技术来提供相同服务的某一机制则将是有益的。提供后向兼容服务尤其重要。换言之，有必要能够也在 WLAN 侧提供来自许可频带蜂窝系统的常见观感服务。这些服务称为传统服务。这种服务的例子包括呼叫转发、预付费、附加费率（premium rate）和免费服务号码、呼叫等待和呼叫转移。通常使用包括 MSC 和 SCP 的智能网络基础设施来提供预付费服务和服务号码。在智能网络的 3GPP 标准化版本中 SCP 称为 CSE。

现在参照图 1，该图图示了现有技术中与为双系统终端提供传统服务相关联的问题。图 1 图示了在实践中必须在 IMS 中重建传统服务这一事实。在 IMS 中网元与协议大相径庭，因此这代表相当数量的工作。在图 1 中有移动台（MS）100，该移动台是能够通过 WLAN 无线接入和许可频带无线接入来通信的双系统移动台。许可频带无线接入例如可以是基于时分多址（TDMA）的 GSM 无线接入或者基于宽带码分多址（WCDMA）的 UMTS 无线接入。在图 1 中也有与 IP 多媒体子系统（IMS）通信的 WLAN 124，该 IMS 至少包括 P-CSCF 102、I-CSCF 104、S-CSCF 106、MGCF 120 和 MGW 122。当在 WLAN 124 的区域中时经由 IMS 提供去往和来自 MS 100 的多媒体通信。WLAN 124 连接到将基于 IP 的用户平面业务转换到电路交换的 PSTN 126 的媒体网关（MGW）122。WLAN 124 也与代理呼叫状态控制功能（P-CSCF）102 通信。信令平面业务被路由到 P-CSCF 如 P-CSCF 102。信令平面业务例如是基于会话发起协议（SIP）的。SIP 在因特网络工程任务组（IETF）文献 RFC 3261 中有定义。P-CSCF 102 用来访问查问呼叫状态控制功能（I-CSCF）104，该 I-CSCF 使用归属订户服务器（HSS）108 来确定其中当前注册了给定订户的服务呼叫状态控制功能（S-CSCF）106。S-CSCF 控制源自于和终止于 MS 100 的多媒体通信。S-CSCF 与将信令平面业务转换成电路交换信令的媒体网关控制功能（MGCF）120 进行通信。例如，MGCF 120 将在 MS 100、P-CSCF 102、I-CSCF 104、S-CSCF 106 与 MGCF 120 之间使用的 SIP 信令转换成在 PSTN 126 中使用的 ISDN 用户部分（ISUP）信令。MGCF 120 也例如

使用国际电信联盟（ITU-T）H.248 协议来控制 MGW 122。S-CSCF 106 连接到三个服务平台，即应用服务器（AS）110、CSE 116 和开放服务架构（OSA）服务器 118。S-CSCF 106 经由 IP 移动性（IM）服务交换功能（SSF）112 连接到 CSE 116。S-CSCF 106 经由服务能力服务器（SCS）114 连接到 OSA 服务器 118。

在图 1 中也有连接到 GSM/UMTS 电路交换核心网络的 GSM/UMTS BSS 160，该网络至少包括 MSC 150、VLR 152、GMSC 156、HLR 154 和 CSE 158。GSM/UMTS BSS 160 连接到 MSC 150。MSC 150 也包括 VLR 152。MSC 150 连接到 GMSC 156。也有存储与订户的位置有关的订户数据及其服务数据的 HLR 154。GMSC 156 也连接到 PSTN 126。CSE 158 在向 BSS 160 所服务的订户提供 IN 服务时控制 GMSC 156 和 MSC 150。CSE 158 也有通向 HLR 154 的接口，该接口允许询问和修改 HLR 154 中的服务数据。多个标准化补充服务由 MSC 150、GMSC 156、VLR 152 和 HLR 154 直接实施。这些服务的例子包括呼叫转发、呼叫等待、呼叫转移、呼叫完成到忙订户、关闭用户组和呼叫禁止。除这些业务之外，还可以有在这些网元中直接实施的各种特定于销售商的补充服务。为了迎合前述传统补充服务之需，在 MSC 150、GMSC 156、VLR 152 和 HLR 154 中存在各种服务功能。这些服务功能在图 1 中图示为服务功能集 170-174。各服务功能集可以包括在给定的网元中掌控的多种不同服务功能。

为了在 MS 100 处于 WLAN 124 的服务区中时支持相同的传统服务，服务功能集 170-174 必须端口连通到至少包括 P-CSCF 102、I-CSCF 104、S-CSCF 106 和 HSS 108 的对应 IMS 网元。这代表相当数量的任务，因为当在 IMS 网元中实施等效服务功能集 180-184 时必须重复在服务功能集 170-174 中投入的所有开发努力。例如，MSC 中的服务功能集 170 将对应于 S-CSCF 106 中的服务功能集 182，而 CSE 中的服务功能集 171 将分别对应于 AS 110、CSE 116 和 OSA 服务器 118 中的服务功能集 181、183 和 184。然而，对应不是直接和明显的。足以认为传统服务功能集从 GSM/UMTS 电路交换核心网络到

IMS 侧的端口连通并非微不足道，因为在 IMS 网元与 MS 100 之间使用的协议与在 GSM/UMTS 电路交换核心网络中使用的协议大相径庭。

在如下出版物中提出了一种在为从 GSM/UMTS BSS 漫游到 WLAN 侧的移动台提供传统服务时的可能性："SIP-Enabled Gateway MSC: Linking WiFi Hot Spots with 2.5/3G Networks"，Amir Atai, Ajay Sahai, Telica，2004 年 3 月 31 日。Atai 所公开的解决方案包括将 WALN 直接连接到电路交换核心网络中也充当服务访问 MSC（VMSC）的 GMSC。Atai 所公开的解决方案的不足在于给定的订户总是由给定的 GMSC 服务。然而，即使在双系统终端的情况下，对于运营商而言仍然必须有可能为任何 GMSC 中的给定终端接收终止呼叫。GMSC 中终止呼叫的处理必须对 2G/3G 和 WLAN 终端都是统一的。无论终端的类型如何都必须使用从 HLR 获得的漫游号码将呼叫路由到正确的服务 VMSC。另外，能够配置 DNS 使得使用例如"sip.operator.com"这样的同一完全限定域名（FQDN）来查询多个 MSC 服务器是有益的，其中"operator"代表运营商名而"sip"代表 SIP 注册器集。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 就有可能以轮循方式向充当 SIP 注册器的不同 MSC 服务器返回 IP-地址。因此，在不同的注册时间，可以从 DNS 提供不同的 IP-地址给双系统终端。此外，一些传统服务可能要求与传统服务有关的呼叫必须路由到语音服务器或者集中式 IN 服务交换点/经由语音服务器或者集中式 IN 服务交换点进行路由。因此，能够在电路交换核心网元之间使用传统 ISUP 信令将是有益的。当使用纯 SIP 信令时，用户的 ITU-T E.164 格式订户号码不可用。

发明内容

本发明涉及一种用于在至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的通信系统中对呼叫进行路由的方法。该方法包括：从所述移动台接收去往所述第一呼叫控制节点的注册消息，所述注册消息包括针对所述移动台的逻辑名；

在所述第一呼叫控制节点的请求下在所述目录中将所述逻辑名映射为针对所述移动台的国际移动订户标识（IMSI）；在所述第一呼叫控制节点的请求下更新所述移动台的位置到所述归属位置寄存器，所述请求包括所述国际移动订户标识；在所述第二呼叫控制节点中接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；在所述归属位置寄存器的请求下从所述第一呼叫控制节点分配漫游号码；从所述归属位置寄存器发送至少包括所述漫游号码的查问响应消息到所述第二呼叫控制节点；从所述第二呼叫控制节点发送呼叫建立请求消息到所述第一呼叫控制节点；以及在所述第一呼叫控制节点的请求下在所述目录中将所述被叫方号码映射为针对所述移动台的所述逻辑名。

本发明也涉及一种至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的系统。该系统还包括：在所述第一呼叫控制节点中的移动性实体，配置用以：从所述移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从所述目录将所述逻辑名映射为针对所述移动台的国际移动订户标识（IMSI）；以及通过指明所述国际移动订户标识（IMS）来请求从所述归属位置寄存器更新所述移动台的位置；在所述第二呼叫控制节点中的呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到所述第一呼叫控制节点；以及在所述第一呼叫控制节点中的呼叫控制实体，配置用以请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

本发明也涉及一种呼叫控制节点，包括：移动性实体，配置用以：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移

动订户标识（IMSI）；以及通过指明所述国际移动订户标识（IMSI）来请求从归属位置寄存器更新所述移动台的位置；以及呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到第二呼叫控制节点；以及请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

本发明也涉及一种包括代码的计算机程序，适于当在数据处理系统上执行时进行以下步骤：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识（IMSI）；请求从归属位置寄存器更新所述移动台的位置，所述请求包括所述国际移动订户标识；接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问消息；发送呼叫建立请求消息到另一呼叫控制节点；以及请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

在本发明的一个实施例中，在第二呼叫控制中获得主叫方号码。例如针对收到的去往第二呼叫控制节点的呼叫建立请求消息来获得主叫方号码。在响应于从归属位置寄存器收到漫游号码而发送的呼叫建立消息中向第一呼叫控制节点提供主叫方号码。当收到呼叫建立请求消息时，第一呼叫控制节点提取主叫方号码并且确定主叫方号码是否包括指示了主叫方号码可以转译成逻辑名的前缀。如果主叫方号码包括这样的前缀，则在所述第一呼叫控制节点的请求下在目录中将它映射为针对主叫方的第二逻辑名。作为响应，目录将第二逻辑名返回到第一呼叫控制节点。在呼叫控制节点中的呼叫控制实体中执行呼叫建立请求消息和主叫方号码分析。

在本发明的一个实施例中，在移动台的通信实体中确定无线局域网（WLAN）在移动台处的可用性。通信实体建立从所述移动台到连接至无线局域网的接入路由器的连接。通信实体经由所述接入路由器获得所述第一呼叫控制节点的标识。接入路由器例如是控制去往和来自 WLAN 的区域中移动台的分组数据服务接入的路由器。路由器也可以针对它所连接到的 WLAN 中的移动台来执行认证、鉴权和记账功能。

在本发明的一个实施例中，通信系统包括无线局域网（WLAN）。

在本发明的一个实施例中，移动通信系统包括全球移动通信系统（GSM）网络和通用移动电话系统（UMTS）网络中的至少一个

在本发明的一个实施例中，第一和第二呼叫控制节点是移动服务交换中心服务器（MSS）。MSS 可以控制至少一个处理用户平面业务的媒体网关或者媒体代理。可以从公共交换电话网络（PSTN）或者其它呼叫控制节点接收用户平面业务作为电路交换连接，该电路交换连接在媒体网关中被转换成分组交换连接。在本发明的一个实施例中，第一和第二呼叫控制节点是移动服务交换中心（MSC）。

在本发明的一个实施例中，移动台包括会话发起协议（SIP）用户代理。当在 WALN 的区域中，用户代理通过发送会话发起协议（SIP）注册消息到第一呼叫控制节点来执行位置注册。呼叫控制节点可以包括使用会话发起协议（SIP）信令来与用户代理通信的呼叫控制实体。呼叫控制实体可以使用电路交换信令如 ISDN 用户部分（ISUP）来与其它呼叫控制节点通信。如果主叫方和被叫方属于同一运营商的网络，则用户平面业务可以不转换成电路交换连接，但是可代之以通过分组数据将用户平面业务从主叫方移动台运送到被叫方移动台。在那一情况下，在 ISUP 信令消息中带有与主叫方和被叫方相关联的用户平面 IP 地址。

在本发明的一个实施例中，主叫方建立请求消息是 ISDN 用户部分（ISUP）呼叫建立请求消息。在本发明的一个实施例中，呼叫建立请求消息是会话发起协议（SIP）邀请消息或者一般而言是任何等

效的基于 IP 的语音呼叫建立请求消息。

在本发明的一个实施例中，目录是轻型目录访问协议（LDAP）目录。使用 LDAP 协议来访问目录。

在本发明的一个实施例中，移动台包括无线局域网终端。在本发明的一个实施例中，移动台包括订户标识模块（SIM）。

在本发明的一个实施例中，移动台是支持 WLAN 和许可频带无线连通性的多无线终端。许可频带无线连通性例如包括在已经为提供 2G 和 3G 服务的运营商所分配的无线频带上的全球移动通信系统（GSM）无线连通性和通用移动电信系统（UMTS）连通性。

在本发明的一个实施例中，在呼叫控制节点内的呼叫控制实体是软件部件。在本发明的一个实施例中，在呼叫控制节点内的移动性实体是软件部件。在本发明的一个实施例中，在移动台节点内的通信实体是软件部件。这些部件中的各部件可以包括至少一个独立编译或者转译的程序模块。部件可以包括在处理器或者虚拟机如 Java 虚拟机中执行的多个进程或者线程。

在本发明的一个实施例中，计算机程序存储于计算机可读介质上。计算机可读介质可以是可移动存储卡、磁盘、光盘或者磁带。

在本发明的一个实施例中，术语呼叫也指代短消息。在这一实施例中，呼叫建立消息是短消息递送消息而呼叫控制实体是短消息递送实体。在这一情况下，漫游号码是用于递送短消息到第一呼叫控制实体的路由号码。

在本发明的一个实施例中，DNS 被配置为使得使用同一完全限定域名（FQDN）如“sip.operator.com”来查询多个 MSC 服务器，其中“operator”代表运营商名而“sip”代表 SIP 注册器集。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 可以用轮循方式为充当 SIP 注册器的不同 MSC 服务器返回 IP-地址。因此，在不同的注册时间可以从 DNS 提供不同的 IP 地址给双系统终端。

从核心网络和补充服务观点来看，本发明的益处与 2G/3G 终端

和双系统终端的统一处理有关。在支持 WLAN 和许可频带接入的任何双系统终端情况下，对于运营商来说有可能为任何 GMSC 中的终端接收终止呼叫。订户编号由于终端是双系统终端的事实而不受影响。无论当前 VMSC 是否充当用于 WLAN 热点的 SIP 注册器或者当前 VMSC 是否只服务于 2G/3G 区域都可以使用从 HLR 获得的漫游号码将呼叫路由到正确的服务 VMSC。

另外，有可能配置 DNS 使得使用同一完全限定域名（FQDN）来查询多个 MSC 服务器。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 可以用轮循方式为充当 SIP 注册器的不同 MSC 服务器返回 IP-地址。因此，在不同的注册时间可以从 DNS 提供不同的 IP 地址到双系统终端。

另外，通过允许在收到的去往网关 MSS 的呼叫建立请求消息中使用 MSISDN 号码，有可能维持普通电路交换核心网络漫游机制，包括使用 HLR、VLR 和漫游号码分配。没有必要为 IP 多媒体子系统利用不同机制。这允许从电路交换核心网络使用传统补充服务。从补充服务的观点来看，以与许可频带无线服务区相似的方式来处理 WLAN 提供了更容易的服务部署和运营。

此外，一些传统服务可能要求与传统服务有关的呼叫必须路由到语音服务器或者集中式 IN 服务交换点/经由语音服务器或者集中式 IN 服务交换点进行路由。因此，能够在电路交换核心网元之间使用传统 ISUP 信令是有益的。

附图说明

被包含用来提供对本发明的进一步理解并且构成本说明书一部分的附图图示了本发明的实施例，并且与描述一起有助于说明本发明的原理。在附图中：

图 1 是图示了现有技术中与为双系统终端提供传统服务相关联的问题的框图；

图 2 是图示了根据本发明的通信系统的框图；

图 3 是图示了在本发明的一个实施例中从会话发起协议（SIP）用户代理（UA）到移动交换中心服务器（MSS）的位置更新的消息序列图；

图 4 是图示了在本发明的一个实施例中在基于会话发起协议（SIP）的两个用户代理（UA）之间的移动台到移动台呼叫的消息序列图；

图 5 是描绘了用于在通信系统中将通信路由到会话发起协议（SIP）用户代理的方法的一个实施例的流程图；以及

图 6 是图示了本发明的一个实施例中的移动交换中心服务器（MSS）的框图。

具体实施方式

现在将具体考虑本发明的实施例，这些实施例的例子在附图中进行图示。

图 2 是图示了根据本发明的通信系统的框图。该通信系统至少包括移动台（MS）200、服务 MSS 220、网关 MSS 222、归属位置寄存器（HLR）230、轻型目录访问协议（LDAP）目录 232、CAMEL 服务实体（CSE）216、基站控制器（BSC）210 和连接到基站收发器（BTS）234 的第一接入网络 218。MS 200 是经由 MSS 220 获得 SIP 连通性的具有 SIP 功能的用户代理。MS 200 是支持 WLAN 和许可频带无线连通性的多无线终端。在本发明的一个实施例中，MS 200 包括执行所有与通信有关的功能的通信实体（未示出）。WLAN 基站收发器（BTS）202 提供 WLAN 无线连通性，而 BTS 246 支持许可频带无线连通性。许可频带无线连通性例如可以基于 WCDMA 无线接入或者 TDMA 无线接入。服务 MSS 220 包括为服务 MSS 220 中当前注册的订户存储订户数据的访问位置寄存器（VLR）214。网关 MSS 222 具有通向公共交换电话网络（PSTN）240 和服务 MSS 220 的信令连接。网关 MSS 222 控制第一 MGW 242 而 MSS 220 控制第二 MGW 244。第一 MGW 242 连接到 PSTN 240 并且向 IP 分组提供到/从电路交换 E1/T1 的用户平面转

换。第二 MGW 244 连接到 PSTN 240 并且向 IP 分组提供到/从电路交换 BSC 210 的用户平面转换。UMA 控制器 208 也可以提供通向第二 MGW 244 的电路交换连接。分别基于来自 MSS 222 和 MSS 220 的请求在第一 MGW 242 与第二 MGW 244 之间对分组进行路由。BSC 210 使用协议接口 250 来连接到 MSS 220。协议接口 250 例如是 GSM A/Gb-接口或者 UMTS Iu-接口。BSC 210 因此也可以是 UMTS 无线网络控制器。

在图 2 中也有第二接入网络 206，该网络的信令平面经由非许可移动接入（UMA）控制器 208 连接到 MSS 220。第二接入网络 206 是基于 IP 的接入网络。UMA 控制器 208 以看似标准 RAN 的方式接口到 MSS 220 中。换言之，UMA 控制器 208 对 MSS 220 而言仿效了 BSC 210。经由会话边界控制器（SBC）203 也连接到第二接入网络 206 的是客户端设备（CPE），该 CPE 例如是接入路由器。WLAN 基站收发器（BTS）202 连接到 CPE 204。可以有经由 CPE 204 连接到第二接入网络 206 的多个 WLAN BTS。SBC 203 充当 SIP 代理并且向 MS 200 隐藏在至少包括第二接入网络 206 的运营商网络内的地址空间。当在 MS 200 与连接到 PSTN 240 的订户之间有呼叫时，去往/来自 MS 200 的用户平面业务经由 SBC 203 去往第一 MGW 242。SBC 203 也可以执行标准的与防火墙有关的任务，比如分组过滤。LDAP 目录 232 用来执行将 SIP URI 转译成 ITU-T E.164 地址并且反之亦然。例如，LDAP 目录在服务 MSS 的请求下将主叫方 SIP URI 转译成主叫方 IMSI 并且在相应的响应消息中提供 IMSI。当 MS 200 在 MSS 220 中执行注册（换言之，初始位置更新过程）时， LDAP 目录向 MSS 220 提供订户信息，该信息通常无法经由从 MS 200 到 MSS 220 的 SIP 信令来获得，但是可在位置更新时或者在呼叫建立请求时经由 GSM A-接口信令或者 UMTS Iu-接口信令来获得。这样的信息例如包括与 MS 200 SIP URI 相对应的 IMSI。该信息在 MSS 220 的请求下从 LDAP 目录 232 提供给 MSS 220。

在本发明的一个实施例中，运营商的网络使用单个 LDAP 目录，例如 LDAP 目录 232。当订户经由配备有 SIP-接口的任何 MSS 注册时，

可以访问同一 LDAP 目录。因此，无论询问 MSS 如何，LDAP 目录都是相同的。在本发明的一个实施例中有多个 LDPA 目录。

图 3 是图示了在本发明的一个实施例中从会话发起协议（SIP）用户代理（UA）到移动交换中心服务器（MSS）的位置更新的消息序列图。在时刻 t_1，MS 200 确定经由 WLAN BTS 202 的 WLAN 接入是可用的并且确定应当经由 WALN 无线接入对去往 MS 200 和来自 MS 200 的通信进行路由。MS 200（换言之，SIP 用户代理）向 DNS 服务器 314 发送 DNS 询问消息，如箭头 301 所示。该 DNS 询问消息指明了 SIP 服务器完全限定域名（FDQN），该 FDQN 由 DNS 服务器 314 解析成至少一个 IP 地址。在图 3 中提供有针对 MSS 220 的单个 IP 地址。DNS 服务器 314 以向 MS 200 提供该 IP 地址的查询响应消息做出响应，如箭头 302 所示。由此，MS 200 向 MSS 220 发送 SIP 注册消息，如箭头 303 所示。该 SIP 注册消息至少带有 MS 200 的 SIP URI 以及用户代理 IP 地址以便由 MSS 220 用来向 MS 200 发送用户平面和信令平面分组。SIP 注册消息可以穿越 SBC（未示出），这会更改用户代理 IP 地址。当 MSS 220 收到 SIP 注册消息时，它向 LDAP 目录 232 发送 LDAP 搜索消息，如箭头 304 所示。该 LDAP 搜索消息至少包括针对 MS 200 的 SIP URI。响应于 LDAP 搜索消息，LDAP 目录 232 获得与 SIP URI 相关联的订户数据。LDAP 目录 232 向 MSS 220 发送 LDAP 搜索响应消息，如箭头 305 所示。该 LDAP 搜索响应消息至少包含与 MS 200 相关联的 IMSI。LDAP 搜索响应消息中所含其它参数可以包括与 MS 200 相关联的主叫方 E.164 地址（MSISDN-A）、用户名以及与认证有关的参数如临时数和来自 MS 200 的预期认证响应。当收到 LDAP 搜索响应消息时，MSS 220 向 MS 200 发送 SIP 401 响应消息，如箭头 306 所示。SIP 401 响应消息包括 WWW-认证/摘要报头，该报头又包括与运营商网络中的 SIP 服务相关联的字段（realm）、运营商的域、从 LDPA 目录 232 接收的临时数以及在认证时所要使用的算法（通常是消息摘要 5（MD5））。响应于收到 SIP 401 响应消息，MS 200 向 MSS 220 提供 SIP 注册消息，如箭头 307 所示。该 SIP 注

册消息包括认证/摘要报头，该报头包括与 MS 200 相关联的用户名、与运营商网络中的 SIP 服务相关联的字段、运营商的域、临时数、与 MSS 220 相关联的 URI 以及 MS 200 基于在 SIP 401 响应消息中接收的参数而生成的响应。在收到 SIP 注册消息时，MSS 220 对 MS 200 所生成的响应与从 LDAP 目录 232 收到的预期响应进行比较。

响应于成功的认证，MSS 220 开始针对 HLR 230 执行位置更新。MSS 220 将 MS 200 的位置更新到与它相关联的 VLR 214。然而，在图 3 的情况下，VLR 214 被视为 MSS 220 的部分而没有单独地示出。在本发明的一个实施例中，MSS 220 获得在来自 LDAP 目录 232 的 SIP 注册消息中没有提供的对于位置更新而言必需的所有 MS 200 参数。在成功的认证之后，MS 200 向 HLR 230 发送位置更新请求消息，如箭头 308 所示。该位置更新请求消息至少包括与 MS 200 相关联的 IMSI。响应于收到位置更新请求消息，HLR 230 向 MSS 220 发送至少一个插入订户数据消息，如箭头 309 所示。该插入订户数据消息提供与 MS 200 相关联的订户数据。该订户数据被更新到与 MSS 220 相关联的 VLR 214。MSS 220 确认该插入订户数据消息，如箭头 310 所示。当所有插入订户数据消息都已经被 MSS 220 确认时，HLR 230 向 MSS 220 发送位置更新响应消息，如箭头 311 所示。由此，MSS 220 向 MS 200 发送 SIP 200 OK 消息，如箭头 312 所示。

图 4 是图示了在本发明的一个实施例中在基于会话发起协议（SIP）的两个用户代理（UA）之间的移动台到移动台呼叫的消息序列图。用户代理是主叫方移动台即 MS 200 而被叫方移动台即 MS 452。主叫方称为 A-方而被叫方称为 B-方，因此将字母 A 和 B 指定给与相应方相关联的相应网元和地址。MS 200 由 MSS 220 处理，因此该 MSS 也称为主叫方的 MSS（MSS-A）。MS 452 由 MSS 450 处理，因此该 MSS 也称为被叫方的 MSS（MSS-B）。起初在时刻 t_1，MS 200 的用户决定向 MS 452 进行传出呼叫。主叫用户通过选择或者输入作为根据 RFC 3261 的 SIP URI 的 SIP-URI-B 来指明被叫方。MS 200 向其中当前注册有 MS 200 的 MSS 220 发送 SIP 邀请消息，如箭头 401 所示。当收

到 SIP 邀请消息时，MSS 220 向 LDAP 目录 232 发送 LDAP 搜索请求消息，如箭头 402 所示。LDAP 搜索请求消息至少包括被叫方 SIP-URI-B。当 SIP-URI-B 由 LDAP 目录 232 获得时，它被转译成 E.164 地址，即 MSISDN-B。LDAP 目录 232 向 MSS 220 发送至少包括 MSISDN-B 的 LDAP 搜索响应消息，如箭头 403 所示。

当收到 LDAP 搜索响应消息和 MSISDN-B 时，MSS 220 现在能够使用 MSC 服务器的路由装置而无需利用 IMS 路由装置将呼叫路由到 MS 452。MSC 服务器的路由装置类似于 GSM/UMTS 核心网络中电路交换呼叫的路由装置。类似地，对于 MSS 220 来说有可能使用迎合电路交换呼叫的补充服务之需的服务功能。另外，对于 MSS 220 来说有可能使用迎合电路交换呼叫之需的计费功能。也应当注意，由于主叫方 E.164 号码 MSISDN-A 可从在位置更新过程中执行的 LDAP 目录询问中获得，所以有可能在提供补充服务时也使用 MSISDN-A。例如，如果向 CSE 216 发送询问则可以使用 MSISDN-A 和 MSISDN-B 来代替 SIP 名以查询主叫方和被叫方，以便发起 CAMEL 补充服务。CAMEL 补充服务只需检查 E.164 地址而不是 SIP URI。

MSS 220 向 HLR 230 发送包括 MSISDN-B 的发送路由指令（SRI）消息，如箭头 404 所示。当收到发送路由指令消息时，HLR 230 获得与被叫订户相关联的订户数据。HLR 230 知道其中注册有被叫订户的 MSC 服务器和 VLR，即 MSS 450。如箭头 405 所示，HLR 又通过发送提供漫游号码（PRN）消息来询问 MSS 450 以及其中的 VLR。该漫游号码也称为移动台漫游号码（MSRN）。VLR 然后使用如箭头 406 所示的消息向 HLR 230 提供漫游号码。该漫游然后用来向 MSS 450 路由呼叫。HLR 在它对 MSS 220 的响应消息 407 中对与被叫订户相关联的数据以及漫游号码进行封装，该 MSS 将根据 GSM/UMTS 电路交换核心网络充当网关 MSC。MSS 220 然后使用漫游号码在朝着 MSS 450 的方向上对呼叫进行路由。MSS 220 发送向 MSS 450 转发的 ISUP 初始地址消息（IAM）并且开始等待来自 MSS 450 方向的 ACM 消息，如箭头 408 所示。该 ISUP IMA 消息例如包括主叫方 E.164 地址即 MSISDN-A

和被叫方 E.164 地址即 MSISDN-B。当从 MSS 220 收到 IAM 消息 408 时，MSS 450 向 LDAP 目录 232 发送 LDAP 搜索请求消息，如箭头 409 所示。该 LDAP 搜索请求消息例如包括来自 ISUP IAM 消息的 MSISDN-A 和 MSISDN-B 参数。响应于该 LDAP 搜索请求消息，LDAP 目录 232 将 MSISDN-A 和 MSISDN-B 映射为 SIP-URI-A 和 SIP-URI-B。LDAP 目录 232 发送包括 SIP-URI-A 和 SIP-URI-B 的 LDAP 搜索请求响应消息，如箭头 410 所示。在已经从 LDAP 搜索响应消息收到 SIP URI 之后，MSS 450 向 MS 452 发送 SIP 邀请消息，如箭头 411 所示。该 SIP 邀请消息至少包括用来向 MS 452 发送用户平面和信令平面分组的 SIP-URI-A 和 SIP-URI-B 参数以及 IP 地址。该 IP 地址在位置更新信令过程中已经提供给 MSS 450。该 IP 地址与 MS 452 直接相关联或者它涉及如下 SBC，SIP 信令消息经由该 SBC 发送到 MS 452。MSS 450 向 MSS 220 发送 ISUP 地址完成消息（ACM），如箭头 412 所示。由此，MSS 220 向 MS 200 发送 SIP 尝试消息，如箭头 413 所示。

在本发明的一个实施例中，在 MSS 220 与 MSS 450 之间使用 SIP 信令。例如在这一情况下，呼叫建立消息是 SIP 邀请消息。即使在 MSS 220 与 MSS 450 之间使用 SIP 信令，仍有可能将 MSISDN 和漫游号码用于将呼叫路由到 MS 200。这允许维持利用 E.164 号码而不是 SIP 名的传统补充服务和计费机制。

在本发明的一个实施例中，与给定的 MS 相关联的用户平面和信令平面分组具有不同的 IP 地址。在本发明的一个实施例中，IP 地址涉及通用分组无线系统（GPRS）网关 GPRS 支持节点（GGSN）内的分组数据协议上下文（PDP）。

图 5 是描绘了用于在通信系统中将通信路由到会话发起协议（SIP）用户代理的方法的一个实施例的流程图。

在步骤 502，第一 MSS 等待来自 MS 的位置更新消息。如果没有收到消息，则该方法在步骤 502 继续。

在步骤 504，第一 MSS 将在来自 MS 的位置更新消息中接收的 SIP URI 映射为与 MS 相关联的 IMSI。

在步骤 506，第一 MSS 向 HLR 发送位置更新请求。在该位置更新请求消息中指明了与 MS 相关联的 IMSI。

在步骤 508，第二 MSS 接收发往 MS 的呼叫建立请求。该呼叫请求至少提供与 MS 相关联的 MSISDN。

在本发明的一个实施例中，呼叫建立请求仅提供与 MS 相关联的 SIP URI。第二 MSS 将 SIP URI 映射为与 MS 相关联的 MSISDN。

在步骤 510，第二 MSS 使用与 MS 相关联的 MSISDN 来询问 HLR 并且保留来自第一 MSS 的漫游号码以便将呼叫路由到 MS。可以从与第一 MSS 有关联的访问位置寄存器保留漫游号码。

在步骤 512，第二 MSS 使用漫游号码将呼叫建立请求路由到第一 MSS。

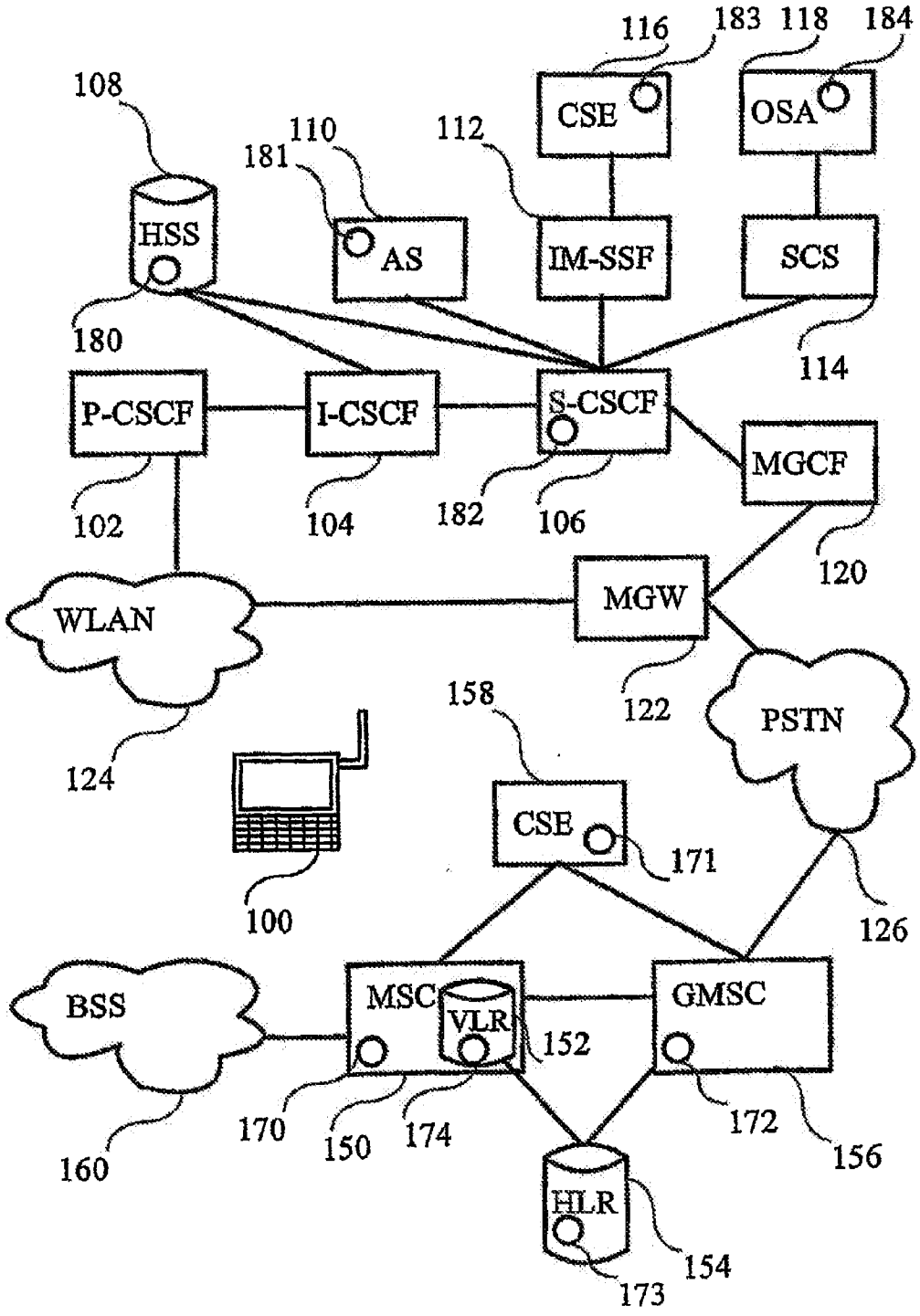
在步骤 514，第一 MSS 接收呼叫建立请求。在本发明的一个实施例中，第一 MSS 将与 MS 相关联的 MSISDN 映射为与 MS 相关联的 SIP URI。

在步骤 516，第一 MSS 检验呼叫建立请求中的主叫方号码是否可以映射为与主叫方相关联的 SIP URI。例如可以通过分析主叫方号码并且确定该号码是否包括指示了主叫方号码可以映射为 SIP URI 的前缀来执行该检验。

图 6 是图示了本发明的一个实施例中的移动交换中心服务器（MSS）的框图。在图 6 中有移动交换中心服务器（MSS）600。MSS 600 包括呼叫控制（CC）实体 602 和移动性管理实体 610。该呼叫控制实体与会话发起协议（SIP）实体 604 通信，该 SIP 实体又例如与移动台如图 2 中的移动台 200 通信。呼叫控制实体 602 也与用来访问归属位置寄存器的移动应用部分（MAP）实体通信。呼叫控制实体 602 也可以与 ISUP 实体通信以便建立、维护和释放呼叫。移动性管理实体 610 经由移动应用部分实体 606 与归属位置寄存器通信。在归属位置寄存器中更新移动台位置时使用移动性管理实体 610。经由会话发起协议实体 604 从移动台接收去往移动性管理实体 610 的注册请求。移动性管理实体 610 和呼叫控制实体 602 使用轻型目录访问协

议（LDAP）实体 612 来与目录通信。在本发明的一个实施例中，移动性管理实体 610 也包括访问位置寄存器。

对于本领域技术人员不言而喻，随着技术的发展，本发明的基本思想可以用各种方式来实施。本发明及其实施例因此不限于上述例子；而代之以它们可以在权利要求书的范围内进行改变。



（现有技术）

图 1

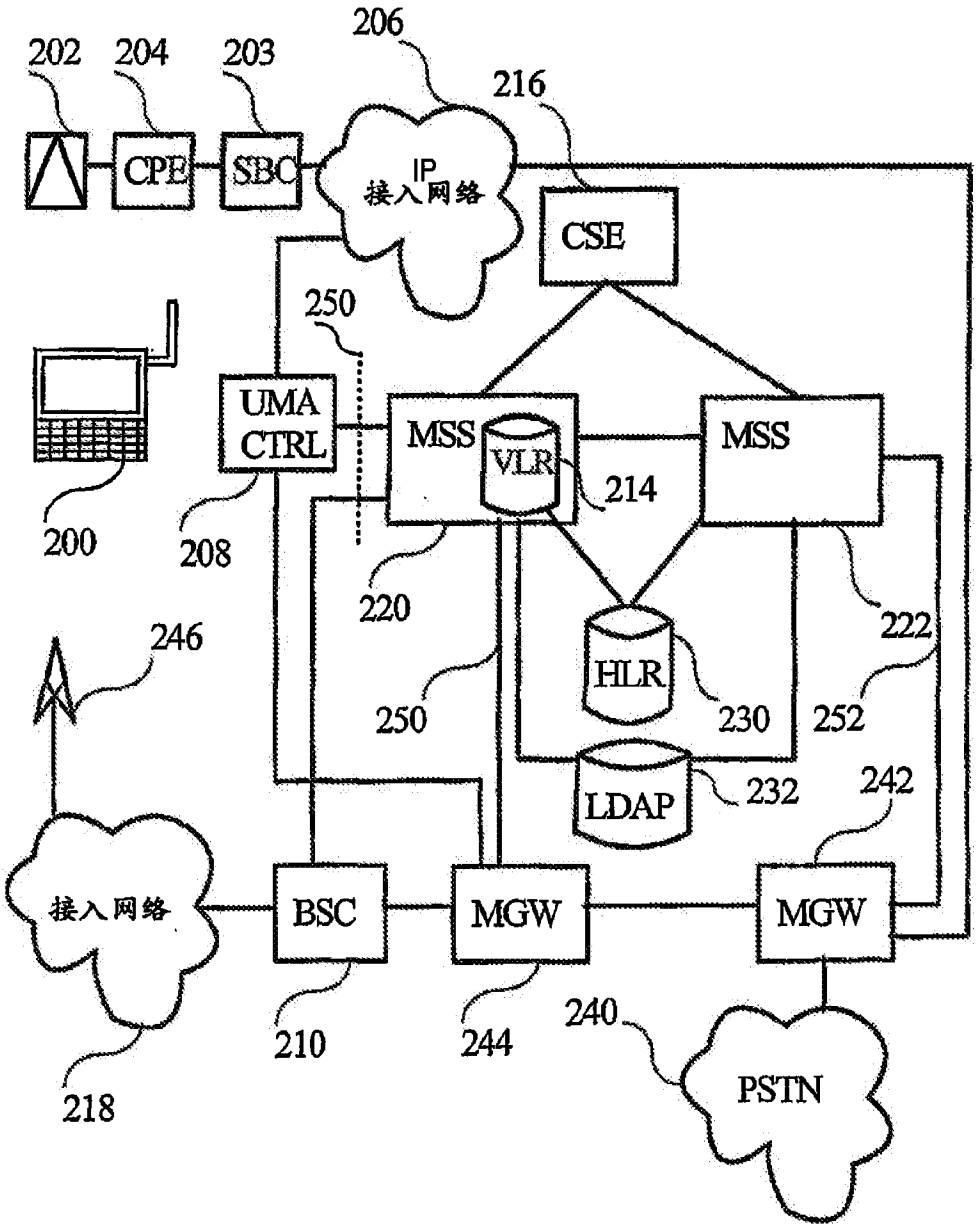


图 2

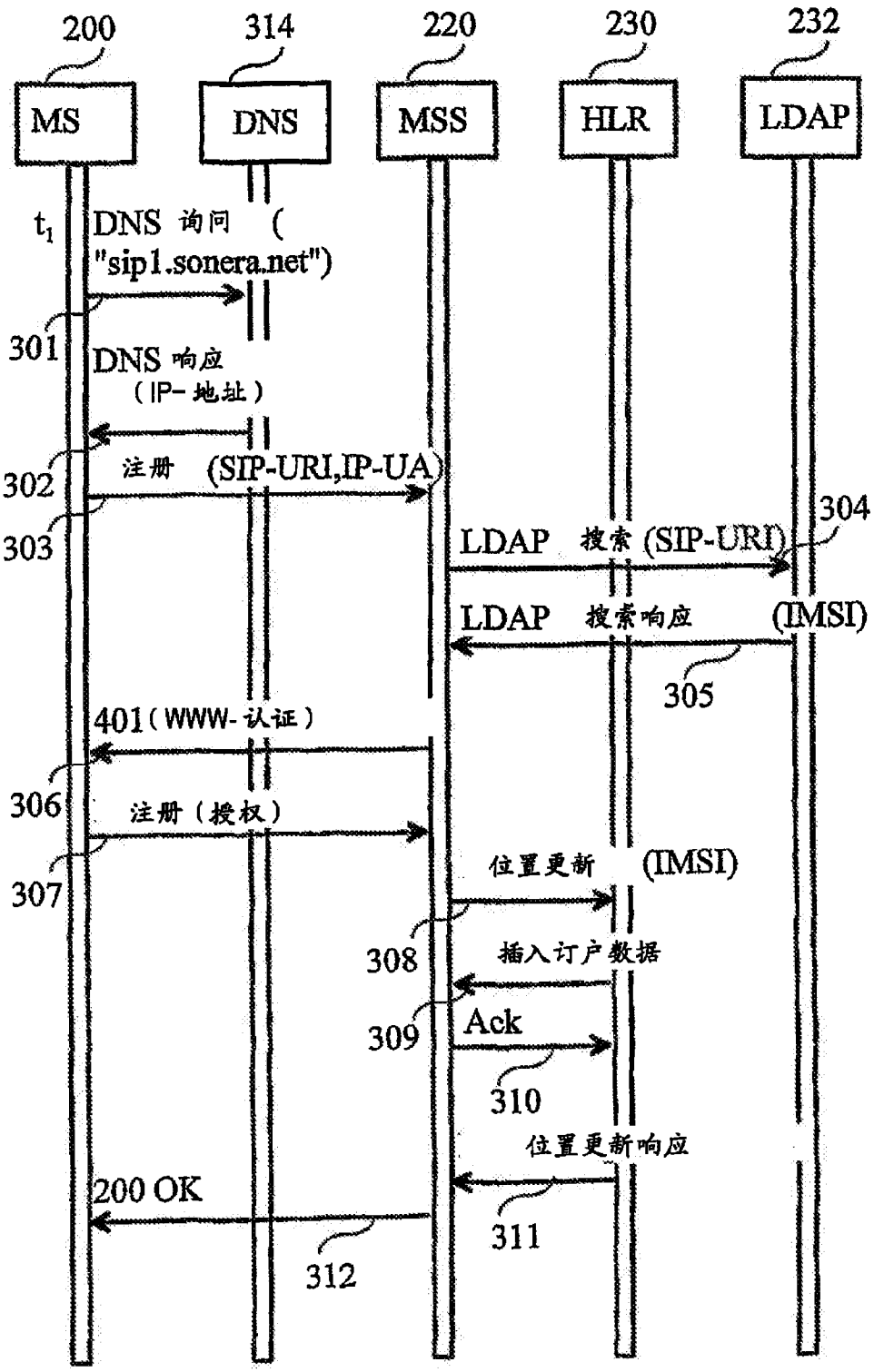


图 3

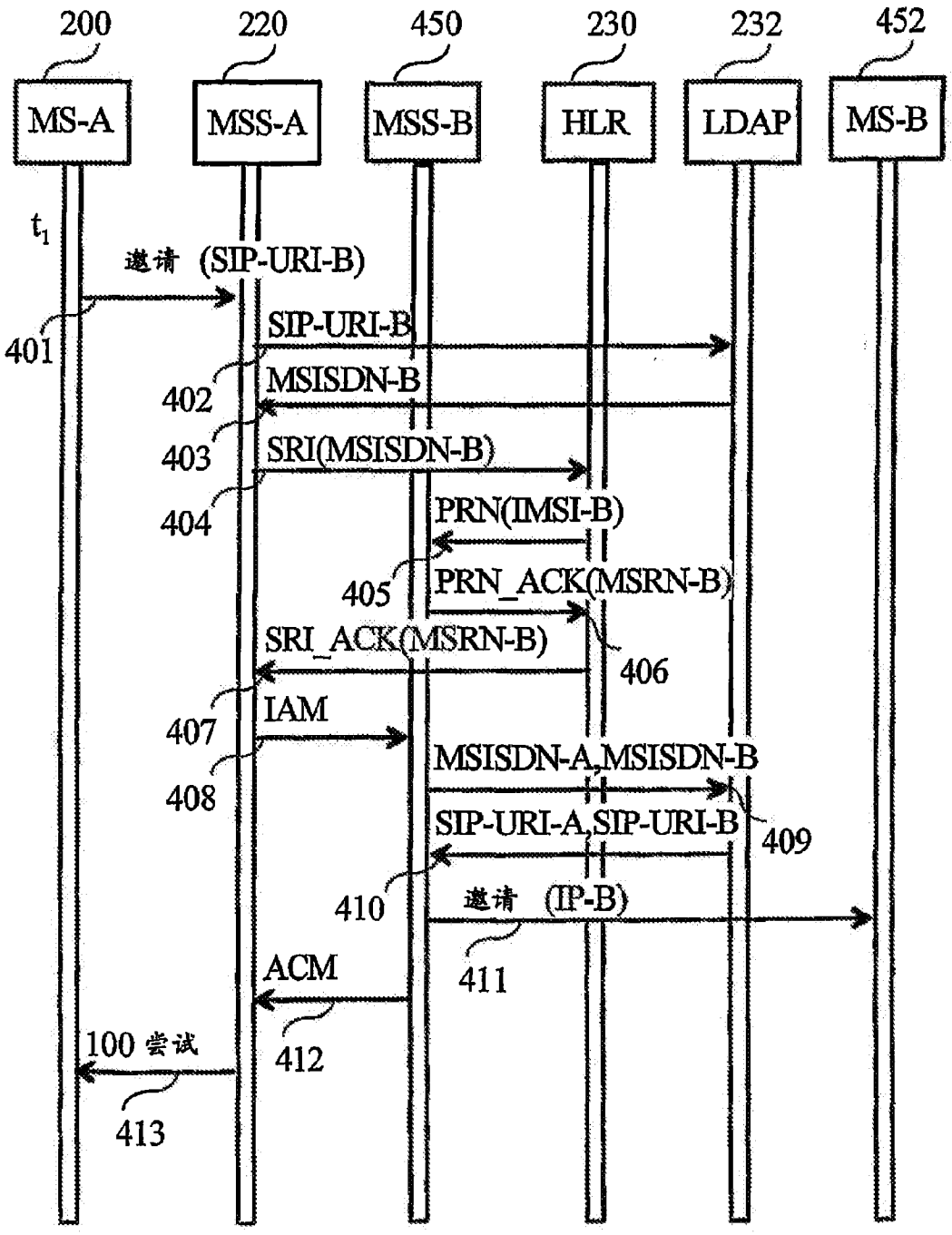


图 4

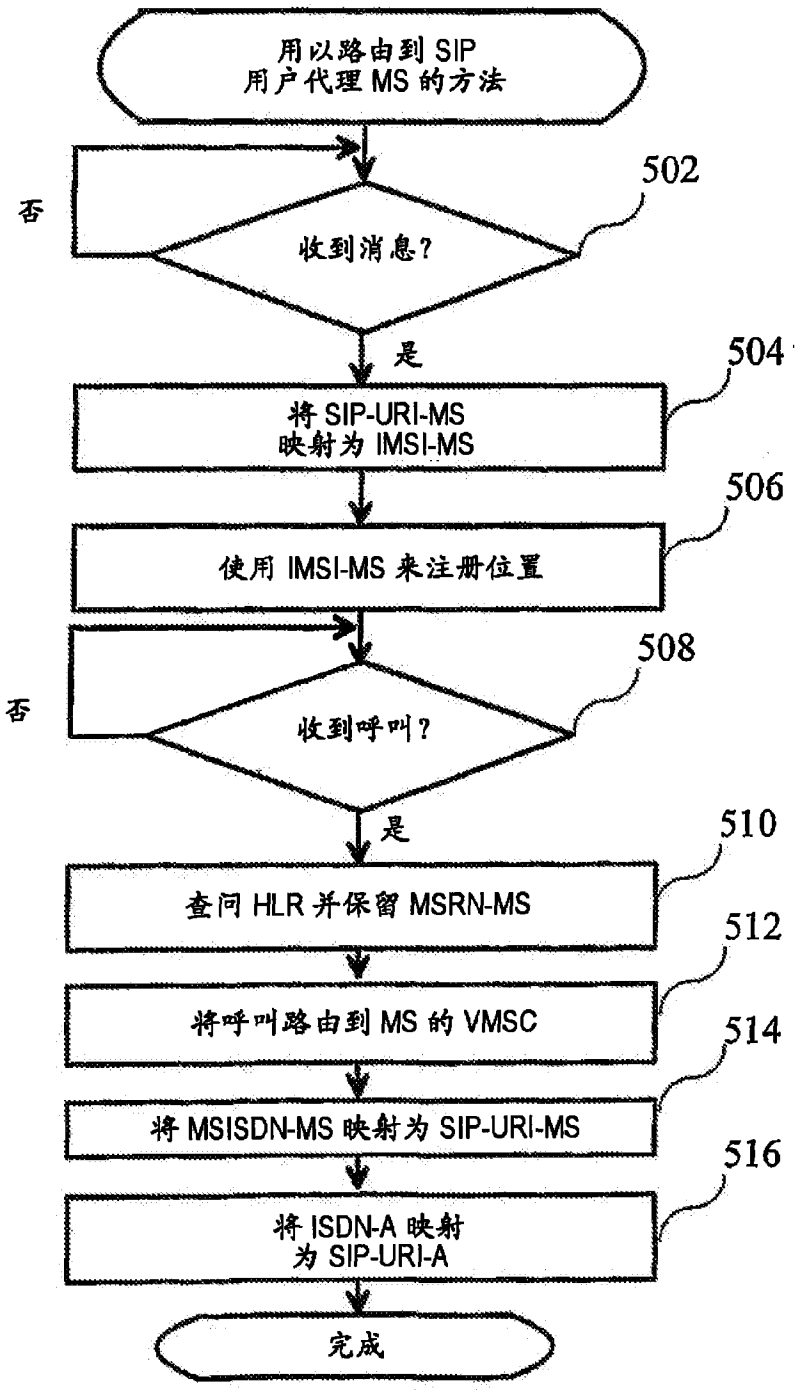


图 5

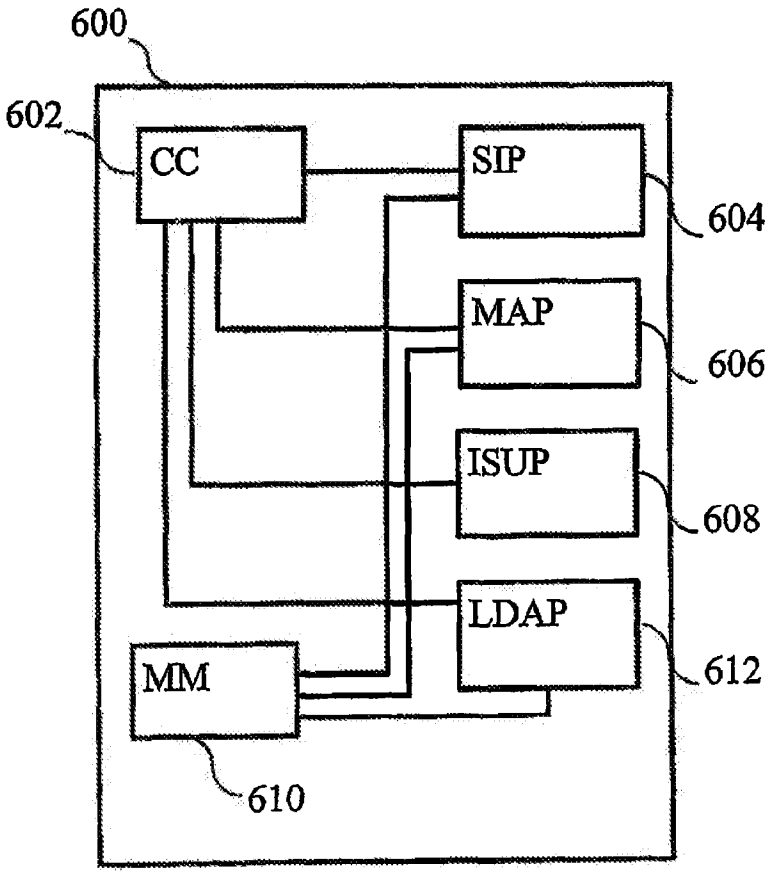


图 6

Espacenet

Bibliographic data: CN101095329 (A) — 2007-12-26

Distributed voice network

Inventor(s): GERALD LEBIZAY [US] + (LEBIZAY GERALD)

Applicant(s): INTEL CORP [US] + (INTEL CORP)

Classification: **- international:*H04L29/06***
- cooperative: G06Q20/102; H04L29/06027; H04L65/103; H04L65/104; H04L65/1043; H04L65/607

Application number: CN2005845760 20051229

Priority number(s): WO2005US47679 20051229 ; US20040027915 20041230

Also published as: CN101095329 (B) WO2006072099 (A1) US2012250624 (A1) US8605714 (B2) US2010008345 (A1) US8204044 (B2) US2006146797 (A1) US7593390 (B2) TWI307592 (B) GB2437666 (A) GB2437666 (B) DE112005003306 (T5) CN102833232 (A) less

Abstract of CN101095329 (A)

A method and apparatus (114, 116) that receives an IP packet and encapsulates the packet with an IP header. Further, time-domain multiplexed voice data is received and converted into VoIP packets. Still further, Signaling System (7) (SS7) compliant signals are decoded. The decoded (SS7) signals are received and encapsulated prior to transmission to a telephony device (102).

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580045760.3

[43] 公开日 2007 年 12 月 26 日

[11] 公开号 CN 101095329A

[22] 申请日 2005.12.29
[21] 申请号 200580045760.3
[30] 优先权
[32] 2004.12.30 [33] US [31] 11/027,915
[86] 国际申请 PCT/US2005/047679 2005.12.29
[87] 国际公布 WO2006/072099 英 2006.7.6
[85] 进入国家阶段日期 2007.7.2
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 G·利比扎伊

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 曾祥夌 魏 军

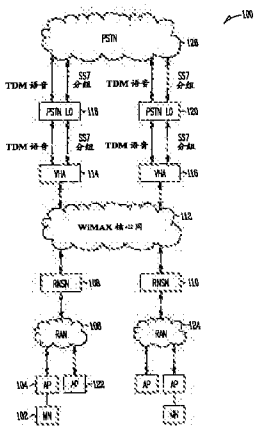
权利要求书 5 页 说明书 12 页 附图 4 页

[54] 发明名称

分布式语音网络

[57] 摘要

一种接收 IP 分组并封装分组与 IP 首标的方法及设备(114，116)。 此外，时域复用语音数据被接收并转换为 VoIP 分组。 此外，对符合信令系统(7)(SS7)的信号解码。 已解码(SS7)信号被接收，并在传送给电话装置(102)之前被封装。



1. 一种装置，包括:

封装电路，接收 IP 分组，并在所述分组前面附加 IP 首标;

基于 IP 的语音(VoIP)电路，接收时域复用语音数据，并把所述数据转换为 VoIP 分组;

信令电路，对符合 7 号信令系统(SS7)的信号解码；以及

控制电路，用于

从所述信令电路接收已解码 SS7 信号，并把所述已解码 SS7 信号传递给所述封装电路，以便传送给电话装置；以及

从所述 VoIP 电路接收 VoIP 分组，并把所述 VoIP 分组传递给所述封装电路，以便传送给所述电话装置。

2. 如权利要求 1 所述的装置，其特征在于，所述封装电路、VoIP 电路、信令电路和控制电路被实施为与存储装置进行数据通信的微处理器。

3. 如权利要求 1 所述的装置，其特征在于:

所述封装电路被实施为第一刀片，所述 VoIP 电路被实施为第二刀片，所述信令电路被实施为第三刀片，以及所述控制电路被实施为第四刀片；以及

所述第一、第二、第三和第四刀片相互进行数据通信。

4. 如权利要求 3 所述的装置，其特征在于，所述第一、第二、第三和第四刀片经由局域网进行通信。

5. 如权利要求 3 所述的装置，其特征在于，所述第四刀片还配置成维护涉及移动电话装置的电话号码、移动 IP(MIP)地址和转交地址的数据库。

6. 如权利要求 3 所述的装置，其特征在于，所述第一刀片包括到 IP 网络的接口。

7. 如权利要求 3 所述的装置，其特征在于，所述第二刀片包括到

传送时域复用语音数据的网络的接口。

8. 如权利要求 3 所述的装置，其特征在于，所述第三刀片包括到 SS7 网络的接口。

9. 一种进行基于 IP 的语音电话会话的方法，包括:

从第一电话装置接收邀请具体电话号码标识的第二电话装置参与基于 IP 的语音电话会话的请求;

使所述电话号码与关联所述电话号码的 IP 地址相关;

把邀请发送到所述 IP 地址;

接收对所述邀请的响应；以及

修改所述响应并将其转发给所述第一电话装置，使得已修改响应包含包括所述第一电话装置的第一 IP 地址的第一 IP 首标以及包括所述第一电话装置的第二 IP 地址的第二 IP 首标，其中所述第一 IP 地址表明所述第一电话装置到网络的连接点，以及其中作为所述第一电话装置向语音归属代理登记的结果产生所述第二 IP 地址。

10. 如权利要求 9 所述的方法，其特征在于，使所述电话号码与 IP 地址相关包括访问数据库以确定服务于所述第二电话装置的语音归属代理的 IP 地址。

11. 如权利要求 9 所述的方法，其特征在于，所述邀请符合会话发起协议(SIP)。

12. 如权利要求 9 所述的方法，其特征在于，还包括:

接收包含表示语音的数据的 IP 分组；以及

采用包含第三 IP 地址的第三 IP 首标以及包含第四 IP 地址的第四 IP 首标把所述 IP 分组转发给所述第一装置;

其中所述第三 IP 地址表明所述第一电话装置到网络的连接点，以及其中作为所述第一电话装置向语音归属代理登记的结果产生所述第四 IP 地址。

13. 如权利要求 9 所述的方法，其特征在于，还包括:

接收包含表示语音的数据的 IP 分组；以及

把所述 IP 分组发送给服务于所述第二装置的语音归属代理。

14. 如权利要求 9 所述的方法，其特征在于，还包括:

确定所述第一电话装置改变了它到所述网络的连接点；以及

重新定义所述第一 IP 地址以标识所述已改变的连接点。

15. 如权利要求 9 所述的方法，其特征在于，所述第一 IP 地址标识耦合到包括所述第一电话装置与之通信的接入点的符合 802.16e 的网络的无线电网络服务节点。

16. 一种提供指令的机器可访问媒体，所述指令在被访问时使所述机器执行操作，其中包括:

从第一电话装置接收邀请具体电话号码标识的第二电话装置参与基于 IP 的语音电话会话的请求;

使所述电话号码与关联所述电话号码的 IP 地址相关;

把邀请发送到所述 IP 地址;

接收对所述邀请的响应；以及

修改所述响应并将其转发给所述第一电话装置，使得已修改响应包含包括所述第一电话装置的第一 IP 地址的第一 IP 首标以及包括所述第一电话装置的第二 IP 地址的第二 IP 首标，其中所述第一 IP 地址表明所述第一电话装置到网络的连接点，以及其中作为所述第一电话装置向语音归属代理登记的结果产生所述第二 IP 地址。

17. 如权利要求 16 所述的媒体，其特征在于，使所述电话号码与 IP 地址相关包括访问数据库以确定服务于所述第二装置的语音归属代理的 IP 地址。

18. 如权利要求 16 所述的媒体，其特征在于，所述邀请符合会话发起协议(SIP)。

19. 如权利要求 16 所述的媒体，其特征在于，所述操作还包括:

接收包含表示语音的数据的 IP 分组；以及

采用包含第三 IP 地址的第三 IP 首标以及包含第四 IP 地址的第四 IP 首标把所述 IP 分组转发给所述第一装置;

其中，所述第三 IP 地址表明所述第一电话装置到网络的连接点，以及作为所述第一电话装置向语音归属代理登记的结果产生所述第四 IP 地址。

20. 如权利要求 16 所述的媒体，其特征在于，所述操作还包括：

接收包含表示语音的数据的 IP 分组；以及

把所述 IP 分组发送给服务于所述第二装置的语音归属代理。

21. 如权利要求 16 所述的媒体，其特征在于，所述操作还包括：

确定所述第一电话装置改变了它到所述网络的连接点；以及

重新定义所述第一 IP 地址以标识所述已改变的连接点。

22. 如权利要求 16 所述的媒体，其特征在于，所述第一 IP 地址标识耦合到包括所述第一电话装置与之通信的接入点的符合 802.16e 的网络的无线电网络服务节点。

23. 一种系统，包括：

封装电路，接收 IP 分组，并在所述分组前面附加 IP 首标；

基于 IP 的语音(VoIP)电路，接收时域复用语音数据，并把所述数据转换为 VoIP 分组；

计费电路，配置成测量所述系统的使用的持续时间和类型，以及使这类测量与用户帐户相关；

信令电路，对符合 7 号信令系统(SS7)的信号解码；以及

控制电路，用于

从所述信令电路接收已解码 SS7 信号，并把所述已解码 SS7 信号传递给所述封装电路，以便传送给电话装置；以及

从所述 VoIP 电路接收 VoIP 分组，并把所述 VoIP 分组传递给所述封装电路，以便传送给所述电话装置。

24. 如权利要求 23 所述的系统，其特征在于，所述封装电路、VoIP 电路、信令电路、计费电路和控制电路被实施为与存储装置进行数据通信的微处理器。

25. 如权利要求 23 所述的系统，其特征在于：

所述封装电路被实施为第一刀片，所述 VoIP 电路被实施为第二刀片，所述信令电路被实施为第三刀片，以及所述控制电路和计费电路被共同实施为第四刀片；以及

所述第一、第二、第三和第四刀片相互进行数据通信。

26. 如权利要求 25 所述的系统，其特征在于，所述第一、第二、第三和第四刀片经由局域网进行通信。

27. 如权利要求 25 所述的系统，其特征在于，所述第四刀片还配置成维护涉及移动电话装置的电话号码、移动 IP(MIP)地址和转交地址的数据库。

28. 如权利要求 25 所述的系统，其特征在于，所述第一刀片包括到 IP 网络的接口。

29. 如权利要求 25 所述的系统，其特征在于，所述第二刀片包括到传送时域复用语音数据的网络的接口。

30. 如权利要求 25 所述的系统，其特征在于，所述第三刀片包括到 SS7 网络的接口。

分布式语音网络

技术领域

本发明的实施例涉及在移动无线宽带网络上实现的基于IP的语音技术。

背景技术

基于IP的语音(VoIP)技术允许各方通过分组交换IP网络进行口头通信。VoIP技术在不断地普及，并且根据某些因素，可提供可与公共交换电话网(PSTN)相比的声音质量。

不断普及的还有无线移动网络。无线移动网络允许装置链接到网络，无需物理导电线路在装置与网络之间传送数据。此外，这类网络通过允许装置以对于无线移动网络域外部的网络单元或节点透明的方式改变接入点来允许移动性。

尽管VoIP技术和无线移动网络的普及性不断增长，但是对于基于因特网的当前VoIP服务没有移动客户装置。阻碍这类移动装置的进步的一个因素涉及找出用以在表现为保持单一IP地址的同时可允许移动装置在大地理区域漫游(因而可能在域之间来回移动)的简单方案。用户数据报协议(UDP)通过使用包含两个连接端点的IP地址和端口号的四元组对连接进行索引。改变这四个号码中的任一个使连接被中断和丢失。因此，重要的是，该装置表现为在地理上漫游的同时保持相同的IP地址。解决这个问题的困难随着允许装置在其中漫游的地理区域增大而增加。

通过上述明显看到，需要一种方案，通过该方案，可允许无线IP电话装置在地理上的大区域、如都市区域漫游。希望这种方案比较简单地实现为在现有无线网络上的重叠。还希望这种方案易于与PSTN

互连。

附图说明

图 1 说明在其中采用语音归属代理的一个实施例的网络环境。

图 2 说明根据本发明的一个实施例构成语音归属代理的协议栈。

图 3 说明图 2 所示的协议栈的移动 IP 层所采用的隧道技术方案。

图 4 说明根据本发明的一个实施例发起 VoIP 电话呼叫的方法。

图 5 说明根据本发明的一个实施例执行 VoIP 电话呼叫的方法。

图 6 说明根据本发明的一个实施例在其中可实施语音归属代理的硬件环境。

具体实施方式

图 1 说明网络环境 100，在其中，可允许一个或多个移动节点 102 在地理上的大区域、例如在都市区域进行漫游。移动节点 102 经由数字传输(通常以 2 至 6 GHz 许可频带，其中典型信道带宽的范围是从 1.5 至 20 MHz)与接入点 104 通信。诸如由参考标号 104 标识的接入点(在本文中又称作基站)接收来自移动节点的传输，并把传输传递给关联区域接入网 106 中的网络单元。根据一个实施例，区域接入网 106 是一种有线网络(即，物理线路互连构成区域接入网的各个单元)，它是一般的基于分组的接入网，例如以太网网络、IP/MPLS 网络或 ATM 网络。接入点 104 与移动节点 102 之间的传输符合电气和电子工程师协会(IEEE)802.16 标准信号，IEEE std.802.16-2001，2001 年发布，以及以后的版本(以下称作 IEEE 802.16 标准或 IEEE 802.16e 标准)。互连符合 IEEE 802.16e 标准的接入点(如 104)的区域接入网 106 称作 WiMAX 网络。

在 WiMAX 区域接入网 106 的外围是无线电网络服务节点 108。无线电网络服务节点 108 提供其它 WiMAX 区域局域网、如参考标号 124 标识的 WiMAX 网络之间的路由选择和控制。各区域接入网 106

和 124 包括无线电网络服务节点(108,110),它把区域接入网 106 或 124 耦合到互连所有区域接入网 106 和 124 的 WiMAX 核心网 112。虽然 WiMAX 核心网 112 在图 1 中表示为互连两个 WiMAX 网络 106 和 124，但是 WiMAX 核心网 112 原则上可互连任何数量的区域接入网。

WiMAX 核心网 112 可以是普通 IP 网络，由常见的 IP 网络单元组成，例如允许高速数据传递的光组网单元。因此，WiMAX 核心网 112 可直接与因特网(图 1 中未示出)互连。

在 WiMAX 核心网 112 的外围是一个或多个语音归属代理 114 和 116。存在与各 WiMAX 区域接入网 106 和 124 关联的语音归属代理 114 或 116。下面详细论述语音归属代理 114 或 116 的结构或者由其制订的方法。简言之，语音归属代理是允许 WiMAX 核心网(例如核心网 112)与公共交换电话网(PSTN)126 之间的 VoIP 综合的网络单元。另外，语音归属代理提供允许移动节点(例如移动节点 102)从一个 WiMAX 区域接入网(例如网络 106)漫游到另一个(例如 124)的功能性。

虽然图 1 描绘了与各区域接入网 106 或 124 关联的单个语音归属代理 114 或 116，但是不止一个语音归属代理可与给定区域接入网关联。因此，虽然参考标号 114 和 116 在本文中用作表示单个语音归属代理，但是各参考标号 114 和 116 可理解为表示服务于它们相应的 WiMAX 区域接入网 106 和 124 的一组语音归属代理。

各语音归属代理 114 和 116 把 WiMAX 核心网 112 与公共交换电话网 126 的本地局 118 或 120 接口。公共交换电话网 126 采用由国际电信联盟(ITU)电信标准化部门(ITU-T)定义的、称作 7 号信令系统(SS7)的带外信令方案。带外信令方案对于呼叫控制采用与用于承载呼叫本身的内容(例如语音数据)不同的物理路径。因此，如图 1 所示，语音归属代理用作两个分开的接口：用于作为时域复用数字语音数据来传送的语音数据的接口，以及用于作为 SS7 分组来传送的 SS7 控制信号的接口。

诸如由参考标号 102 标识的移动节点之类的移动节点可被实施为电话手机(以与蜂窝电话相似的方式)，可被实施为个人数字助理，或者可被实施为另一个移动计算装置。一旦上电，移动节点就向最接近的可用接入点进行初始传输。在传输时，接入点为移动节点分配管理信道，它向接入点标识移动节点。接入点和移动节点可在范围从一至五或十英里的距离上与另一个进行通信。给定这种区域的大小，其它移动节点可位于其中。因此，接入点可与数百个移动节点进行通信。管理信道的使用允许接入节点区分不同的接入点。

WiMAX 区域接入网中的各接入点具有标识它的 IP 地址。但是，这个 IP 地址仅在接入点所在的区域接入网(又称作域)中才起作用。因此，接入点可直接向它所在的区域接入网中的另一个接入点发送数据。为了把数据导向另一个域中的接入点，服务于接入点所在的特定域的无线电网络服务节点必须用作中间件。

如上所述，在移动节点上电期间，为了建立管理信道并对用户鉴权，对基站进行初始传输。此后，移动节点与服务于移动节点所在的域的语音归属代理进行初始通信。这个通信标记登记过程的开始，移动节点通过它来通知语音归属代理关于移动节点在哪一个域中。作为响应，语音归属代理对移动节点分配称作移动 IP(MIP)地址的 IP 地址。语音归属代理还记录移动节点的转交地址。即使移动节点移动到它在其中与另一个接入点或者完全与另一个 WiMAX 区域接入网进行通信的地理区域，移动节点的 MIP 地址也不改变。另一方面，转交地址标识移动节点与之通信的域，因而在移动节点从一个区域接入网漫游到另一个区域接入网时会改变。

语音归属代理可对移动节点分配不止一个 IP 地址。例如，移动节点可具有分配给它的用于传送语音数据的一个 IP 地址以及分配给它的用于传送信令数据的另一个 IP 地址。为了简单起见，本公开以下列假设继续进行：各移动节点在登记期间具有分配给它的单一 IP 地址。

在登记时，语音归属代理更新它维护的数据库。数据库可包含与

移动节点所支持的特征(呼叫等待、语音邮件等)有关的信息。数据库经过更新以便关联用来标识移动节点的电话号码、分配给移动节点的MIP地址以及移动节点所在的域(即，移动节点的转交地址)。

WiMAX区域接入网106或124采用称作隧道技术的技术。利用这个技术，在给定WiMAX域106或124服务的地理区域内的移动节点的移动对于该域外部的网络单元或节点是透明的。因此，例如，WiMAX域106外部的网络节点无法知道移动节点102是否正与接入点104或接入点122进行通信。域106外部的网络单元仅需要知道，移动节点102处于域106中以便与移动节点102通信。因此，每当移动节点(例如移动节点102)从一个域移动到另一个域时，移动节点向它先前登记所用的语音归属代理重新登记。作为响应，语音归属代理更新其数据库，以便把新的转交地址(即，移动节点与之通信的域的网络地址)与该移动节点关联。

前面的论述集中于语音归属代理114或116工作的网络环境。以下论述简要地提供组成语音归属代理114或116的协议层。

图2说明语音归属代理114或116执行的协议栈200。从图2中可以看到，协议栈200包括移动IP(MIP)层202，它提供符合诸如“IP移动性支持”(C.Perkins, ed., IETF RFC 2002，1996年10月)中所述的标准之类的工业公认MIP标准的功能性。MIP层202提供的功能性可用于栈200的上层204－210。

MIP层提供以上所述的隧道技术功能性。图3说明接收具有IP首标302的分组300的MIP层202。IP首标302在其32位目标IP地址字段中包含分配给具体移动节点的MIP地址，因而称作IP首标$_{MIP}$。对接收这种分组300进行响应，MIP层202把分组300附接到第二IP首标304。第二IP首标采用MIP地址标识的具体移动节点的转交地址，因而称作IP首标$_{CareOf}$。因此，WiMAX核心网112观察第二IP首标304，并按照第二IP首标304来路由分组300，表示分组300被路由到适当的域106或124。在由移动节点接收之前，第二IP首标304

被去掉。

参照图 3 所述的隧道技术的作用在于，各移动节点接收包含在登记过程中分配给它的 MIP 地址的 IP 分组。因此，各移动节点可在保留登记过程中分配给它的 IP 地址的同时漫游－甚至在域之间漫游。

隧道技术的许多层可用于图 1 所示的网络环境 100。例如，各 WiMAX 区域接入网 106 和 124 可采用隧道技术，使得设置在域外部的单元仅需要把 IP 分组送往适当域，以便让分组到达预期移动节点。

再来看图 2，可以看到，协议栈 200 还包括提供基于 IP 的语音功能性的 VoIP 层 204，基于 IP 的语音功能性可符合工业公认 VoIP 标准，诸如 IETF RFC 1889 定义的实时传输协议(RTP)和/或 IETF RFC 2326 定义的实时流式传播协议(RTSP)。简言之，VoIP 层 204 接收 VoIP 分组，并把那些分组变换为用于公共交换电话网(PSTN)118 和 120 的时域复用数字语音数据，反过来也是一样。如下面所述，在移动节点的用户与 PSTN 的用户之间的论述的上下文中，VoIP 层 204 把时域复用数字数据转换为 VoIP 分组。VoIP 分组包含分配给具体移动节点的 MIP 地址。VoIP 分组被传递给 MIP 层 202，MIP 层 202 把 VoIP 分组附接到包含具体移动节点的转交地址的 IP 首标。

协议栈 200 还包括会话发起协议层 206，它提供可能符合工业公认标准、如 IETF RFC 3261 的 SIP 功能性。简言之，SIP 层 206 提供用于创建、修改和终止与一个或多个参与方的通信会话的应用层控制功能性。例如，SIP 层 206 包含发信号通知移动节点关于另一方希望与其通信的功能性。

协议栈 200 还包括与 PSTN 接口的层 210。层 210 包括把时域复用语音数据转换为 IP 分组的媒体网关(MGW)。它还包括 SS7 接口，SS7 接口接收 SS7 信号，对信号解码，以及把所提取信息传递给语音归属代理控制平面 208。

语音归属代理控制平面 208 协调其它层的动作。它在主要网关与 VoIP 层 204 之间协调通信，并且还在 SS7 接口与 SIP 层 206 之间协调

通信。例如，语音归属代理控制平面 208 可从 SS7 接口 210 接收表明需要到具体电话号码的连接的信号。作为响应，控制平面 208 调用 SIP 平面 206 向对应于该电话号码的移动节点发送 SIP 邀请消息。类似地，控制平面 208 在具体时隙中接收语音数据，并且把数据转发给 VoIP 层，用于转换为 VoIP 分组以及用于传递给具体移动节点(这样，维持语音路径)。

前面的论述简要提供组成语音归属代理 114 或 116 的协议层 202-210。与关于呼叫发起和呼叫执行的语音归属代理 114 或 116 的操作相关的论述如下。这个论述总体(与基于逐层相对)描述语音归属代理的操作，并提供语音归属代理的操作的高级综合视图。

图 4 描绘在对移动节点发起电话呼叫的过程中语音归属代理 114 或 116 的操作。该过程可由 PSTN 的用户或者由语音归属代理 114 或 116 服务的移动节点的用户发起。如果该过程由 PSTN 的用户发起，则语音归属代理 114 或 116 接收表明希望与具体电话号码标识的移动节点进行电话呼叫的 SS7 信号，如操作 400 中所示。电话号码从 SS7 信号中提取(操作 400)。SS7 信号被转换为邀请消息(操作 400)，它是表明希望通信会话的 SIP 消息。因此，在操作 400 完成时，语音归属代理 114 或 116 已经构造送往具体电话号码的邀请消息。

另一方面，该过程可能由语音归属代理 114 或 116 服务的移动节点发起。当移动节点发起电话呼叫时，移动节点把送往所选电话号码的 SIP 邀请消息发送给语音归属代理 114 或 116。这个 SIP 邀请消息由语音归属代理接收，如操作 402 所示。

无论 SIP 邀请消息被接收(如移动节点发起电话呼叫时的情况)还是被语音归属代理创建(如 PSTN 的用户发起电话呼叫时的情况)，操作流程随后进入操作 404。在操作 404 中，语音归属代理查询数据库以标识与嵌入邀请消息的电话号码关联的 MIP 地址和转交地址。

如果在操作 404 中标识的电话号码对应于由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 采用参照图 3 所述的隧道

技术向移动节点发送 SIP 邀请消息(操作 406)。

如果在操作 404 中标识的电话号码对应于不是由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 向服务于与被邀请移动节点对应的域的语音归属代理 114 或 116 发送 SIP 邀请消息(操作 408)。

如果电话号码表明，电话号码表示由 PSTN 服务的电话装置，则邀请消息被转换为 SS7 信号，以便在 PSTN 上发起电话呼叫(操作 410)。

在已经发送邀请消息(通过 SIP 邀请消息或者通过 SS7 信号)之后，语音归属代理 114 或 116 等待对邀请消息的响应，如操作 412 所示。如果被邀请电话装置的用户希望应答电话呼叫，则表明这种希望的响应由语音归属代理 114 或 116 接收(操作 412)。如果响应从移动节点始发，则响应可通过 SIP 确认(ack)消息的形式到达语音归属代理 114 或 116。另一方面，如果响应从 PSTN 电话装置始发，则响应可通过可被转换为 SIP ack 消息的 SS7 信号的形式到达语音归属代理 114 或 116。

在响应被接收之后，它被转发给发起方(操作 414)。如果电话呼叫的发起方为移动节点，则转发操作包括使用 MIP 层 202 把响应发送给移动节点，以便采用参照图 3 所述的隧道技术。另一方面，如果电话呼叫的发起方是 PSTN 上的电话装置，则响应被转换为 SS7 信号，并通过 SS7 接口 210 导向到 PSTN。

最后，假定在操作 412 接收的响应表明被邀请移动节点的用户希望参与通信会话(即希望应答呼叫)，则建立邀请与被邀请装置之间的语音路径(操作 416)。建立语音路径可包括把来自 PSTN 本地局 118 或 120 的时域复用语音数据中的具体时隙与具体 MIP 地址关联(反之亦然)。另外，还可包括把移动节点的 MIP 地址与服务于具体移动节点的语音归属代理 114 或 116 的转交地址或地址关联。

在已经建立 VoIP 会话之后(如图 4 所示)，各方可相互通话。在各

方通话时，语音归属代理 114 或 116 接收 VoIP 分组或者来自 PSTN 的时域复用语音数据，如图 5 的操作 500 所示。如果语音归属代理接收来自 PSTN 的时域复用语音数据，则这种数据被转换为 VoIP 分组，如上所述。

随后，如操作 502 所示，VoIP 分组或语音数据沿图 4 的操作 416 中建立的语音通路发送。在向移动节点发送 VoIP 分组的情况中，这可表示把所接收 VoIP 分组发送给服务于移动节点的语音归属代理 114 或 116，或者可表示采用参照图 3 所述的隧道技术把所接收 VoIP 分组直接发送给移动节点。在向 PSTN 上的电话装置发送语音数据的情况中，操作 502 包括把 VoIP 数据转换为时域复用数字语音数据，并把这种语音数据插入到适当的时隙，使得 PSTN 交换设备把数据路由到适当的位置。

前面的论述涉及电话呼叫的发起和执行期间的语音归属代理的操作。以下论述从系统级的角度陈述在图 1 所示的网络环境 100 的上下文中的电话呼叫的发起和执行。

在 PSTN 电话装置(呼叫的发起方)与移动节点(呼叫的应答方)之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理 114 或 116 接收表明希望与对应于给定电话号码的移动装置进行通信会话的 SS7 信号。语音归属代理提取电话号码，并创建送往被邀请移动节点的 MIP 地址的 SIP 邀请消息。(如果被邀请移动节点不可用，则呼叫可被重新路由到语音邮件服务。)

通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。同时，语音归属代理 114 或 116 向邀请电话装置发送产生回铃音的 SS7 信号。

如果移动节点的用户接受该呼叫，则 SIP 确认消息被发送给语音归属代理 114 或 116。语音归属代理 114 或 116 把 SIP 确认消息转换为

SS7 信号，并建立语音路径。这时，PSTN 电话装置和移动节点的用户开始通话。

在两个移动节点(在不同的域中)之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理接收来自邀请移动节点的 SIP 邀请消息。SIP 邀请消息被送往与预期移动节点对应的电话号码。作为响应，语音归属代理把 SIP 邀请消息转发给服务于被邀请移动节点所在的域的语音归属代理。后一个语音归属代理向被邀请移动节点的 MIP 地址发送响应。

通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。此外，邀请移动节点的 IP 地址包含在 SIP 邀请消息中。

如果被邀请移动节点的用户接受该呼叫，则 SIP 确认消息被发送给服务于被邀请移动节点所在的域的语音归属代理 114 或 116。作为响应，语音归属代理 114 或 116 把 SIP 确认消息转发给服务于邀请移动节点所在的域的语音归属代理 114 或 116。后一个语音归属代理 114 或 116 把 SIP 确认消息转发到邀请移动节点的 MIP 地址。SIP 确认消息包含被邀请节点的 IP 地址。

语音通信这时可通过两种方式之一进行。首先，移动节点可相互通信而无需语音归属代理的介入。这是可行的，因为通过 SIP 邀请和确认消息，各移动节点知道另一个的 IP 地址。但是，如果移动节点中的任一个漫游到不同的域，则两个移动节点之间的连接将丢失。

其次，语音路径可在两个语音归属代理之间延伸。这个方案允许移动节点中任一个从一个域漫游到另一个域。

图 6 描绘其中可实施语音归属代理 114 或 116 的硬件环境。该环境包括四个刀片 600、602、604 和 606。各刀片包含它自己的计算环境，其中包括处理器、存储器以及提供对网络接口或存储装置的访问

的输入/输出模块(例如，控制集线器和I/O总线)。各刀片600－606可经由局域网、例如经由以太网集线器进行通信。刀片600-606可被实施为可安装在机架中的薄板。

各刀片可专用于执行先前所述的控制平面功能或数据平面功能的各种小方面。例如，刀片602可执行与MIP层202相关的功能。这个刀片602还执行在接收到VoIP分组并且需要被路由到另一个语音归属代理或者移动节点时所需的路由功能性，如上所述。刀片602包括允许在其中运行的软件/固件与WiMAX核心网112进行通信的网络接口。

刀片604可执行以上参照图2中所述的VoIP层204所描述的VoIP功能性。刀片604包括允许在其中运行的软件/固件与来自PSTN的时域复用数字语音数据交互的时域复用接口。

刀片606可对SS7信号解码，并把所提取内容发送给驻留在刀片600上的SS7应用层功能性。刀片606包括允许在其中运行的软件/固件与来自PSTN本地局的SS7分组交互的SS7接口。

刀片600可执行如上所述的语音归属代理控制平面功能性。为此，该刀片包括存储装置(以便维护为执行这种功能性所必需的数据库)。刀片600还执行SS7子系统的SIP功能性和应用层功能性。在一个实施例中，刀片600执行计费例程。计费例程可根据逐个用户或逐个帐户来跟踪给定用户连接到网络的时间量、用户消耗的业务量、用户消耗的服务的类型(本地呼叫、长途呼叫等)或者用户消耗的带宽。所跟踪信息可存储在数据库中，以及可从其中产生定期帐单。

本发明的实施例可通过硬件、固件和软件其中之一或者它们的组合来实现。本发明的实施例还可实现为存储于机器可读媒体中的指令，所述指令可由至少一个处理器读取和运行，以便执行本文所述的操作。机器可读媒体可包括用于存储或传送机器(例如计算机)可读形式的信息的任何机构。例如，机器可读媒体可包括：只读存储器(ROM)，随机存取存储器(RAM)，磁盘存储媒体，光存储媒体，闪速

存储装置，电、光、声或其它形式的传播信号(例如载波、红外信号、数字信号等)，等等。

摘要是根据要求摘要以允许读者确定技术公开的性质和要点的37 C.F.R.第 1.72(b)节来提供的。应当理解，它的提供并不是用于限制或解释权利要求的范围或含意。

在前面的详细描述中，各种功能有时集中到单一实施例中，用于简化本公开。这种公开的方法不应解释为反映了要求其权益的主题的实施例要求超过各权利要求中明确陈述的特征的意图。相反，如以下权利要求所反映的那样，本发明主题在于少于单个公开实施例的全部特征。因此，以下权利要求由此结合到详细描述中，其中各权利要求本身代表单独的优选实施例。

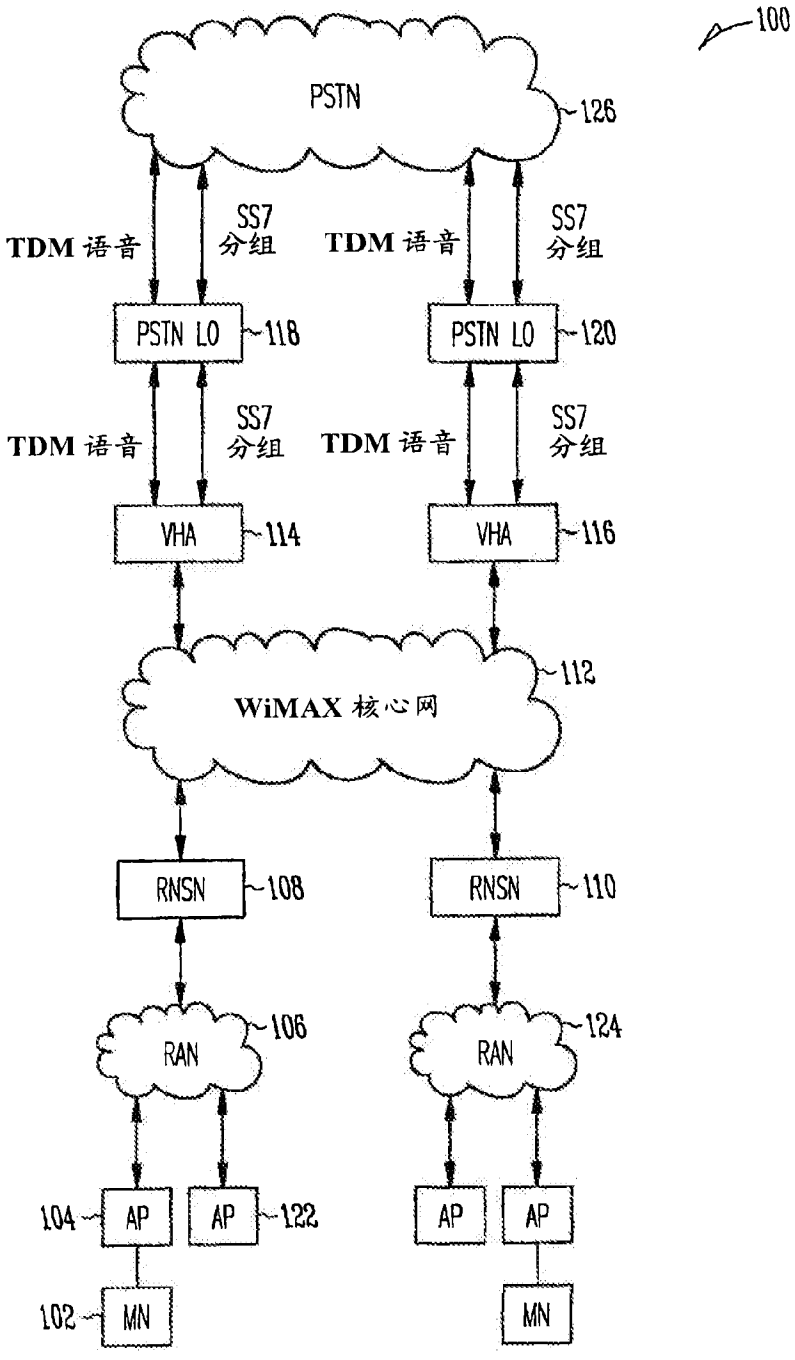


图 1

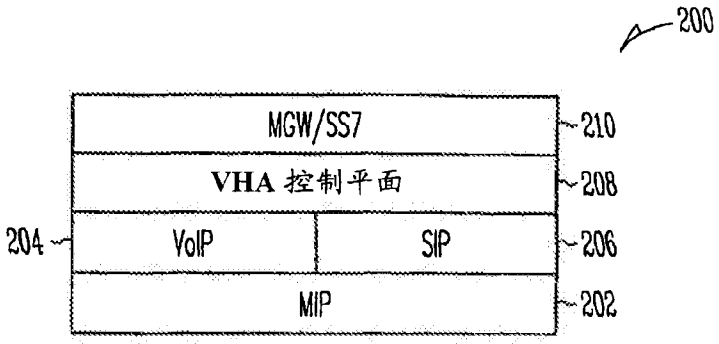


图 2

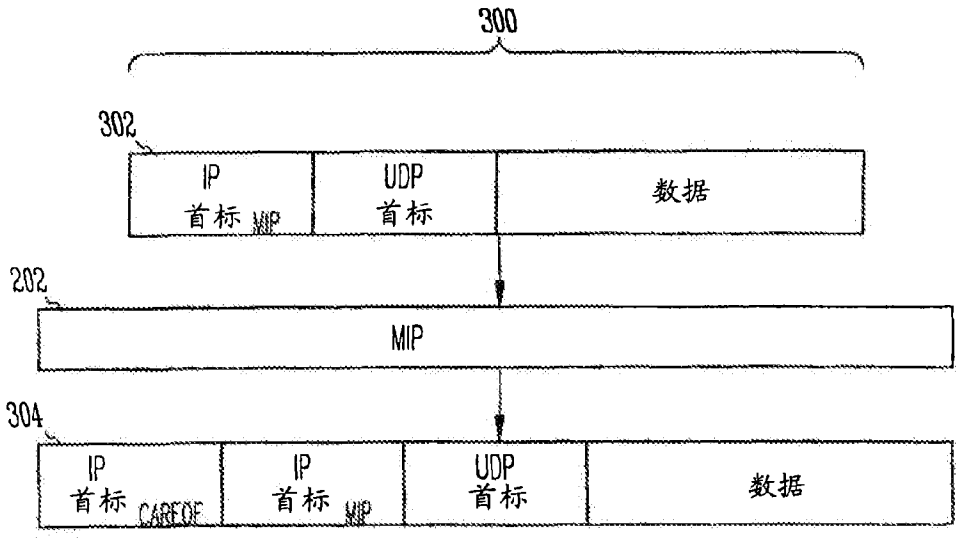


图 3

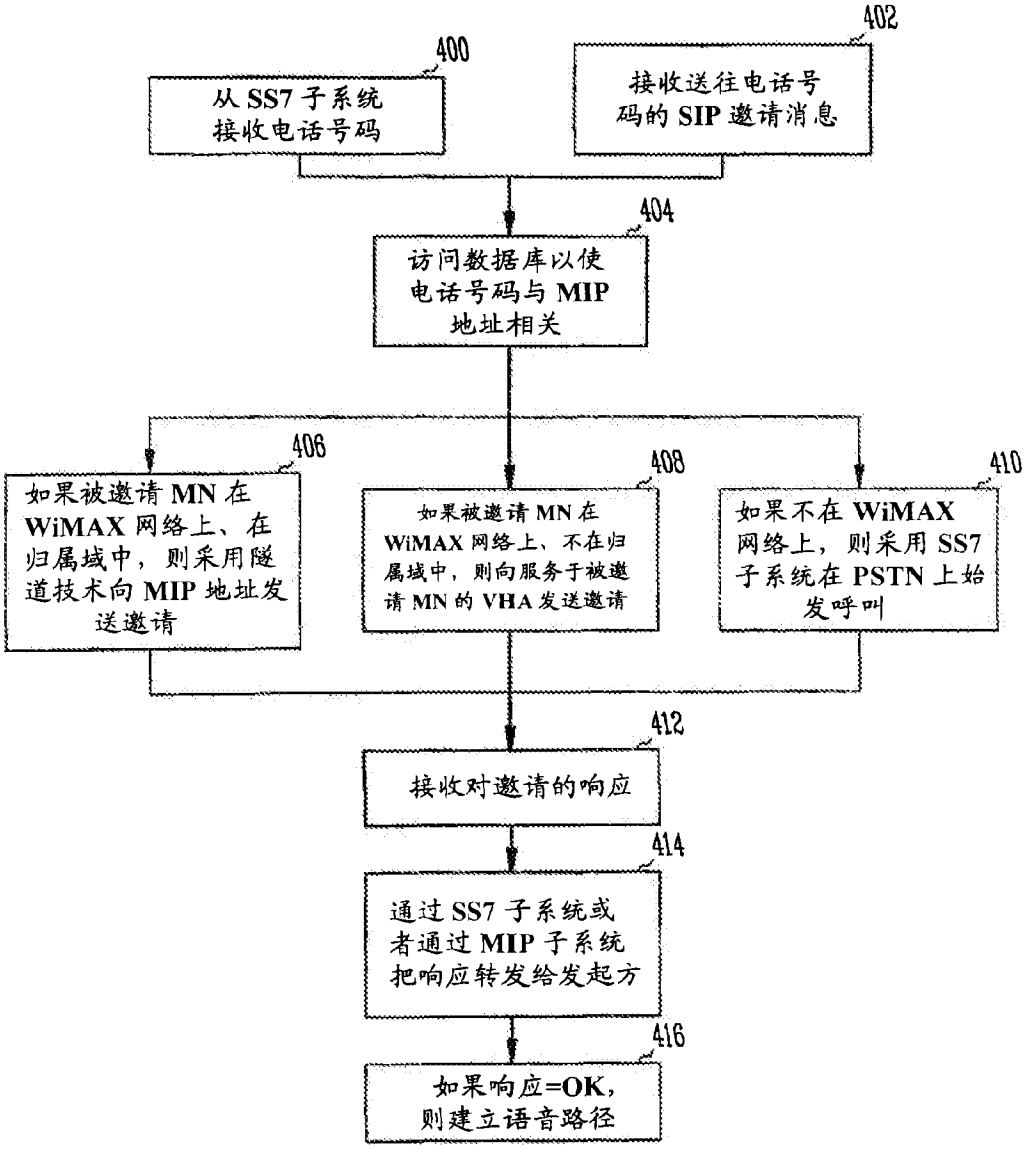


图 4

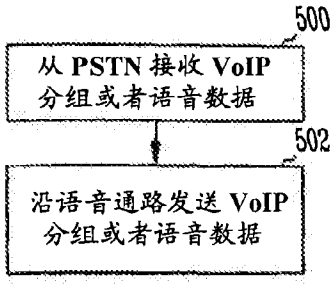


图 5

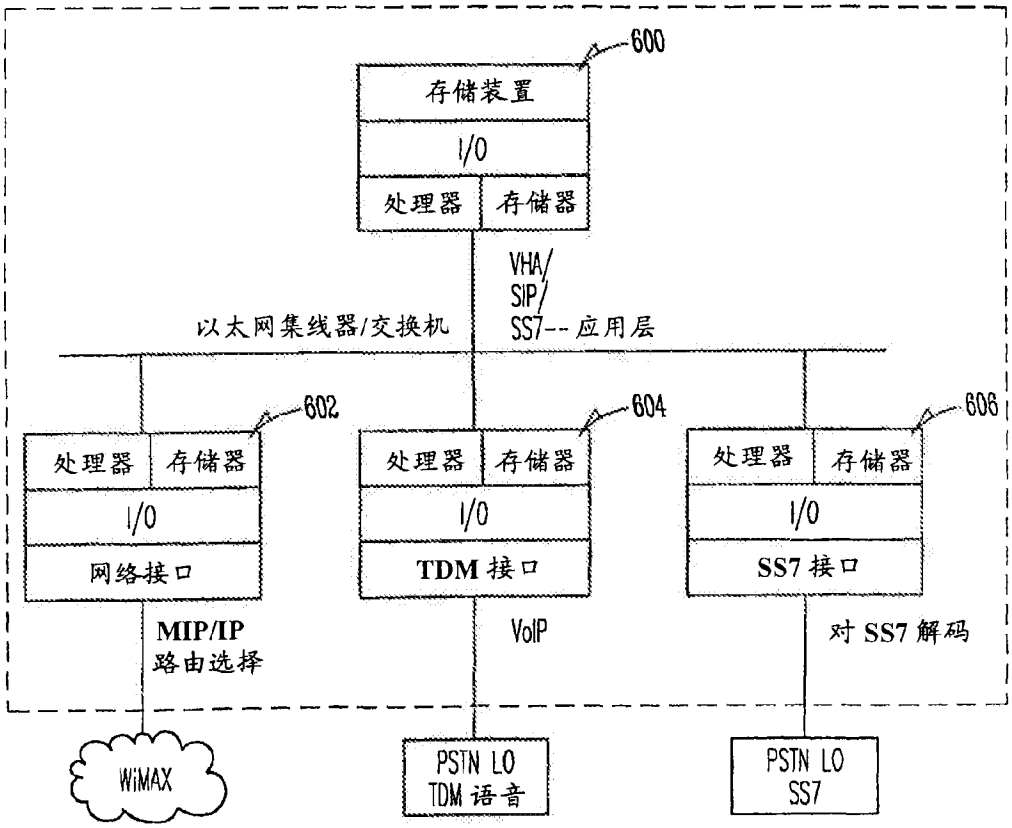


图 6

Espacenet

Bibliographic data: CN1498029 (B) — 2010-05-12

Emergency call-back method

Inventor(s): CHEN MARRY W; ROLAND DOUGLAS H ± (MARRY W. CHEN, ; DOUGLAS H. ROLAND)

Applicant(s): LUCENT TECHNOLOGIES INC ± (LUCENT TECHNOLOGIES INC)

Classification: **- international:*H04B7/26; H04M1/26; H04M3/42; H04W4/16; H04W4/22; H04W76/00; H04W76/02***
- cooperative: H04W4/22; H04W76/007

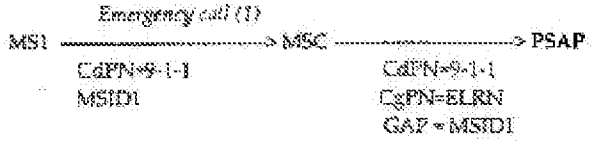
Application number: CN20031101083 20031015

Priority number(s): US20020270629 20021016

Also published as: CN1498029 (A) EP1411743 (A1) EP1411743 (B1) US2004203565 (A1) US7676215 (B2) KR20040034410 (A) KR101010868 (B1) JP2004140838 (A) JP4335636 (B2) ES2295524 (T3) DE60317751 (T2) AT379940 (T) less

Abstract of CN1498029 (B)

Fig. 1



An emergency routing number is assigned to each switch in a wireless network. When a switch of the wireless network routes an emergency call to a Public Service Answering Point (PSAP), the switch sends the emergency routing number as the calling party number and provides the PSAP with the identifier of the mobile station. If the emergency call drops, the PSAP performs a call back using the emergency routing number as the called party number. The switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. When a switch receives its emergency routing number as the called party number, the switch recognizes an emergency call back situation and pages the mobile station identified by the mobile station identifier received in association with the emergency routing number.; The mobile station is then reconnected with the PSAP.

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1498029 B
(45)授权公告日 2010.05.12

(21)申请号 200310101083.5

(22)申请日 2003.10.15

(30)优先权数据
10/270,629 2002.10.16 US

(73)专利权人 朗迅科技公司
地址 美国新泽西州

(72)发明人 玛丽·W·陈 道格拉斯·H·罗兰德

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华 黄倩

(51)Int.Cl.
H04W 76/00(2009.01)
H04M 1/26(2006.01)
H04M 3/42(2006.01)

(56)对比文件
CN 1225217 A,1999.08.04,说明书1－7页、权利要求1－16.
US 005689548 A,1997.11.18,说明书第1－6栏、权利要求1－23、附图3.
WO 0011879 A,2000.03.02,第四页第十二行到第二十六行.

审查员 林燕琼

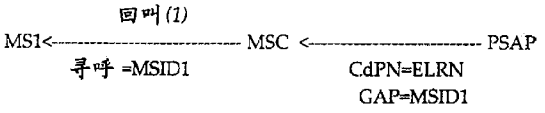
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

应急回叫方法

(57)摘要

对无线网内的每个交换机分配一个应急路由选择号码。在无线网内的交换机使应急呼叫路由选择到公用业务应答中心(PSAP)时,该交换机发送所述应急路由选择号码作为主叫方号码,并将移动台的标识符送到PSAP。如果应急呼叫中断,则PSAP利用所述应急路由选择号码作为被叫方号码进行回叫。使应急呼叫从移动台路由选择到PSAP的交换机接收该回叫。PSAP还将移动台标识符发送到该交换机。在交换机接收作为被叫方号码的其应急路由选择号码时,该交换机识别应急回叫情况,并寻呼利用与应急路由选择号码相关接收的移动台标识符识别的移动台。然后,该移动台重新连接到该PSAP。



CN 1498029 B

1. 一种应急回叫方法，所述应急回叫方法包括：

对无线网内的每个交换机分配一个不同的应急路由选择号码，用作通过每个交换机路由选择到公用业务应答中心 PSAP 的各应急无线呼叫的主叫方号码，使得在一个呼叫中作为被叫方号码接收到对其分配的应急路由选择号码的每个交换机将所述呼叫识别为应急回叫。

2. 根据权利要求 1 所述的方法，其中分配的每个应急路由选择号码是不可移植的。

3. 一种应急回叫方法，所述应急回叫方法包括：

发送无线网内一个用于处理发出应急呼叫的移动台的通信需要的交换机的应急路由选择号码和所述移动台的标识符到公用业务应答中心 PSAP，使得在一个呼叫中作为被叫方号码接收到对其分配的应急路由选择号码的所述交换机将所述呼叫识别为应急回叫。

4. 一种应急回叫方法，所述应急回叫方法包括：

在公用业务应答中心 PSAP 接收无线网内一个用于处理发出应急呼叫的移动台的通信需要的交换机的应急路由选择号码和所述移动台的标识符；以及

在所述移动台发出的应急呼叫中断时，在 PSAP 处通过呼叫所述应急路由选择号码向所述交换机发出回叫，使得在一个呼叫中作为被叫方号码接收到对其分配的应急路由选择号码的所述交换机将所述呼叫识别为应急回叫，并且在所述 PSAP 处向所述交换机发送所述移动台的标识符，以便所述交换机根据所述移动台的标识符将所述回叫发送到所述移动台。

5. 根据权利要求 4 所述的方法，所述方法进一步包括：

在发出回叫时，将所述移动台的标识符发送到所述交换机。

6. 根据权利要求 5 所述的方法，其中所述发送步骤在通用地址参数中发送所述移动台的标识符。

7. 一种应急回叫方法，所述应急回叫方法包括：

在无线通信系统的一个交换机接收被叫方号码和移动台标识符，使得在一个呼叫中作为所述被叫方号码接收到对其分配的应急路由选择号码的所述交换机将所述呼叫识别为应急回叫；以及

当所述被叫方号码与对所述交换机分配的应急路由选择号码匹配时，寻呼由所述移动台标识符识别的移动台。

8. 根据权利要求 7 所述的方法，其中所述接收步骤在通用地址参数中接收所述移动台标识符。

9. 根据权利要求 7 所述的方法，其中在所述交换机处以比其它任务高的优先级执行所述寻呼步骤。

10. 根据权利要求 7 所述的方法，其中所述交换机是移动交换中心。

应急回叫方法

背景技术

[0001] 在北美地区，通过拨“9-1-1”发出应急业务呼叫。世界上的其他地区可能使用某个其他简化可拨号数字串，例如在墨西哥使用“6-1-1”，它们的共同之处是意在有助于主叫用户利用容易记忆的数字以简单方式进行呼叫以寻求帮助。这些呼叫路由选择到本地公用业务应答中心 (Public Service Answering Point，PSAP)，在这里，在主叫用户通话的同时，可以启动应急响应（警察、消防队、公路抢修、救护车等）。如果在完全报告紧急情况之前或响应者到达之前该呼叫由于某种原因断线或中断，则 PSAP 可以利用其数据库提供的回叫号码回叫始发者。

[0002] 例如，通过有线网始发 911 呼叫的呼叫记录可以包括自动线路标识 (ANI) 或通过其始发呼叫的用户接入线的电话号码。然而，无线用户的移动电话薄号码 (MDN) 或电话号码与物理线路或移动台不相关。不是利用 MDN，而是利用移动台标识 (MSID)，将对无线用户的呼叫路由选择到移动台。因此，对移动台进行应急回叫遇到了用例如陆线设备不会遇到的障碍。

[0003] 通常，MSID 是由移动台用户已经与其达成业务协议的业务提供商编程到移动台内的 10 位数字移动标识号码 (MIN) 或 15 位数字国际移动用户标识符 (IMSI)。因此，MSID 不必是可拨号号码。

[0004] 移动台的 MDN 是可拨号号码。主叫用户拨 MDN，并利用 MDN 通过网络使呼叫路由选择到无线用户的归属系统。在用户的归属系统，归属位置寄存器 (HLR) 含有与用户的 MDN 相关的 MSID。然后，不利用 MDN，而利用 MSID，通过网络使呼叫路由选择到在服务无线系统并寻呼该用户。归属系统将用户的 MDN 在一个被称为用户概况的单独数据文件中提供给在服务系统。

[0005] 对 MDN 和 MSID 使用单独号码对于某些系统是新的。历史上，在 TIA/EIA-41 系统中，在根据本地路由选择号码 (LRN) 方法和国际漫游 (IR) 实现无线号码可移植性 (WNP) 或成千块号码汇集 (TBNP) 之前，移动台的移动标识号码 (MIN) 与 MDN 相同。然而，利用 WNP 和 TBNP，MDN 变得可以从一个业务提供商“移植”或“汇集”到另一个业务提供商。由于 MSID 不可移植或汇集，所以接收者业务提供商对用户分配带有被植入或被汇集的 MDN 的新 MSID。

[0006] 国际漫游也迫使 MSID 与 MDN 分离。尽管 MIN 是按照北美编号方案的 10 位数字 MDN 编制的 10 位数字号码，但是采用不同电话薄编号方案的其他国家的电信公司可能不允许其 MDN 等效于国际识别的 MIN 格式。另一个标准 MSID 是 IMSI。它用于世界各地的 TIA/EIA-41 系统和 GSM 系统。IMSI 是 15 位数字号码，因此，不能用作 10 位数字的 MDN。

[0007] 历史上，在 MDN 与 MIN 相同时，MIN 可被传送到 PSAP，而且可以用作回叫号码。如上所述，如果将 MIN 与 MDN 分离，就必须将 MDN 作为单独回叫号码与主叫用户的 MSID 一起传送到 PSAP。存在某些与实现该解决方案相关的问题。主要问题是，在服务系统可能仅使 MSID 与呼叫一起传送到 PSAP，而不使主叫用户的 MDN 传送到 PSAP。其中一些原因与根据标准实现 MSID-MDN 分离的方式相关。

[0008] 老式在服务 TIA/EIA-41 系统可能不支持 WNP、TBNP 或 IR。这意味着，老式在服务

系统可能希望 MIN 与 MDN 相同。更老式系统甚至可能不知道在用户业务概况（不是以 MDN 而是以 MIN 为关键字的）中查找单独的 MDN。因为该限制，可以不允许这些用户使用基本业务，但是必须允许他们呼叫应急业务。因此，通过老式系统拨“9-1-1”的漫游用户将使他或她的呼叫带有 MSID 而没有 MDN 传送到 PSAP。因此，不可能进行回叫。

[0009] 一个支持 WNP 和 LR 的新式在服务系统可能不能将 MDN 传送到 PSAP。如果主叫移动台未注册到任何业务提供商（例如，存在仅用于应急呼叫的移动电话机），可能发生这种情况。此外，用户还可以在 HLR 利用含有 MDN 的用户业务概况响应在服务系统之前发出应急呼叫。

[0010] 国际漫游用户的回叫 MDN 可以要求 PSAP 发出国际呼叫以传送到其本地应急业务区 (ESZ) 内的用户。对于通常不发出国际呼叫而且为了挽救某人的生命可能需要立即回叫信息的 PSAP，这不是一个实用的、及时的或充分可靠的解决方案。此外，不能将全部国际 MDN（多至包括国家代码的 15 位数字）送到 PSAP 用于回叫。

[0011] 对这些问题的一种已建议的解决方案要求，在 MDN 不可用时，将 9-1-1+ 主叫移动台的电子序列号 (ESN) 的后 7 位传送到 PSAP，作为回叫号码。尽管这可以用于对 PSAP 和在服务系统识别主叫用户，但是不能通过网络路由选择该“9-1-1+ESN7”，而且该“9-1-1+ESN7”不能用于发出回叫。

发明内容

[0012] 根据本发明的回叫方法对无线网内的每个交换机分配一个应急本地路由选择号码 (ELRN)。在无线网内的一个交换机使应急呼叫路由选择到公用业务应答中心 (PSAP) 时，该交换机发送其应急本地路由选择号码作为主叫方号码 (CgPN)，并将移动台的标识符 (MSID) 送到 PSAP。如果应急呼叫中断，则 PSAP 利用所述应急路由选择号码作为被叫方号码 (CdPN) 进行回叫。结果，使应急呼叫从移动台路由选择到 PSAP 的交换机接收该回叫。PSAP 还将该移动台的标识符发送到该交换机。该 MSID 用于寻呼正确的移动台。在本发明的一个实施例中，PSAP 在通用地址参数中将移动台标识符发送到交换机。

[0013] 在交换机接收作为被叫方号码的其应急本地路由选择号码时，该交换机识别应急回叫情况，并寻呼利用与该应急路由选择号码相关接收的移动台标识符识别的移动台。在本发明一个实施例中，在一个 ELRN 是所述 CdPN 时，交换机对处理回叫赋予的优先级比处理其他任务的优先级高。这样，PSAP 与该移动台重新连接在一起。

附图说明

[0014] 根据以下对本发明所做的详细说明以及仅作为示例用的附图，可以更全面地理解本发明，其中对各附图中的相应部分指定类似的参考编号，附图包括：

[0015] 图 1 至 6 是示出根据本发明的回叫方法的运行过程的通信流程图。

具体实施方式

[0016] 根据本发明的回叫方法对无线通信系统内的每个交换机（例如，移动交换中心 (MSC)）分配唯一可路由选择的回叫号码。以下将该号码称为“应急本地路由选择号码”或 ELRN。可以认为 ELRN 与为了实现无线号码可移植性 (WNP) 或成千块号码汇集 (TBNP) 而对

每个本地交换机分配的本地路由选择号码 (LRN) 类似。然而，ELRN 可以仅路由选择到拥有该号码的交换机，每个交换机的 ELRN 是唯一的，而且是不可移植的。

[0017] 我们知道，在移动台进行应急呼叫时，提供与应急呼叫相关的移动台标识符 (MSID)。例如，MSID 是移动标识号码 (MIN)、用于那些不属于北美编号方案范围的 10 位数字号码的 10 位数字国际漫游移动标识号码 (IRM)、或国际移动用户标识符 (IMSI)。在无线系统的一个交换机接收来自移动台特别是没有 MDN 的移动台的应急呼叫 (例如，9-1-1 呼叫) 时，该交换机将该交换机的 ELRN 发送到服务该交换机的公用业务应答中心 (PSAP)。该交换机提供 ELRN 作为主叫方号码 (CgPN)，而且还将移动台的 MSID 提供给 PSAP。例如，在 ISUP 通用地址参数 (GAP) 中发送 MSID。

[0018] 如果应急呼叫中断，则 PSAP 利用 ELRN 作为被叫方号码 (CdPN) 进行回叫。结果，已将应急呼叫从移动台路由选择到 PSAP 的交换机接收该回叫。PSAP 还将该移动台的标识符发送到该交换机。例如，与回叫一起诸如在 ISUP 通用地址参数 (GAP) 中发送 MSID。

[0019] 在交换机接收作为被叫方号码的其应急路由选择号码时，该交换机识别应急回叫情况，并寻呼利用与 ELRN 相关接收的 MSID 识别的移动台，然后，建立应急回叫。这种 ELRN 技术还可以在交换机中具有优先级排队，其中交换机以比其他呼叫任务高的优先级处理回叫号码。这样，即使在该交换机的业务高峰期，仍可以提高应急回叫的接通率。此外，尽管对所有应急呼叫进行了描述，但是使用该方法可以仅局限于由没有 MDN 或 MDN 不可用的移动台发出的应急呼叫。

[0020] 图 1 至 6 是根据本发明的回叫方法的运行过程的通信流程图。如图 1 所示，第一移动台 MS1 发出应急呼叫，在该例中为 9-1-1，MSC 接收该应急呼叫。因此，被叫方号码是 9-1-1，而且还将第一移动台 MS1 的 MSID1 送到 MSC。然后，MSC 使该应急呼叫路由选择到在服务 PSAP。在这样做的过程中，被叫方号码保持 9-1-1，而 MSC 提供其 ELRN 作为主叫方号码。MSC 还在通用地址参数 (GAP) 中提供第一移动台 MS1 的 MSID1。

[0021] 如果应急呼叫中断，则 PSAP 利用该 ELRN 作为被叫方号码进行回叫，因为该 ELRN 已被送到 PSAP 作为主叫方号码。结果是使回叫路由选择到 MSC，如图 2 所示。如图 2 进一步所示，与回叫一起在 ISUP GAP 中发送第一移动台的 MSID1。如图 3 所示，MSC 利用第一移动台 MS1 的 MSID1 寻呼第一移动台 MS1 并接通该回叫。

[0022] 假定在正在回叫第一移动台 MS1 时，第二移动台 MS2 发出 9-1-1 应急呼叫，如图 4 所示。与第一移动台 MS1 发出应急呼叫的情况一样，第二移动台 MS2 一起发送其移动台标识符 MSID2 和应急呼叫 (例如，被叫方号码为 9-1-1)。然后，MSC 使应急呼叫路由选择到 PSAP。在这样做的过程中，被叫方号码保持 9-1-1，而 MSC 提供其 ELRN 作为主叫方号码。MSC 还将第二移动台 MS2 的 MSID2 送到 PSAP。因此，图 4 示出 MSC 将同一个主叫方号码 (即，ELRN) 送到 PSAP 用于这两个应急呼叫。

[0023] 如果第二应急呼叫中断，则 PSAP 利用 ELRN 作为被叫方号码进行回叫，因为该 ELRN 已被送到 PSAP 作为主叫方号码。结果是使第二回叫路由选择到 MSC，如图 5 所示。如图 5 进一步所示，与第二回叫一起在 ISUP GAP 中发送第二移动台的 MSID2。如图 6 所示，MSC 利用第二移动台 MS2 的 MSID2 寻呼第二移动台 MS2 并接通该回叫。

[0024] 根据本发明的应急回叫方法确保连同来自移动台的每个应急呼叫将一个可路由选择的回叫号码提供给 PSAP。具体地说，ELRN 是一个用于使一个或者多个应急业务回叫路

由选择到始发交换机（例如，MSC）的号码。特别是在没有可用于伴随应急呼叫的本地 MDN 时，将始发交换机的 ELRN 发送到 PSAP 作为主叫方号码（CgPN）。

[0025] 在北美编号方案中，ELRN 是 10 位数字号码（NAP-NXX-XXXX），其中头 6 位数字（NAP-NXX）是为了进行路由选择而对北美地区的每个本地交换机唯一分配的。后面的 4 位数字是交换机运营商分配的。然而，所述应急回叫方法可以应用于位于世界各地的公用交换网。也就是说，ELRN 含有为了使呼叫路由选择到特定交换机而根据任何国家编号方案分配的数字。此外，可以连同任何移动业务或无线接入技术，应用应急回叫方法。

[0026] 该应急回叫方法与号码可移植性和号码汇集无关。这些网络能力取决于根据与移植的或汇集的拨号号码相关的 LRN，使呼叫路由选择到在服务交换机的本地路由选择号码（LRN）方法。与之相比，ELRN 与拨号号码无关，而与交换机相关。

[0027] 从某种意义上说，ELRN 在公用网内的作用类似于为本地号码可移植性要求的本地路由选择号码（LRN），例如，它们二者均可以作为使许多呼叫路由选择到特定交换机的单一号码。然而，不要求进行数据库查询以识别使呼叫路由选择到在服务 MSC 所需的 ELRN。因此，在用作使回叫从 PSAP 路由选择到在服务 MSC 的被叫方号码（CdPN）时，ELRN 可以附带为了指出不需要进行号码可移植性数据库查询而设置的 ISUP 前向呼叫指示符（FCI）。

[0028] 如上所述，ELRN 与任何特定 MDN 不相关，它用于使回叫直接路由选择到在服务交换机，而非归属系统。ELRN 使得不需要 PSAP 利用 MDN 进行应急回叫。不需要为了通过归属系统路由选择回叫，而根据现有移动通信应用部分（MAP）标准请求 MDN 或 LRN。此外，还不需要通过区外归属系统发送国际呼叫来回叫本地区内的国际漫游用户。这样就减少了信令，节省了时间而且提高了业务的可靠性。此外，不象在 TIA/EIA-41 网内那样需要临时长途号码（TLDN），或者不象在 GSM 网内那样需要移动台路由选择号码（MSRN）来使回叫从归属系统路由选择到在服务系统。这样就减少了信令，节省了时间而且不要求提供 TLDN 或 MSRN。

[0029] 尽管这样对本发明进行了说明，但是显然，可以以许多方式对其进行变更。可以认为这些变更属于本发明的实质范围，而且试图使所有这些修改包括在所附权利要求所述的范围内。

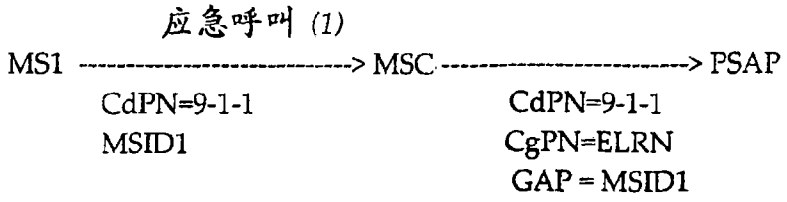


图 1

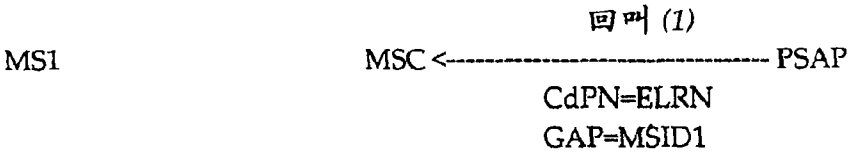


图 2

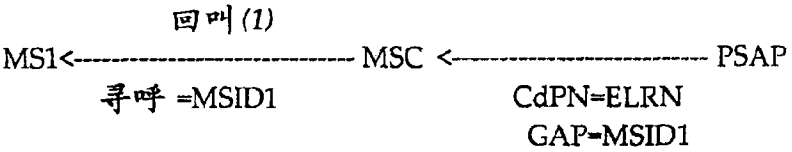


图 3

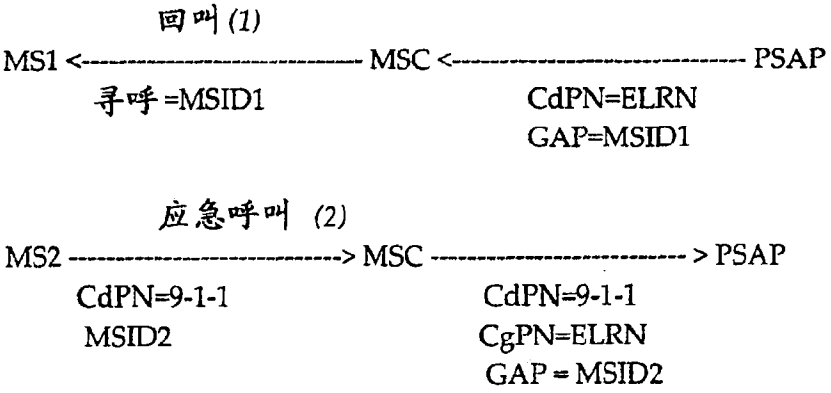


图 4

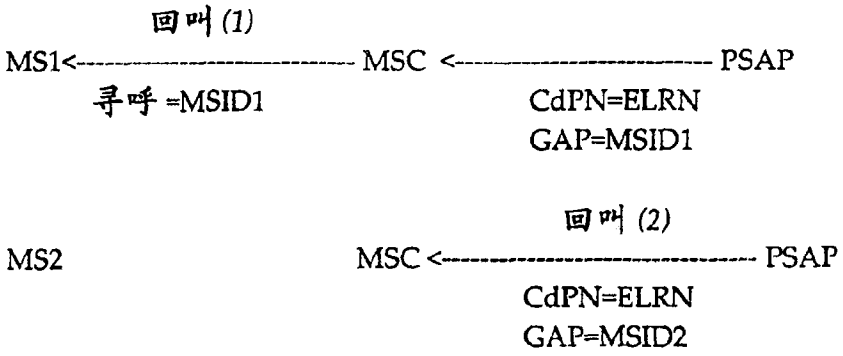


图 5

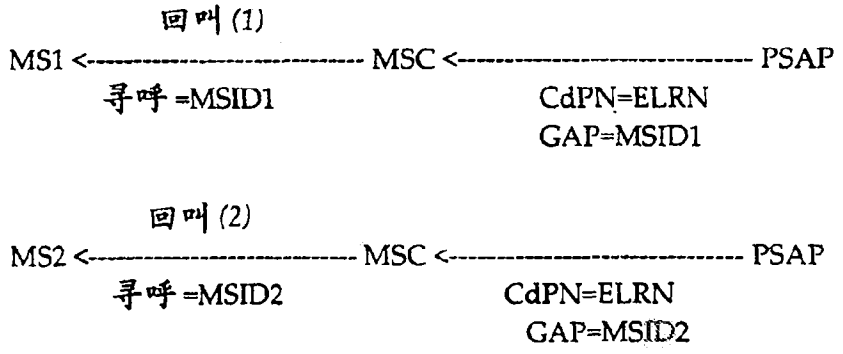


图 6

Espacenet

Bibliographic data: CN101772929 (A) — 2010-07-07

System and method for indicating emergency call back to user equipment

Inventor(s): PURNADI RENE W; KHALEDUL ISLAM M ± (PURNADI RENE W, ; ISLAM M. KHALEDUL)

Applicant(s): RESEARCH IN MOTION LTD ± (RESEARCH IN MOTION LIMITED)

Classification: - international: ***H04L12/66; H04M11/06; H04Q3/64***
- cooperative: **H04M3/5116**; **H04Q3/64**; H04L65/1016; H04M1/72538; H04Q2213/13152; H04Q2213/13176; H04Q2213/13204; H04Q2213/13248; H04Q2213/13348; H04Q2213/1337; H04Q2213/13389

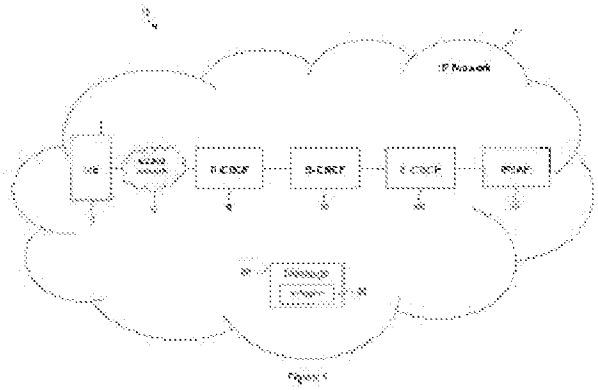
Application number: CN20078100171 20071204

Priority number(s): WO2007CA02176 20071204 ; US20070944258P 20070615

Also published as: CN101772929 (B) WO2008151406 (A1) WO2008151406 (A8) US2008310599 (A1) MX2009013633 (A) KR20120051078 (A) KR101162903 (B1) KR20100029124 (A) KR101162847 (B1) EP2165489 (A1) EP2165489 (A4) CA2690236 (A1) less

Abstract of CN101772929 (A)

A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.



(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101772929 A
(43)申请公布日 2010.07.07

(21)申请号 200780100171.X

(22)申请日 2007.12.04

(30)优先权数据
60/944,258 2007.06.15 US

(85)PCT申请进入国家阶段日
2010.02.05

(86)PCT申请的申请数据
PCT/CA2007/002176 2007.12.04

(87)PCT申请的公布数据
WO2008/151406 EN 2008.12.18

(71)申请人 捷讯研究有限公司
地址 加拿大安大略省

(72)发明人 雷纳·W·普尔纳迪
M·哈立德·伊斯兰

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮

(51)Int.Cl.
H04L 12/66(2006.01)
H04Q 3/64(2006.01)
H04M 11/06(2006.01)

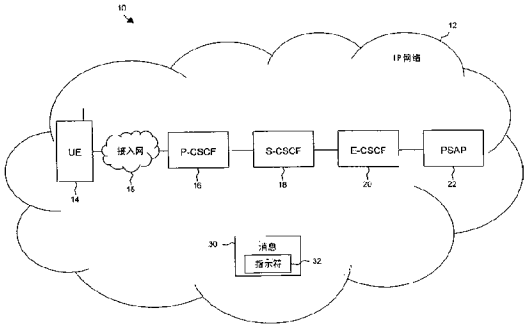
权利要求书 2 页 说明书 8 页 附图 5 页

(54)发明名称

向用户设备指示紧急回叫的系统和方法

(57)摘要

提供了一种用于向用户设备 14 和接入网 15 指示 IMS(互联网协议多媒体子系统)紧急回叫的方法。该方法包括:将该紧急回叫来自 PSAP(来自公共安全应答点)22 的指示 32 包括在从 PSAP 至用户设备 14 和接入网 15 的消息 30 中。



CN 101772929 A

1. 一种向用户设备和接入网指示IMS(互联网协议多媒体子系统)紧急回叫的方法,包括:

将所述紧急回叫来自PSAP(公共安全应答点)的指示包括在从PSAP至用户设备和接入网的消息中。

2. 根据权利要求1所述的方法,其中,所述消息是SIP(会话发起协议)Invite消息。

3. 根据权利要求1所述的方法,其中,所述指示被包括在来自首部中。

4. 根据权利要求1所述的方法,其中,所述指示是将PSAP标识为紧急相关实体的字符串。

5. 根据权利要求1所述的方法,其中,所述指示被包括在去往首部中。

6. 根据权利要求1所述的方法,其中,所述指示是用户设备的紧急公共标识符。

7. 根据权利要求6所述的方法,其中,所述紧急公共标识符是每当用户设备发起IMS紧急呼叫时创建的。

8. 根据权利要求1所述的方法,还包括:用户设备和接入网以促使成功完成紧急回叫的方式对所述指示作出响应。

9. 根据权利要求1所述的方法,还包括:当在用户设备接收到所述指示之后预定义时间长度内用户设备没有接收到响应于紧急回叫的输入时,用户设备触发自主动作。

10. 根据权利要求9所述的方法,其中,所述自主动作是以下至少一项:

向PSAP发送自动化消息;

向PSAP发送用户设备的位置;以及

向除PSAP以外的紧急相关实体发送自动化消息。

11. 根据权利要求2所述的方法,其中,所述用户设备检查所有输入SIP Invite消息以发现所述指示,并且,代理呼叫会话控制功能检查所有输入SIP Invite消息以发现所述指示,以通知接入网准备和以优先顺序排列针对紧急回叫的资源。

12. 根据权利要求2所述的方法,其中,所述用户设备仅在所述用户设备向PSAP发起IMS紧急呼叫之后预定义时间长度内,检查输入SIP Invite消息以发现所述指示。

13. 一种用户设备,包括:

处理器,被配置为将IMS(互联网协议多媒体子系统)呼叫识别为来自PSAP(公共安全应答点)的紧急回叫。

14. 根据权利要求13所述的用户设备,其中,所述处理器将利用包括紧急回叫指示符的所述IMS呼叫,将所述IMS呼叫识别为来自PSAP的紧急回叫。

15. 根据权利要求14所述的用户设备,其中,所述紧急回叫指示符是将PSAP标识为紧急相关实体并且被包括在从PSAP至用户设备的SIP(会话发起协议)Invite消息中的字符串。

16. 根据权利要求14所述的用户设备,其中,所述紧急回叫指示符被包括在来自首部中。

17. 根据权利要求14所述的用户设备,其中,所述紧急回叫指示符是被包括在“去往首部”中的、用户设备的紧急公共标识符。

18. 根据权利要求17所述的用户设备,其中,所述紧急公共标识符是每当用户设备发起IMS紧急呼叫时创建的。

19. 根据权利要求 14 所述的用户设备，其中，当在用户设备接收到所述紧急回叫指示符之后预定义时间长度内用户设备没有接收到响应于紧急回叫的输入时，用户设备触发自主动作。

20. 根据权利要求 19 所述的用户设备，其中，所述自主动作是以下至少一项：

向 PSAP 发送自动化消息；

向 PSAP 发送用户设备的位置；以及

向除 PSAP 以外的紧急相关实体发送自动化消息。

21. 根据权利要求 14 所述的用户设备，其中，代理呼叫会话控制功能检查所有输入 SIP Invite 消息以发现所述紧急回叫指示符，以通知接入网准备和以优先顺序排列针对紧急回叫的资源。

22. 一种系统，包括：

一个或多个处理器；以及

指令，当被所述一个或多个处理器执行时，促使在从 PSAP（公共安全应答点）至用户设备的消息中提供紧急回叫指示符。

23. 根据权利要求 22 所述的系统，其中，所述紧急回叫指示符是以下之一：

字符串，将 PSAP 标识为紧急相关实体，并且被包括在从 PSAP 至用户设备的 SIP（会话发起协议）Invite 消息的来自首部中；以及

用户设备的紧急公共标识符，被包括在 SIP Invite 消息的去往首部中，并且是每当用户设备发起 IMS 紧急呼叫时创建的。

24. 根据权利要求 22 所述的系统，其中，当在用户设备接收到所述紧急回叫指示符之后预定义时间长度内用户设备没有接收到响应于紧急回叫的输入时，用户设备触发自主动作。

25. 根据权利要求 24 所述的系统，其中，所述自主动作是以下至少一项：

向 PSAP 发送自动化消息；

向 PSAP 发送用户设备的位置；以及

向除 PSAP 以外的紧急相关实体发送自动化消息。

向用户设备指示紧急回叫的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求由Purnadi等于2007年6月15日提交的、标题为“System and Method for Indicating IMS Emergency Call Back to UserEquipment”的美国临时专利申请的优先权，其全部内容并入此处以供参考。

背景技术

[0003] IP（互联网协议）多媒体子系统（IMS）是用于提供许多电话服务提供商开始实现的移动和固定多媒体服务的标准化架构。IMS架构可以包括使用标准协议进行通信的不同功能（即，网络元件）的集合。

[0004] 使用移动设备或任何用户设备（UE）的IMS网络用户可以进行紧急呼叫，例如911呼叫（在北美）或112呼叫（在欧洲大多数地区）。典型地，这种呼叫由公共安全应答点（PSAP）来处理，所述公共安全应答点可能协调对紧急事件的适当响应。在紧急呼叫终止之后，PSAP可以出于多种原因对用户进行回叫。例如，如果紧急呼叫出现异常终止，则PSAP可能回叫用户以确定用户是否希望传达任何附加信息。备选地，PSAP可能回叫用户以要求在初始呼叫中因疏忽而未请求的信息。在紧急呼叫终止之后从PSAP至紧急呼叫者的回叫的其他原因可以是本领域技术人员所熟悉的。

附图说明

[0005] 为了更完整地理解本公开，现在参照结合附图和详细的说明书而作出的以下简要描述，其中，类似的参考标记表示类似的部分。

[0006] 图1是根据本公开的实施例的包括用户设备和公共安全应答点在内的示意性IP网络的图。

[0007] 图2是示出了根据本公开的实施例的呼叫流程的顺序图。

[0008] 图3是包括可操作于本公开的各个实施例中的一些的用户设备在内的无线通信系统的图。

[0009] 图4是可操作于本公开的各个实施例中的一些的用户设备的框图。

[0010] 图5是可在可操作于本公开的各个实施例中的一些的用户设备上实现的软件环境的图。

[0011] 图6是适于本公开的各个实施例中的一些的示意性通用计算机系统。

具体实施方式

[0012] 起初应当理解，尽管以下提供了本公开的一个或多个实施例的示意性实施方式，但所公开的系统和/或方法是可以使用任何数目的技术来实现的，不论该技术是当前已知的还是现有的。本公开绝不应限于示意性实施方式、附图和以下示意的技术，包括此处示意和描述的示例设计和实施方式，但是在所附权利要求及其等同替换的全部范围内可以修改本公开。

[0013] 在实施例中，提供了一种向用户设备和接入网指示 IMS（互联网协议多媒体子系统）紧急回叫的方法。所述方法包括：将所述紧急回叫来自 PSAP（来自公共安全应答点）的指示包括在从 PSAP 至用户设备和接入网的消息中。

[0014] 在另一实施例中，提供了一种用户设备，包括被配置为将 IMS（互联网协议多媒体子系统）呼叫识别为来自 PSAP 的紧急回叫的处理器。

[0015] 在另一实施例中，提供了一种系统，包括一个或多个处理器和指令。所述指令在被所述一个或多个处理器处理器执行时，促使在从 PSAP 至用户设备 (UE) 的消息中提供紧急回叫指示符。

[0016] 当在从 UE 至 PSAP 的 IMS 紧急呼叫终止之后 PSAP 试图对 UE 进行 IMS 回叫时，如果 UE 没有识别出该回叫是来自 PSAP 的，则可能出现不期望的结果。例如，UE 可以将该回叫视为常规的呼叫并将其置为中断或呼叫等待，回叫可能被阻止，或 UE 可能无法对回叫适当地作出响应。本公开提供了通过将向 UE 的、回叫来自 PSAP 的指示包括在回叫中，来向 UE 指示来自 PSAP 的 IMS 紧急回叫。这允许 UE 在紧急回叫与常规呼叫之间进行区分。将向 UE 的呼叫标识为来自 PSAP 的回叫的指示或指示符可以以不同方式与该呼叫相关联，这些方式中的一些方式将在以下更详细地讨论。其他方式是本领域技术人员根据本公开将容易地想到的。在 US 专利 7,050,785 和 7,139,549 中提供了其他技术，这两个专利都是 Islam 等的，出于所有目的并入此处以供参考。

[0017] 图 1 示出了包括 IP（互联网协议）网络 12 的系统 10，系统 10 还可以包括 IMS 网络的一个或多个组件。示出了 UE 14，UE 14 可以包括连接至 IMS 网络的任何终端用户设备或系统（例如，移动电话、移动无线设备（包括数字、蜂窝或双模式设备）个人数字助理、膝上型 / 写字板 / 笔记本计算机、台式计算机等）。CSCF（呼叫会话控制功能）（未明确示出）是 IMS 网络中的公知元件，负责例如维护 SIP（会话发起协议）呼叫以及针对访问 IMS 网络内的服务的订户提供会话控制。

[0018] UE 14 经由接入网 15 来与 P-CSCF（代理 CSCF）16 进行通信。接入网 15 可能是任何公知的组件（例如，基站以及可以促使与后续网络组件进行无线连接的其他无线发送和接收设备）的集合。P-CSCF 16 是 SIP 代理，该 SIP 代理可以是针对 IMS 终端的第一接触点，并且如果所访问的网络还不是 IMS 兼容的，则 SIP 代理可以位于在全 IMS 网络中或归属网络中的所访的问网络中。P-CSCF 16 与 S-CSCF（服务 CSCF）18 进行通信。S-CSCF 18 是 SIP 服务器，该 SIP 服务器可以位于归属网络中，并可以执行会话控制、用户简档的下载和上载、以及其他功能。S-CSCF18 与 E-CSCF（紧急 CSCF）20 进行通信。E-CSCF 20 提供针对 PSAP（公共安全应答点）22 的会话控制功能，PSAP 22 可以是 911 系统或者另一紧急呼叫中心或系统。

[0019] 为了进行紧急呼叫或 911 呼叫，UE 14 可能经由 P-CSCF 16、S-CSCF 18 和 E-CSCF 20 来与 PSAP 22 进行通信。然而，仅当 UE 14 漫游时，才可能进行经由 P-CSCF 16 的通信。当 UE 14 处于其归属网络中时，可以不需要 P-CSCF 16，并且 UE 14 可能直接与 S-CSCF 18 进行通信。以下，被描述为经由 P-CSCF 16 进行的任何通信都应被理解为可能在不存在 P-CSCF 16 的情况下进行。

[0020] 当前 3GPP（第 3 代合作伙伴计划）和 3GPP2（第 3 代合作伙伴计划 2）规范 (3GPP 中的 TS 23.167 和 3GPP2 中的 X.P0049) 没有指定使 UE 14 确定输入呼叫是否实际上是来

自紧急系统（如 PSAP 22）的回叫的方法。根据一个实施例，PSAP 22 提供了 IMS 紧急回叫消息 30（如 SIPInvite），包括紧急回叫指示或指示符 32。UE 14 可以使用指示符 32 来将呼叫标识为来自 PSAP 22 的 IMS 紧急回叫，然后可以对该回叫适当地作出响应。例如，UE 14 可能使用指示符 32 来在与接入网 15 的承载建立期间设置合适的优先级，可能在必要时丢弃和阻止其他呼叫，或者可能采取其他动作以促进或增大成功完成紧急回叫的可能性。指示符 32 还可以允许 UE 14 提供向 UE 用户通知来电紧急回叫的事件（例如，可听的或视频显示的警告）。

[0021] 如果 UE 用户在过了特定时间之后尚未对回叫作出相应，则 UE 14 还可以使用指示符 32 来触发动作。无法以及时的方式应答紧急回叫可能是用户丧失了能力或需要紧急服务的指示。当在接收到指示符 32 之后预定义时间长度内没有进行对紧急回叫的响应时，UE 14 可能向 PSAP 22 发起指示用户不能作出应答的自动答复，可能发送 UE 14 的位置坐标，可能向另一紧急系统发送自动化消息，或者可能触发其他动作。例如，UE 14 可能在没有来自用户的物理输入的情况下完成呼叫，这在用户不能物理激活 UE 14 以接收呼叫时可能是有益的。P-CSCF 16 可以向接入网 15 提供紧急回叫指示符 32，并且接入网 15 可以使用紧急回叫指示符 32 来准备和以优先顺序排列紧急回叫的适当资源。

[0022] 可以基于当前规范以多种方式来传送紧急回叫指示符 32。然而，本公开不限于此，还可适用于多种不同系统和环境中。在一个实施例中，可以通过将 PSAP 公共指示符 (PSAP PUID) 包括于在终止来自 UE14 的紧急呼叫之后从 PSAP 22 发送至 UE 14 的 SIP 消息中来提供指示符 32。更具体地，可以将 PSAP PUID 包括在 SIP Invite 消息中作为指示符 32。在这种情况下，PSAP PUID 具有将 PSAP 22 标识为紧急相关实体的标准命名约定或格式（如 name@sos.domain、psap@domain 等）可以是有益的。即，单词或者字母、数字或其他字符的排列（如‘psap’、‘sos’或‘emergency’）可能用在 SIP Invite 中，以指示消息 30 是来自紧急系统（如 PSAP 22）的。

[0023] 可以在从 PSAP 22 发送至 UE 14 的 SIP Invite 消息中的各个位置提供 PSAP PUID。例如，PSAP PUID 可以置于典型地提供与 SIP 消息发送者身份有关的信息的“来自首部”中。SIP Invite “来自首部”中的标准化 PSAP PUID 格式可以使 SIP Invite 可容易地被 UE 14 识别为与来自 PSAP 22 的紧急回叫相关联的消息。即，UE 14 可能检验“来自首部”以找到指示 SIP Invite 来自 PSAP 22 的名称或字符串（如‘psap’、‘sos’或‘emergency’）。如果找到了这种字符串，则 UE 14 知道该消息来自 PSAP22 并相应地作出响应。UE 14 可能检验每个 SIP Invite 消息以发现该名称或字符串，或者可能仅在 UE 14 进行 911 呼叫或其他紧急呼叫之后的一段时间内进行检验。

[0024] 在另一实施例中，UE 紧急公共标识符 (ePUID) 可以用作指示符 32。作为背景，仅当 UE 14 执行 IMS 紧急注册时，UE 14 当前获得与标准 PUID 不同的 ePUID。然而，在当前指导原则下，仅当 UE 14 在处于其归属网络之外的同时进行紧急呼叫时，或者仅当 UE 14 不具有足够证书来执行 IMS 常规注册时，UE 14 才执行 IMS 紧急注册。因此，ePUID 可能不始终可用作指示符 32。

[0025] 本实施例提供了以下情况：每当 UE 14 进行紧急呼叫时 UE14 都执行紧急 IMS 注册，而不论 UE 14 时处于其归属网络中还是在漫游，也不论 UE 14 是否具有足够证书来进行常规注册。于是，甚至当 UE 14 从其归属网络内进行紧急呼叫时，UE 14 也可能具有 ePUID，

并且每当UE 14进行紧急呼叫时,UE 14都可以将该ePUID通过给PSAP 22。当PSAP 22向UE 14进行紧急回叫时,PSAP 22就可以使用ePUID作为消息30中的指示符32。更具体地,ePUID可以置于标识SIP消息接收者的SIP Invite“去往首部”中。当UE 14接收到包括自身ePUID的消息(例如在“去往首部”中具有UE ePUID的SIP Invite)时,UE 14可以将该消息识别为与来自PSAP 22的紧急回叫相关联并可以适当地作出响应。

[0026] 在其他实施例中,可以以多种其他方式将紧急回叫指示符32包括在从PSAP 22至UE 14的SIP Invite中。例如,可能添加显式的新紧急回叫首部,或者可能将隐式的紧急回叫指示符32置于现有首部(如P-Asserted-Identity首部)内。备选地,其他消息30可以包括或可以用作指示符32,或者可以采用本领域技术人员借助本公开容易想到的多种其他方式或技术。

[0027] 图2示出了先前使用其标准PUID发起了IMS紧急呼叫会话的UE14的示例性呼叫流程图。在该实施例中,当紧急呼叫终止时,PSAP 22试图使用SIP Invite消息来回叫UE 14。SIP Invite在“去往首部”中包括UE PUID,并在“来自首部”中包括标准化的或经识别的PSAP PUID(如name@sos.domain)。在“来自首部”中使用的标准化PSAP PUID格式由P-CSCF 16(或不存在P-CSCF 16时由S-CSCF 18)和UE 14识别为来自PSAP 22的紧急呼叫的指示。P-CSCF 16或S-CSCF 20触发接入网15,从而如上所述,UE 14和接入网15可以针对该呼叫设置最高优先级以确保成功的紧急回叫和/或可以执行其他动作。

[0028] 在事件202处,响应于异常紧急呼叫终止,或处于某种其他原因,PSAP 22向UE 14发起回叫。PSAP 22形成SIP Invite消息,该SIP Invite消息在“去往首部”中包括UE PUID并使用标准化的或经识别的PSAPPUID格式作为“来自首部”中的指示符。在该示例中,PSAP PUID使用name@sos.domain作为标准格式。从PSAP 22发起的SIP Invite中的‘sos’向UE 14指示这是紧急回叫。然而,置于SIP Invite消息中或其他消息中其他位置的其他参数也可以用作指示符。然后,将以这种方式形成的SIP Invite发送至E-CSCF 20。

[0029] 在事件204处,E-CSCF 20将SIP Invite转发至S-CSCF 18。在事件206处,S-CSCF 18将SIP Invite转发至P-CSCF 16。在事件208处,P-CSCF 16将SIP Invite转发至UE 14。P-CSCF 16可以使用紧急回叫指示符作为触发以通知接入网准备和以优先顺序排列紧急回叫的资源。在事件210处,UE 14检查输入SIP Invite中的“来自首部”,并将‘sos’识别为指示SIP Invite来自PSAP 22且SIP Invite与紧急回叫相关联的标准化格式。然后,UE 14可以使用该指示来将呼叫置为最高优先级,以确保成功的紧急回叫。UE 14也可以采取其他动作,包括:丢弃其他正在进行的呼叫、在无线承载建立过程中设置适当的优先级等等。

[0030] 在事件212处,UE 14形成SIP 200OK消息以对SIP Invite作出响应。UE 14将PSAP PUID置于“去往首部”中,并将其自身的UE PUID置于“来自首部”中。然后,将SIP 200OK发送至P-CSCF 16。注意,根据3GPP2规范,P-CSCF 16可能不允许通过在“去往首部”中具有PSAPPUID的SIP Invite来进行紧急呼叫初始化。然而,事件212处发送的消息不是SIP Invite初始化消息,而可以是SIP 200OK。因此,如事件214处所示,P-CSCF 16允许在“去往首部”中具有PSAP PUID的消息。应当注意,P-CSCF 16典型地需要知道并准备好接收SIP 200OK,或者P-CSCF 16可能拒绝SIP 200OK。在P-CSCF 16已从PSAP 22接收到SIPInvite之后,可以使P-CSCF 16知道UE 14可能发送200OK。

[0031] 在事件 216、218 和 220 处，P-CSCF 16 经由 S-CSCF 18 和 E-CSCF 20 来向 PSAP 22 路由 SIP 200OK。在事件 222 处，PSAP 22 形成 SIP ACK 消息以对 SIP 200OK 作出响应。PSAP 22 将 UE PUID 置于“去往首部”中，并将其自身的 PSAP PUID 置于“来自首部”中，并将 SIP ACK 发送至 E-CSCF 20。在事件 224、226 和 228 处，经由 S-CSCF 18 和 P-CSCF 16 来向 UE 14 路由 SIP ACK。在这一点上，如事件 230 处所示，完成紧急回叫的建立。应当理解，图 2 仅示出了本公开的一个实施例的一个呼叫流程，并且本公开不仅限于所示出的呼叫流程。对于此处公开的多个其他实施例，可能发生其他其他呼叫流程。

[0032] 图 3 示出了包括 UE 14 的实施例在内的无线通信系统。UE 14 可操作用于实现本公开的方面，但本公开不应限于这些实施方式。尽管被示为移动电话，但 UE 14 可以采取多种形式，包括无线手机、寻呼机、个人数字助理 (PDA)、便携式计算机、写字板计算机或膝上型计算机。许多合适的设备将这些功能当中的一些或全部相结合。在本公开的一些实施例中，UE 14 不是如便携式、膝上型或写字板计算机之类的通用计算设备，而是如移动电话、无线手持机、寻呼机、PDA 或车辆中安装的电信设备之类的专用通信设备。在另一实施例中，UE 14 可以是便携式、膝上型或其他计算设备。UE 14 可以支持专门的活动，例如游戏、库存控制、作业控制和 / 或任务管理功能等。

[0033] UE 14 包括显示器 402。UE 14 还包括触敏表面、键盘或由用户输入的总体称为 404 的其他输入键。键盘可以是全字母数字键盘或简化字母数字键盘（如 QWERTY、Dvorak、AZERTY 和顺序类型）或与电话键区相关联的带有字母表字母的传统数字键区。输入键可以包括滚轮、退出或换码键、轨迹球以及其他导航或功能键，其可以被向内按下以提供更多的输入功能。UE 14 可以呈现供用户选择的选项、供用户驱动的控件和 / 或供用户导向的光标或其他指示符。

[0034] UE 14 还可以接受来自用户的数据条目，该数据条目指示用于拨打的号码或用于对 UE 14 的操作进行配置的不同参数值。UE 14 还可以响应于用户命令来执行一个或多个软件或固件应用程序。这些应用程序可以将 UE 14 配置为响应于用户交互来执行不同定制功能。此外，可以用无线电来编程和 / 或配置 UE 14，例如从无线基站、无线接入点或对等端 UE 14 来配置 UE 14。

[0035] 在可由 UE 14 执行的各种应用程序当中有网页浏览器，其使显示器 402 能够示出网页。该网页是可以经由与无线网络接入节点、蜂窝塔、对等端 UE 14 或者任何其他无线通信网络或系统 400 进行无线通信来获得的。网络 400 耦合至有线网络 408（如互联网）。经由无线链路和有线网络，UE 14 可以访问不同服务器（如服务器 410）上的信息。服务器 410 可以提供可在显示器 402 上示出的内容。备选地，UE 14 可以以中继类型或跳类型的连接，通过充当中间媒介的对等端 UE 14，来接入网络 400。

[0036] 图 4 示出了 UE 14 的框图。尽管示出了 UE 14 的多种已知组件，但在实施例中，可以在 UE 14 中包括所列出的组件和 / 或未列出的附加组件的子集。UE 14 包括数字信号处理器 (DSP)502 和存储器 504。如图所示，UE 14 还可以包括天线和前端单元 506、射频 (RF) 收发器 508、模拟基带处理单元 510、麦克风 512、听筒扬声器 514、耳机端口 516、输入 / 输出接口 518、可拆卸式存储卡 520、通用串行总线 (USB) 端口 522、短距离无线通信子系统 524、警报器 526、键区 528、液晶显示器 (LCD)，该液晶显示器 (LCD) 可以包括触敏表面 530、LCD 控制器 532、电荷耦合器件 (CCD) 摄像机 534、摄像机控制器 536 和全球定位系统 (GPS) 传感

器 538。在实施例中，UE 14 可以包括另一种显示器，其不提供触敏屏幕。在实施例中，DSP 502 可以直接与存储器 504 进行通信而不经过输入 / 输出接口 518。

[0037] DSP 502 或某其他形式的控制器或中央处理单元操作用于根据在存储器 504 中存储的或在 DPS 502 本身内包含的存储器中存储的嵌入式软件或固件，来控制 UE 14 的各种组件。除了嵌入式软件或固件之外，DPS 502 还可以执行其他应用程序，该其他应用程序存储在存储器 504 中，或者是可经由如便携式数据存储介质（如可拆卸式存储卡 520）之类的信息载体介质、或经由有线或无线网络通信而获取到的。应用软件可以包括将 DSP 502 配置为提供所期望的功能的、已编译的机器可读指令集，或者应用软件可以是要由解释器或编译器来处理以间接配置 DSP 502 的高级软件指令。

[0038] 可以提供天线和前端单元 506 以在无线信号和电信号之间进行转换，使得 UE 14 能够发送和接收来自蜂窝网络或某些其他可用无线通信网络或来自对等端 UE 14 的信息。在实施例中，天线和前端单元 506 可以包括多个天线以支持波束成形和 / 或多输入多输出 (MIMO) 操作。本领域技术人员已知，MIMO 操作可以提供空间多样性，其可以用于克服困难的信道条件和 / 或增加信道吞吐量。天线和前端单元 506 可以包括天线调谐和 / 或阻抗匹配组件、RF 功率放大器和 / 或低噪声放大器。

[0039] RF 收发器 508 提供了频移，将接收到的 RF 信号转换到基带并将基带发送信号转换到 RF。在一些描述中，无线电收发器或 RF 收发器可以被理解为包括其他信号处理功能，如调制 / 解调、编码 / 解码、交织 / 去交织、扩频 / 解扩、快速傅立叶逆变换 (IFFT) / 快速傅立叶变换 (FFT)、循环前缀附加 / 移除以及其他信号处理功能。出于清楚的目的，此处的描述将该信号处理的描述与 RF 和 / 或无线电级 (radio stage) 分开，并在构思上将信号处理分配给模拟基带处理单元 510 和 / 或 DSP 502 或其他中央处理单元。在一些实施例中，RF 收发器 508、天线和前端 506 的部分以及模拟基带处理单元 510 可以被组合在一个或多个处理单元和 / 或特定用途集成电路 (ASIC) 中。

[0040] 模拟基带处理单元 510 可以提供对输入和输出的各种模拟处理，例如对来自麦克风 512 和耳机 516 的输入的模拟处理以及对向听筒 514 和耳机 516 的输出的模拟处理。为此，模拟基带处理单元 510 可以具有用于连接至内置麦克风 512 和听筒扬声器 514 的端口，使得 UE 14 能够用作蜂窝电话。模拟基带处理单元 510 还可以包括用于连接至耳机或其他免提麦克风和扬声器配置的端口。模拟基带处理单元 510 可以沿一个信号方向提供数模转换并沿相反的信号方向提供模数转换。在一些实施例中，模拟基带处理单元 510 的至少一些功能可以由数字处理组件来提供，例如由 DSP 502 或其他中央处理单元来提供。

[0041] DSP 502 可以执行调制 / 解调、编码 / 解码、交织 / 去交织、扩频 / 解扩、快速傅立叶逆变换 (IFFT) / 快速傅立叶变换 (FFT)、循环前缀附加 / 移除以及其他与无线通信相关联的信号处理功能。在实施例中，例如在码分多址 (CDMA) 技术应用中，针对发射器功能，DSP 502 可以执行调制、编码、交织和扩频，而针对接收器功能，DSP 502 可以执行解扩、去交织、解码和解调。在另一实施例中，例如在正交频分多址 (OFDMA) 技术应用中，针对发射器功能，DSP 502 可以执行调制、编码、交织、快速傅立叶逆变换和循环前缀附加，而针对接收器功能，DSP 502 可以执行循环前缀移除、快速傅立叶变换、去交织、解码和解调。在其他无线技术应用中，DSP 502 可以执行其他信号处理功能和信号处理功能的组合。

[0042] DSP 502 可以经由模拟基带处理单元 510 与无线网络进行通信。在一些实施例中，

该通信可以提供互联网连接性，使得用户能够访问互联网上的内容并能够发送和接收电子邮件或文本消息。输入 / 输出接口 518 与 DSP 502 以及各种存储器和接口互相连接。存储器 504 和可拆卸式存储卡 520 可以提供软件和数据以配置 DSP 502 的操作。在接口当中可以有 USB 接口 522 和短距离无线通信子系统 524。USB 接口 522 可以用于为 UE 14 充电，还可以使 UE 14 能够充当外围设备，以与个人计算机或其他计算机系统交换信息。短距离无线通信子系统 524 可以包括红外端口、蓝牙接口、遵循 IEEE 802.11 的无线接口、或可以使 UE 14 能够与其他附近移动设备和 / 或无线基站进行无线通信的任意其他短距离无线通信子系统。

[0043] 输入 / 输出接口 518 还可以将 DSP 502 连接至警报器 526，警报器 526 在被触发时使 UE 14 例如通过振铃、播放旋律或震动来向用户提供通知。警报器 526 可以充当一种机制，用于通过无声震动或针对特定呼叫者播放预先指定的具体旋律来向用户告警诸如如来电呼叫、新文本消息和约会提醒等不同事件中的任何事件。

[0044] 键区 528 经由接口 518 耦合至 DSP 502，以为用户提供一种进行选择、输入信息以及向 UE 14 提供输入的机制。键区 528 可以是全字母数字键盘或简化字母数字键盘（如 QWERTY、Dvorak、AZERTY 和顺序类型）或者与电话键区相关联的带有字母表字母的传统数字键区。输入键可以包括滚轮、退出或换码键、轨迹球和其他导航或功能键，其可以被向内按下以提供更多的输入功能。另一种输入机制可以是 LCD530，其可以包括触摸屏能力，也可以向用户显示文本和 / 或图形。LCD 控制器 532 将 DSP 502 耦合至 LCD 530。

[0045] 如果配备有 CCD 摄像机 534，则 CCD 摄像机 534 使 UE 14 能够拍摄数字图像。DSP 502 经由摄像机控制器 536 与 CCD 摄像机 534 进行通信。在另一实施例中，可以采用根据与电荷耦合器件摄像机不同的技术而操作的摄像机。GPS 传感器 538 耦合至 DSP 502，以对全球定位系统信号进行解码，从而使 UE 14 能够确定其位置。也可以包括多种其他外围设备以提供附加的功能，例如，无线电和电视接收。

[0046] 图 5 示出了可由 DSP 502 实现的软件环境 602。DSP 502 执行操作系统驱动器 604，操作系统驱动器 604 提供其余软件操作的平台。操作系统驱动器 604 向无线设备硬件的驱动器提供了可访问应用软件的标准化接口。操作系统驱动器 604 包括应用程序管理服务（“AMS”）606，该服务在运行于 UE 14 上的应用程序之间传送控制。图 5 还示出了网页浏览器应用程序 608、媒体播放器应用程序 610 和 Java 小应用程序 612。网页浏览器应用程序 608 将 UE 14 配置为充当网页浏览器，允许用户向表格中输入信息和选择链接以检索和观看网页。媒体播放器应用程序 610 将 UE 14 配置为检索和播放音频或视听媒体。Java 小应用程序 612 将 UE 14 配置为提供游戏、实用程序和其他功能。组件 614 可以提供与紧急呼叫相关的功能。

[0047] UE 14、P-CSCF 16、S-CSCF 18、E-CSCF 20 和 PSAP 22 以及此处描述的其他组件可以完全或部分地在通用计算机上实现或者可以包括该通用计算机，该通用计算机具有足够处理能力、存储资源和网络吞吐能力以处理置于该通用计算机上的必要工作量。图 6 示出了可适于实现此处描述的一个或多个实施例的典型通用计算机系统 700。计算机系统 700 包括处理器 720（可称为中央处理单元或 CPU），处理器 720 与包括辅助存储器 750、只读存储器 (ROM)740、随机存取存储器 (RAM)730、输入 / 输出 (I/O) 设备 710 和网络连接性设备 760 在内的存储设备进行通信。该处理器可以被实现为一个或多个 CPU 芯片。

[0048] 辅助存储器 750 典型地包括一个或多个盘驱动器或磁带驱动器，辅助存储器 750 用于数据的非易失性存储，并在 RAM 730 不足够大以容纳所有工作数据的情况下用作溢出数据存储设备。辅助存储器 750 可以用于存储当被选择以执行时被加载到 RAM 730 中的程序。ROM740 用于存储在程序执行期间读取的指令以及可能的数据。ROM 740 是非易失性存储设备，其典型地具有与辅助存储器的较大存储容量相比较小的存储容量。RAM 730 用于存储易失性数据以及可能存储指令。对 ROM 740 和 RAM 730 的访问典型地比对辅助存储器 750 的访问要快。

[0049] I/O 设备 710 可以包括打印机、视频监视器、液晶显示器 (LCD)、触屏显示器、键盘、键区、开关、拨号盘、鼠标、轨迹球、语音识别器、卡读取器、纸带读取器或其他公知输入设备。

[0050] 网络连接设备 760 可以采用以下形式：调制解调器、调制解调器组、以太网卡、通用串行总线 (USB) 接口卡、串行接口、令牌环卡、光纤分布式数据接口 (FDDI) 卡、无线局域网 (WLAN) 卡、无线电收发器卡（如，码分多址 (CDMA) 和 / 或全球移动通信系统 (GSM) 无线电收发器卡）以及其他公知网络设备。这些网络连接 760 设备可以使处理器 720 能够与互联网或者一个或多个内联网进行通信。利用这种网络连接，可以想到，处理器 720 在执行上述方法步骤的过程中可能从网络接收信息或可能向网络输出信息。常被示作要使用处理器 720 执行的一系列指令的这种信息是可以例如以在载波中体现的计算机数据信号的形式从网络接收和输出至网络的。

[0051] 可包括例如要使用处理器 720 执行的数据或指令在内的这种信息是可以例如以计算机数据基带信号或体现在载波中的信号的形式从网络接收和输出至网络的。由网络连接 760 设备产生的基带信号或体现在载波中的信号可以在电导体表面中或电导体表面上、在同轴电缆中、在波导中、在光学介质（例如光纤）中或者在空气或自由空间中进行传播。在基带信号或嵌入载波中的信号中所包含的信息可以是根据不同事件来排序的，如这对于处理或产生该信息或者发送或接收该信息而言可能是需要的）。基带信号或嵌入载波中的信号或者当前使用或今后开发的其他类型的信号（这里称为传输介质）可以是根据本领域技术人员若干方法来产生的。

[0052] 处理器 720 执行其从硬盘、软盘、光盘（基于这些各种盘的系统都可以被视为辅助存储器 750）、ROM 740、RAM 730 或网络连接设备 760 访问的指令、代码、计算机程序、脚本。尽管仅示出了一个处理器 720，但可以存在多个处理器。如被讨论为由处理器实现的指令或处理可以由一个或多个处理器同时、串行或以其他方式处理。

[0053] 尽管在本公开中已提供了多个实施例，但应当注意，在不脱离本公开的精神或范围的情况下，可以以许多其他具体形式来体现所公开的系统和方法。当前示例应被视为示意性的而非限制性的，并且并不意在限制此处给出的细节。例如，可以在另一系统中组合或结合各种元件或组件，或者可以省略或不实现特定特征。

[0054] 此外，在不脱离本公开的范围的情况下，在各个实施例中描述和示出为分离或单独的技术、系统、子系统和方法可以与其他系统、模块、技术或方法组合或结合。被示出或讨论为彼此耦合或直接耦合或进行通信的其他项目可以通过某种接口、设备或中间组件来（不论是电、机械还是以其他方式）间接耦合或进行通信。在不脱离此处公开的精神和范围的情况下，本领域技术人员可确定改变、替换和变更的其他示例。

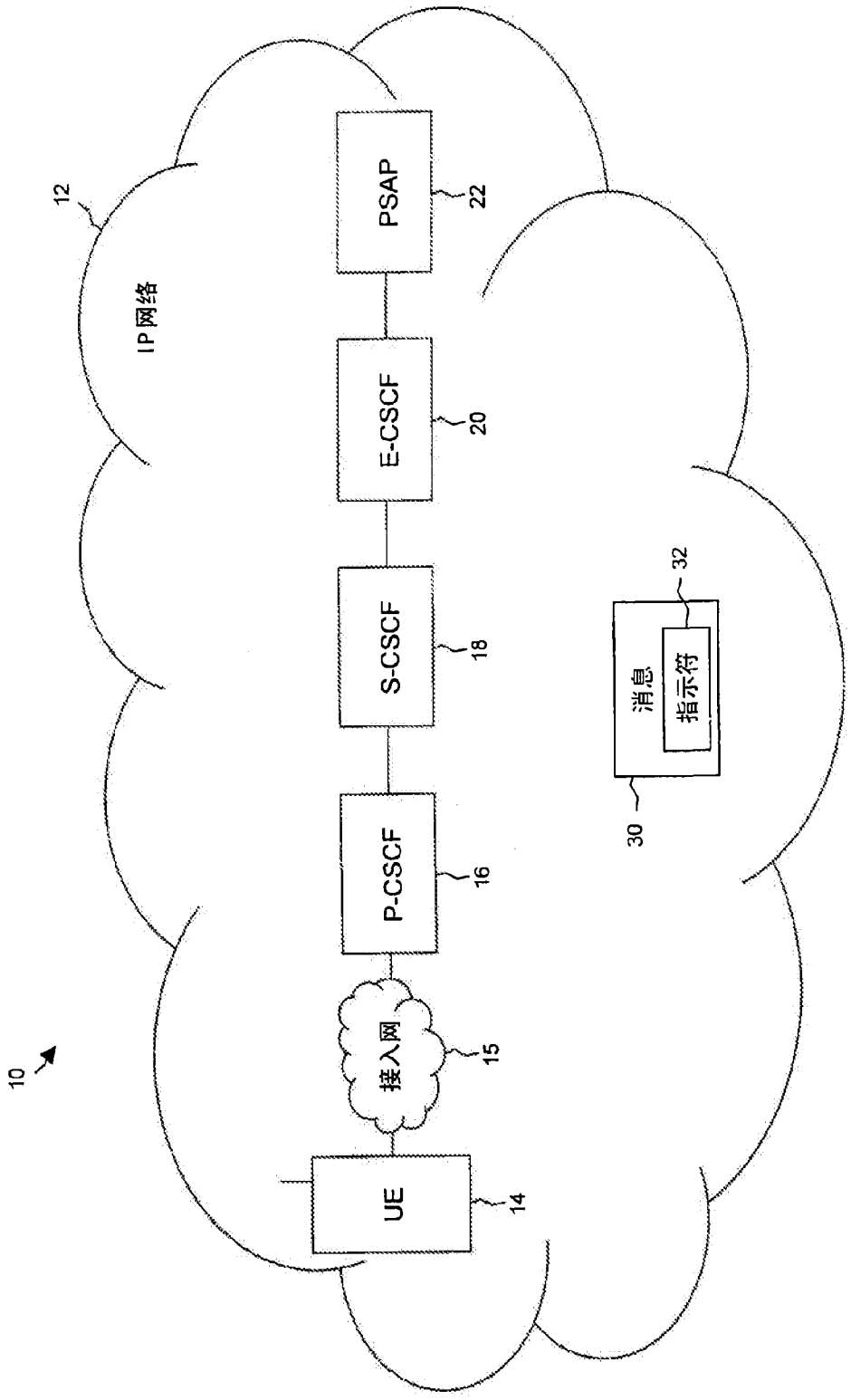


图 1

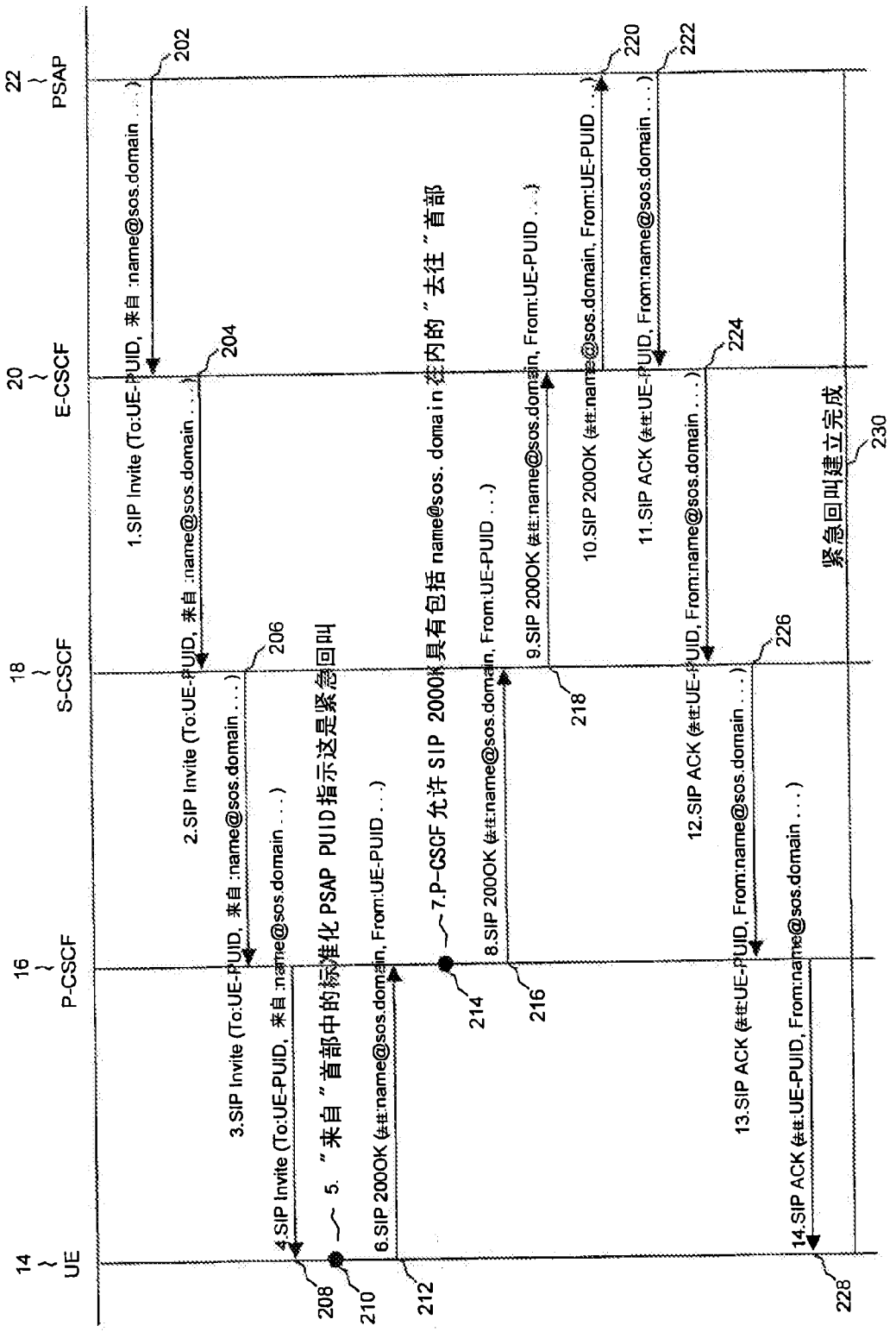


图 2

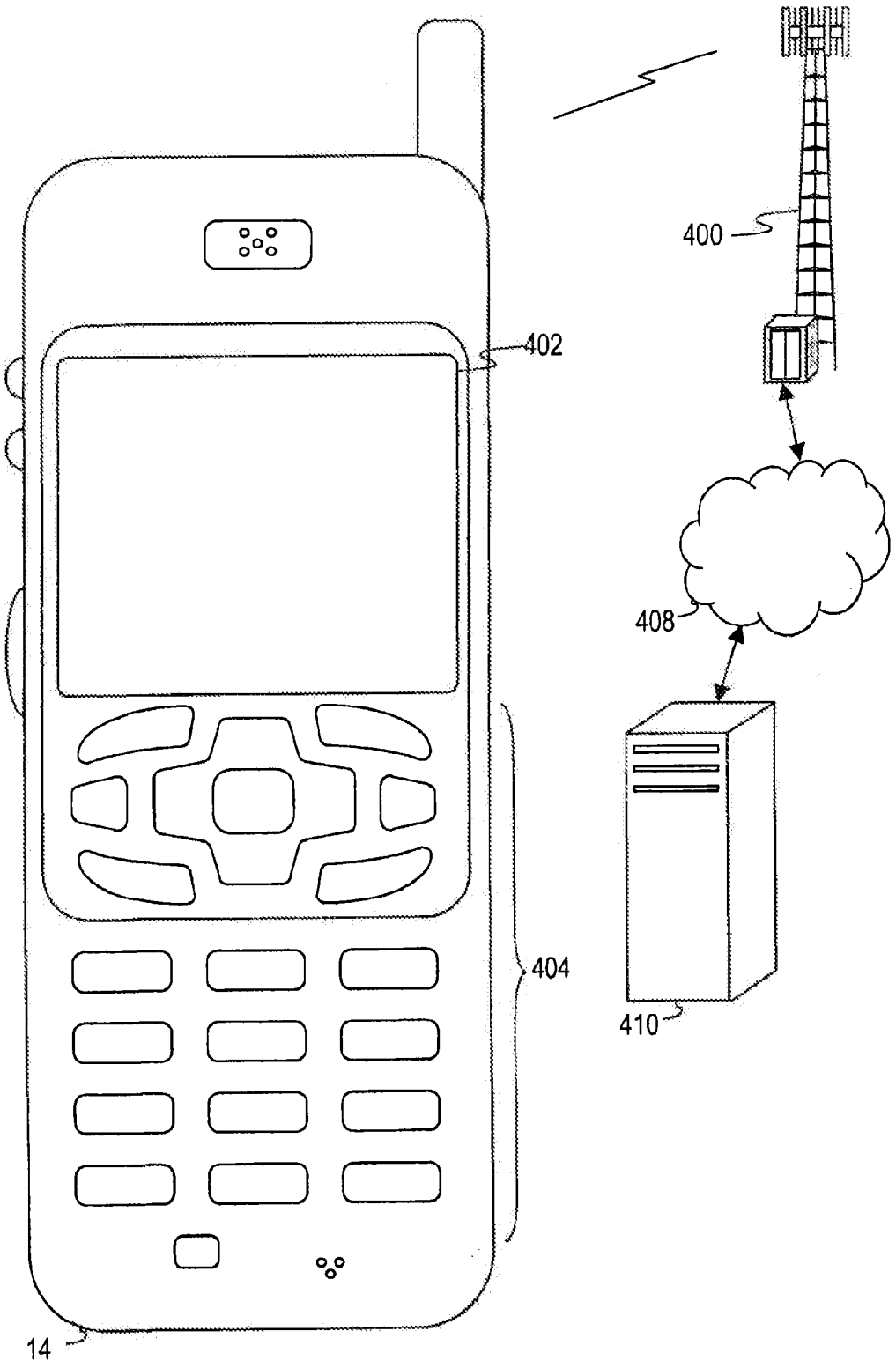


图 3

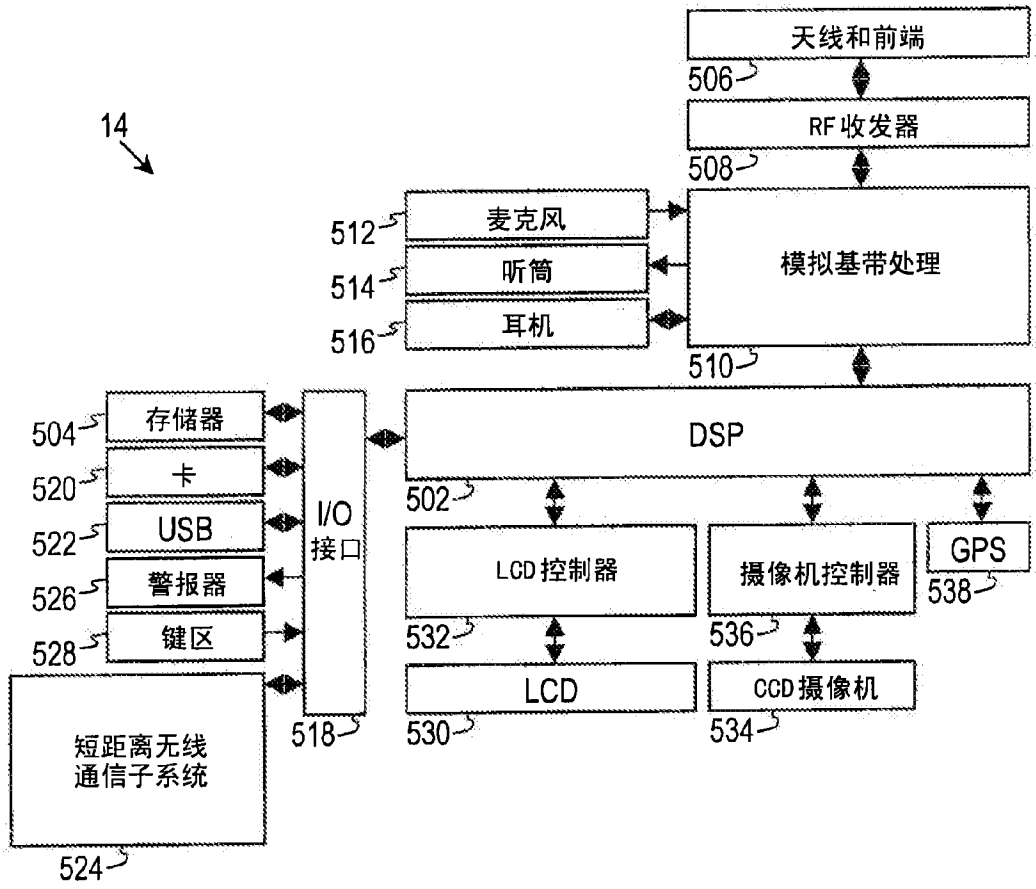


图 4

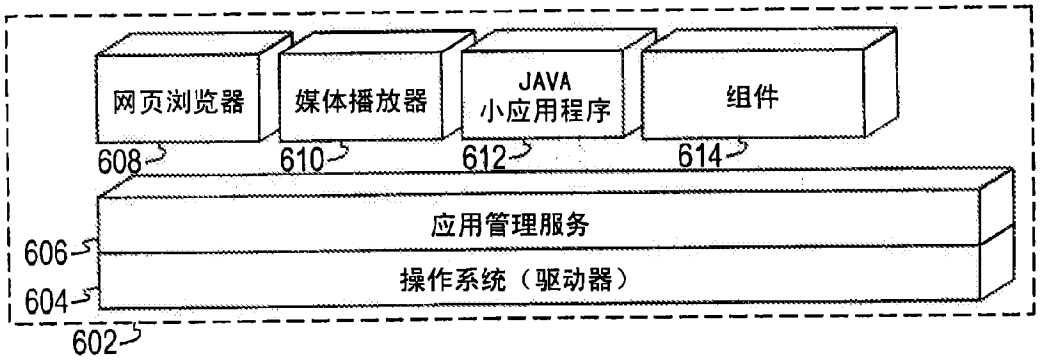


图 5

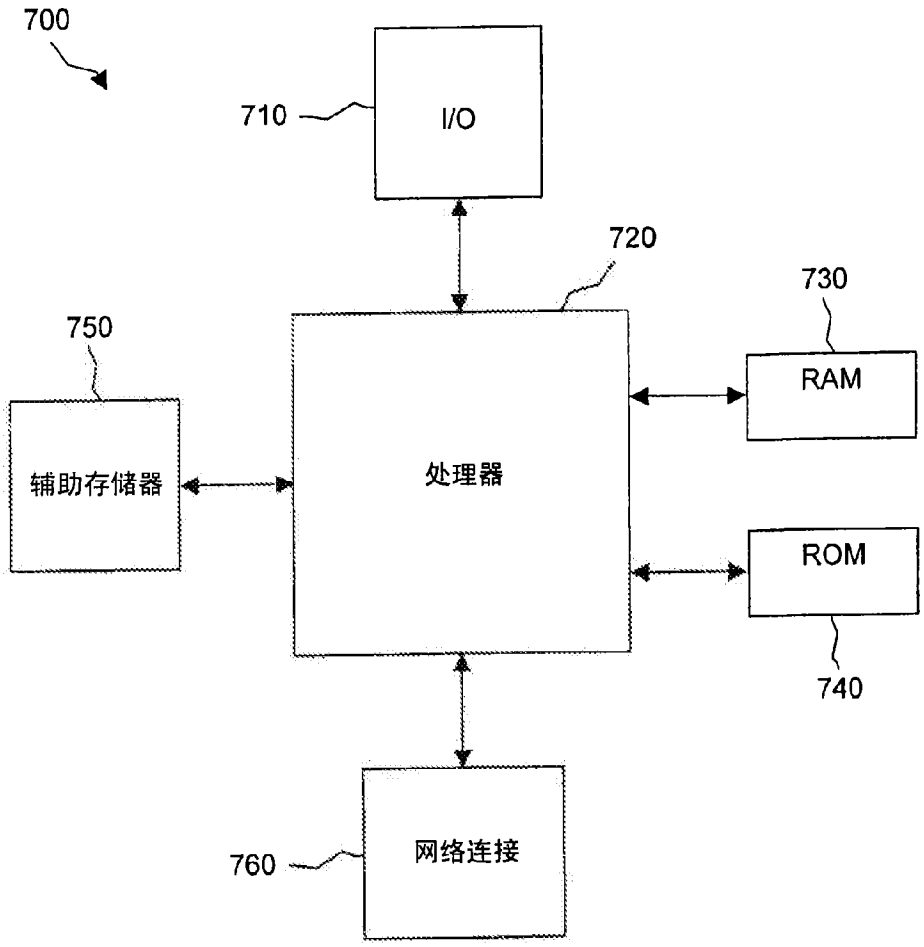


图 6

Espacenet

Bibliographic data: CN101069390 (B) — 2010-12-22

Method for the routing of communications to a voice over internet protocol terminal in a mobile communication system

Inventor(s): JUHA KALLIO ± (KALLIO JUHA)

Applicant(s): NOKIA CORP ± (NOKIA CORP)

Classification: - international: ***H04W60/00; H04W76/02;*** *H04W8/26;* ***H04L***
- cooperative: **H04W76/021**; **H04W8/10**; H04W8/26

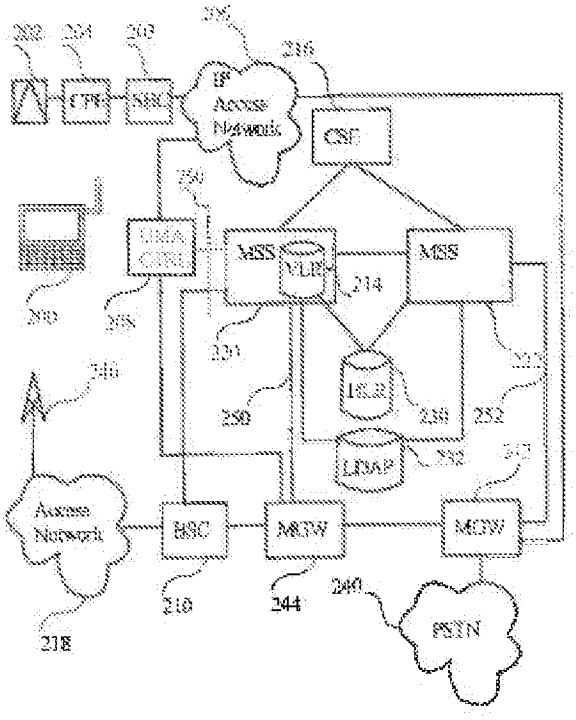
Application number: CN2005841159 20051220

Priority number (s): FI20040001659 20041223 ; WO2005FI00540 20051220

Also published as: CN101069390 (A) WO2006067269 (A1) US2006142011 (A1) US7400881 (B2) KR20070097526 (A) more

Abstract of CN101069390 (B)

The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile station. The call control node translates



PETITIONER APPLE INC. EX. 1004-446

the called party number to the logical name using the directory.

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101069390 B
(45)授权公告日 2010.12.22

(21)申请号 200580041159.7

(22)申请日 2005.12.20

(30)优先权数据
20041659 2004.12.23 FI

(85)PCT申请进入国家阶段日
2007.05.30

(86)PCT申请的申请数据
PCT/FI2005/000540 2005.12.20

(87)PCT申请的公布数据
WO2006/067269 EN 2006.06.29

(73)专利权人 诺基亚公司
地址 芬兰埃斯波

(72)发明人 J·卡利奥

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 冯谱

(51)Int.Cl.
H04W 60/00(2009.01)
H04W 76/02(2009.01)

(56)对比文件
CN 1501720 A,2004.06.02, 全文.
CN 1474626 A,2004.02.11, 全文.
CN 1509116 A,2004.06.30, 全文.
WO 2004017564 A1,2004.02.26, 全文.
WO 0122766 A1,2001.03.29, 全文.
US 20020119775 A1,2002.08.29, 全文.
WO 0079814 A1,2000.12.28, 全文.

审查员 刘艳

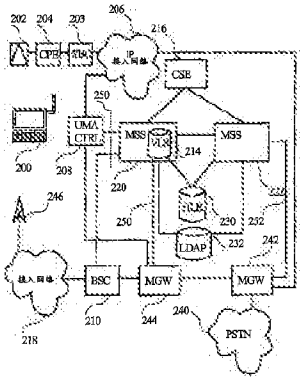
权利要求书 3 页 说明书 10 页 附图 6 页

(54)发明名称

用于在移动通信系统中将通信路由到基于网际协议的语音终端的方法

(57)摘要

本发明涉及一种用于在通信系统中对呼叫和消息进行路由的方法。在该方法中移动台使用逻辑名来注册到呼叫控制节点。逻辑名在目录中映射为国际移动订户标识。呼叫控制节点使用国际移动订户标识来执行位置更新到归属位置寄存器。使用被叫方号码来联系移动台。当收到去往核心网络的终止呼叫或者消息时,为移动台分配漫游号码,而将该呼叫或者消息路由到当前服务于移动台的呼叫控制实体。呼叫控制节点使用目录将被叫方号码转译成逻辑名。



CN 101069390 B

1. 一种用于在至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的通信系统中对呼叫进行路由的方法，所述方法包括：

从移动台接收去往第一呼叫控制节点的注册消息，所述注册消息包括针对所述移动台的逻辑名；

在所述第一呼叫控制节点的请求下在目录中将所述逻辑名映射为针对所述移动台的国际移动订户标识；

在所述第一呼叫控制节点的请求下更新所述移动台的位置到归属位置寄存器，所述第一呼叫控制节点的所述请求包括所述国际移动订户标识；

在第二呼叫控制节点中接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；

从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；

在所述归属位置寄存器的请求下从所述第一呼叫控制节点分配漫游号码；

从所述归属位置寄存器发送至少包括所述漫游号码的查问响应消息到所述第二呼叫控制节点；

从所述第二呼叫控制节点发送所述呼叫建立请求消息到所述第一呼叫控制节点；以及

在所述第一呼叫控制节点的第二请求下在所述目录中将所述被叫方号码映射为针对所述移动台的所述逻辑名。

2. 根据权利要求 1 所述的方法，所述方法还包括：

在所述第二呼叫控制节点中获得主叫方号码；

在所述第一呼叫控制节点中确定所述主叫方号码是否包括指示了所述主叫方号码可以转译成第二逻辑名的前缀；以及

在所述第一呼叫控制节点的第三请求下在所述目录中将所述主叫方号码映射为针对主叫方的所述第二逻辑名。

3. 根据权利要求 1 所述的方法，所述方法还包括：

在所述移动台确定无线局域网的可用性；

建立从所述移动台到连接至所述无线局域网的接入路由器的连接；以及

经由所述接入路由器获得所述第一呼叫控制节点的标识。

4. 根据权利要求 1 所述的方法，其中所述通信系统包括无线局域网。

5. 根据权利要求 1 所述的方法，其中所述通信系统包括全球移动通信系统网络和通用移动电话系统网络中的至少一个。

6. 根据权利要求 5 所述的方法，其中所述第一呼叫控制节点和所述第二呼叫控制节点是移动服务交换中心服务器。

7. 根据权利要求 1 所述的方法，其中所述移动台包括会话发起协议用户代理。

8. 根据权利要求 7 所述的方法，其中所述注册消息是会话发起协议注册消息。

9. 根据权利要求 1 所述的方法，其中所述呼叫建立请求消息是 ISDN 用户部分呼叫建立请求消息。

10. 根据权利要求 1 所述的方法，其中所述目录是轻型目录访问协议目录。

11. 一种至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄

存器的系统，所述系统还包括：

在所述第一呼叫控制节点中的移动性实体，配置用以：从所述移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从所述目录将所述逻辑名映射为针对所述移动台的国际移动订户标识；以及通过指明所述国际移动订户标识来请求从所述归属位置寄存器更新所述移动台的位置；

在所述第二呼叫控制节点中的呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到所述第一呼叫控制节点；以及

在所述第一呼叫控制节点中的呼叫控制实体，配置用以请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

12. 根据权利要求 11 所述的系统，其中在所述第一呼叫控制节点中的所述呼叫控制实体被配置用以：确定主叫方号码是否包括指示了所述主叫方号码可以转译成第二逻辑名的前缀；以及请求从所述目录中将所述主叫方号码映射为针对主叫方的所述第二逻辑名。

13. 根据权利要求 11 所述的系统，所述系统还包括：

在所述移动台中的通信实体，配置用以：确定无线局域网的可用性；建立从所述移动台到连接至所述无线局域网的接入路由器的连接；以及经由所述接入路由器获得所述第一呼叫控制节点的标识。

14. 根据权利要求 11 所述的系统，其中所述系统包括无线局域网。

15. 根据权利要求 11 所述的系统，其中所述系统包括全球移动通信系统网络和通用移动电话系统网络中的至少一个。

16. 根据权利要求 15 所述的系统，其中所述第一呼叫控制节点和所述第二呼叫控制节点是移动服务交换中心服务器。

17. 根据权利要求 11 所述的系统，其中所述移动台包括会话发起协议用户代理。

18. 根据权利要求 17 所述的系统，其中所述注册消息是会话发起协议注册消息。

19. 根据权利要求 11 所述的系统，其中所述呼叫建立请求消息是 ISDN 用户部分呼叫建立请求消息。

20. 根据权利要求 11 所述的系统，其中所述目录是轻型目录访问协议目录。

21. 一种呼叫控制节点，包括：

移动性实体，配置用以：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识；以及通过指明所述国际移动订户标识来请求从归属位置寄存器更新所述移动台的位置；

呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到第二呼叫控制节点；以及请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

22. 一种用于在至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属

位置寄存器的通信系统中对呼叫进行路由的设备，所述设备包括：

用于从移动台接收去往第一呼叫控制节点的注册消息的装置，所述注册消息包括针对所述移动台的逻辑名；

用于在所述第一呼叫控制节点的请求下，在目录中将所述逻辑名映射为针对所述移动台的国际移动订户标识的装置；

用于在所述第一呼叫控制节点的请求下，更新所述移动台的位置到归属位置寄存器的装置，所述第一呼叫控制节点的所述请求包括所述国际移动订户标识；

用于在第二呼叫控制节点中接收呼叫建立请求消息的装置，所述呼叫建立请求消息至少包括被叫方号码；

用于从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器的装置，所述查问消息至少包括所述被叫方号码；

用于在所述归属位置寄存器的请求下从所述第一呼叫控制节点分配漫游号码的装置；

用于从所述归属位置寄存器向所述第二呼叫控制节点发送至少包括所述漫游号码的查问响应消息的装置；

用于从所述第二呼叫控制节点向所述第一呼叫控制节点发送所述呼叫建立请求消息的装置；以及

用于在所述第一呼叫控制节点的第二请求下在所述目录中将所述被叫方号码映射为针对所述移动台的所述逻辑名的装置。

23. 根据权利要求 22 所述的设备，所述设备还包括：

用于在所述第二呼叫控制节点中获得主叫方号码的装置；

用于在所述第一呼叫控制节点中确定所述主叫方号码是否包括指示了所述主叫方号码可以转译成第二逻辑名的前缀的装置；以及

用于在所述第一呼叫控制节点的第三请求下在所述目录中将所述主叫方号码映射为针对主叫方的所述第二逻辑名的装置。

24. 根据权利要求 22 所述的设备，所述设备还包括：

用于在所述移动台确定无线局域网的可用性的装置；

用于建立从所述移动台到连接至所述无线局域网的接入路由器的连接的装置；以及

用于经由所述接入路由器获得所述第一呼叫控制节点的标识的装置。

25. 根据权利要求 22 所述的设备，其中所述通信系统包括无线局域网。

26. 根据权利要求 22 所述的设备，其中所述通信系统包括全球移动通信系统网络和通用移动电话系统网络中的至少一个。

27. 根据权利要求 26 所述的设备，其中所述第一呼叫控制节点和所述第二呼叫控制节点是移动服务交换中心服务器。

28. 根据权利要求 22 所述的设备，其中所述移动台包括会话发起协议用户代理。

29. 根据权利要求 28 所述的设备，其中所述注册消息是会话发起协议注册消息。

30. 根据权利要求 22 所述的设备，其中所述呼叫建立请求消息是 ISDN 用户部分呼叫建立请求消息。

31. 根据权利要求 22 所述的设备，其中所述目录是轻型目录访问协议目录。

用于在移动通信系统中 将通信路由到基于网际协议的语音终端的方法

技术领域

[0001] 本发明涉及在移动通信系统中进行路由。具体而言，本发明涉及在移动通信系统中将通信路由到基于 IP 的语音 (VoIP) 终端。

背景技术

[0002] 近来无线局域网 (WLAN) 在移动通信中已经变得重要。WLAN 相较于比如通用移动电信系统 (UMTS) 和全球移动通信系统 (GSM) 这样的许可频带蜂窝通信系统而言的优点在于它们使用非许可频带并且小区大小小得多的事实。这些事实使得有可能构建由小型公司实体和个人用户运营的专用 WLAN。无线通信在这些 WLAN 中的成本比在许可频带蜂窝系统中要低廉得多。WLAN 已经主要用于因特网络接入，但是通过 WLAN 提供语音通信的想法近来已经赢得契机。为了针对基于 WLAN 技术的语音而获得广阔的市场份额以及为终端用户提供可靠的服务体验，有必要能够提供支持基于 WLAN 和基于许可频带的无线接入的双系统终端。换言之，对于用户来说必须有可能在 WLAN 和许可频带蜂窝系统中漫游。通常，WLAN 无线接入在存在有 WLAN 基础设施的市区中使用，而许可频带蜂窝系统在 WLAN 覆盖以外的区域中使用。

[0003] 3G 伙伴项目已经将 IP 多媒体子系统 (IMS) 标准化以便迎合 VoIP 和其它基于 IP 的多媒体服务之需。通常，UMTS 无线接入网络用来接入支持 IMS 的核心网络。然而，包括移动交换中心 (MSC)、归属位置寄存器 (HLR)、访问位置中心 (VLR)、CAMEL 服务实体 (CSE) 和服务控制点 (SCP) 的现有电路交换核心网络基础设施提供范围广阔的服务。当运营商希望向双系统终端提供 WLAN 和许可频带无线接 入能力时，如果运营商具有通过两种无线接入技术来提供相同服务的某一机制则将是有益的。提供后向兼容服务尤其重要。换言之，有必要能够也在 WLAN 侧提供来自许可频带蜂窝系统的常见观感服务。这些服务称为传统服务。这种服务的例子包括呼叫转发、预付费、附加费率 (premium rate) 和免费服务号码、呼叫等待和呼叫转移。通常使用包括 MSC 和 SCP 的智能网络基础设施来提供预付费服务和服务号码。在智能网络的 3GPP 标准化版本中 SCP 称为 CSE。

[0004] 现在参照图 1，该图图示了现有技术中与为双系统终端提供传统服务相关联的问题。图 1 图示了在实践中必须在 IMS 中重建传统服务这一事实。在 IMS 中网元与协议大相径庭，因此这代表相当数量的工作。在图 1 中有移动台 (MS) 100，该移动台是能够通过 WLAN 无线接入和许可频带无线接入来通信的双系统移动台。许可频带无线接入例如可以是基于时分多址 (TDMA) 的 GSM 无线接入或者基于宽带码分多址 (WCDMA) 的 UMTS 无线接入。在图 1 中也有与 IP 多媒体子系统 (IMS) 通信的 WLAN 124，该 IMS 至少包括 P-CSCF 102、I-CSCF 104、S-CSCF 106、MGCF 120 和 MGW 122。当在 WLAN 124 的区域中时经由 IMS 提供去往和来自 MS 100 的多媒体通信。WLAN 124 连接到将基于 IP 的用户平面业务转换到电路交换的 PSTN 126 的媒体网关 (MGW) 122。WLAN 124 也与代理呼叫状态控制功能 (P-CSCF) 102 通信。信令平面业务被路由到 P-CSCF 如 P-CSCF 102。信令平面业务例如是基于会话发起协

议 (SIP) 的。SIP 在因特网络工程任务组 (IETF) 文献 RFC 3261 中有定义。P-CSCF 102 用来访问查问呼叫状态控制功能 (I-CSCF)104，该 I-CSCF 使用归属订户服务器 (HSS)108 来确定其中当前注册了给定订户的服务呼叫状态控制功能 (S-CSCF)106。S-CSCF 控制源自于和终止于 MS 100 的多媒体通信。S-CSCF 与将信令平面业务转换成电路交换信令的媒体网关控制功能 (MGCF)120 进行通信。例如，MGCF 120 将在 MS 100、P-CSCF 102、I-CSCF 104、S-CSCF 106 与 MGCF 120 之间使用的 SIP 信令转换成在 PSTN 126 中使用的 ISDN 用户部分 (ISUP) 信令。MGCF 120 也例如 使用国际电信联盟 (ITU-T)H.248 协议来控制 MGW 122。S-CSCF 106 连接到三个服务平台，即应用服务器 (AS)110、CSE 116 和开放服务架构 (OSA) 服务器 118。S-CSCF 106 经由 IP 移动性 (IM) 服务交换功能 (SSF)112 连接到 CSE 116。S-CSCF 106 经由服务能力服务器 (SCS)114 连接到 OSA 服务器 118。

[0005] 在图 1 中也有连接到 GSM/UMTS 电路交换核心网络的 GSM/UMTSBSS 160，该网络至少包括 MSC 150、VLR 152、GMSC 156、HLR 154 和 CSE 158。GSM/UMTS BSS 160 连接到 MSC 150。MSC 150 也包括 VLR152。MSC 150 连接到 GMSC 156。也有存储与订户的位置有关的订户数据及其服务数据的 HLR 154。GMSC 156 也连接到 PSTN 126。CSE 158 在向 BSS 160 所服务的订户提供 IN 服务时控制 GMSC 156 和 MSC 150。CSE 158 也有通向 HLR 154 的接口，该接口允许询问和修改 HLR 154 中的服务数据。多个标准化补充服务由 MSC 150、GMSC 156、VLR 152 和 HLR 154 直接实施。这些服务的例子包括呼叫转发、呼叫等待、呼叫转移、呼叫完成到忙订户、关闭用户组和呼叫禁止。除这些业务之外，还可以有在这些网元中直接实施的各种特定于销售商的补充服务。为了迎合前述传统补充服务之需，在 MSC 150、GMSC 156、VLR 152 和 HLR 154 中存在各种服务功能。这些服务功能在图 1 中图示为服务功能集 170-174。各服务功能集可以包括在给定的网元中掌控的多种不同服务功能。

[0006] 为了在 MS 100 处于 WLAN 124 的服务区中时支持相同的传统服务，服务功能集 170-174 必须端口连通到至少包括 P-CSCF 102、I-CSCF 104、S-CSCF 106 和 HSS 108 的对应 IMS 网元。这代表相当数量的任务，因为当在 IMS 网元中实施等效服务功能集 180-184 时必须重复在服务功能集 170-174 中投入的所有开发努力。例如，MSC 中的服务功能集 170 将对应于 S-CSCF 106 中的服务功能集 182，而 CSE 中的服务功能集 171 将分别对应于 AS 110、CSE 116 和 OSA 服务器 118 中的服务功能集 181、183 和 184。然而，对应不足直接和明显的。足以认为传统服务功能集从 GSM/UMTS 电路交换核心网络到 IMS 侧的端口连通并非微不足道，因为在 IMS 网元与 MS 100 之间使用的协议与在 GSM/UMTS 电路交换核心网络中使用的协议大相径庭。

[0007] 在如下出版物中提出了一种在为从 GSM/UMTS BSS 漫游到 WLAN 侧的移动台提供传统服务时的可能性：“SIP-Enabled Gateway MSC：Linking WiFi Hot Spots with 2.5/3G Networks”，Amir Atai，AjaySahai，Telica，2004 年 3 月 31 日。Atai 所公开的解决方案包括将 WALN 直接连接到电路交换核心网络中也充当服务访问 MSC(VMSC) 的 GMSC。Atai 所公开的解决方案的不足在于给定的订户总是由给定的 GMSC 服务。然而，即使在双系统终端的情况下，对于运营商而言仍然必须有可能为任何 GMSC 中的给定终端接收终止呼叫。GMSC 中终止呼叫的处理必须对 2G/3G 和 WLAN 终端都是统一的。无论终端的类型如何都必须使用从 HLR 获得的漫游号码将呼叫路由到正确的服务 VMSC。另外，能够配置 DNS 使得使用例如“sip.operator.com”这样的同一完全限定域名 (FQDN) 来查询多个 MSC 服务器是有益的，

其中“operator”代表运营商名而“sip”代表 SIP 注册器集。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 就有可能以轮循方式向充当 SIP 注册器的不同 MSC 服务器返回 IP- 地址。因此，在不同的注册时间，可以从 DNS 提供不同的 IP- 地址给双系统终端。此外，一些传统服务可能要求与传统服务有关的呼叫必须路由到语音服务器或者集中式 IN 服务交换点 / 经由语音服务器或者集中式 IN 服务交换点进行路由。因此，能够在电路交换核心网元之间使用传统 ISUP 信令将是有益的。当使用纯 SIP 信令时，用户的 ITU-T E.164 格式订户号码不可用。

发明内容

[0008] 本发明涉及一种用于在至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的通信系统中对呼叫进行路由的方法。该方法包括：从所述移动台接收去往所述第一呼叫控制节点的注册消息，所述注册消息包括针对所述移动台的逻辑名；在所述第一呼叫控制节点的请求下在所述目录中将所述逻辑名映射为针对所述移动台的国际移动订户标识 (IMSI)；在所述第一呼叫控制节点的请求下更新所述移动台的位置到所述归属位置寄存器，所述请求包括所述国际移动订户标识；在所述第二呼叫控制节点中接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；在所述归属位置寄存器的请求下从所述第一呼叫控制节点分配漫游号码；从所述归属位置寄存器发送至少包括所述漫游号码的查问响应消息到所述第二呼叫控制节点；从所述第二呼叫控制节点发送呼叫建立请求消息到所述第一呼叫控制节点；以及在所述第一呼叫控制节点的请求下在所述目录中将所述被叫方号码映射为针对所述移动台的所述逻辑名。

[0009] 本发明也涉及一种至少包括移动台、第一呼叫控制节点、第二呼叫控制节点、目录和归属位置寄存器的系统。该系统还包括：在所述第一呼叫控制节点中的移动性实体，配置用以：从所述移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从所述目录将所述逻辑名映射为针对所述移动台的国际移动订户标识 (IMSI)；以及通过指明所述国际移动订户标识 (IMS) 来请求从所述归属位置寄存器更新所述移动台的位置；在所述第二呼叫控制节点中的呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；从所述第二呼叫控制节点发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到所述第一呼叫控制节点；以及在所述第一呼叫控制节点中的呼叫控制实体，配置用以请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

[0010] 本发明也涉及一种呼叫控制节点，包括：移动性实体，配置用以：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识 (IMSI)；以及通过指明所述国际移动订户标识 (IMSI) 来请求从归属位置寄存器更新所述移动台的位置；以及呼叫控制实体，配置用以：接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问响应消息；以及发送呼叫建立请求消息到第二呼叫控制节点；以及请求

从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

[0011] 本发明也涉及一种包括代码的计算机程序，适于当在数据处理系统上执行时进行以下步骤：从移动台接收注册消息，所述注册消息包括针对所述移动台的逻辑名；请求从目录将所述逻辑名映射为针对所述移动台的国际移动订户标识（IMSI）；请求从归属位置寄存器更新所述移动台的位置，所述请求包括所述国际移动订户标识；接收呼叫建立请求消息，所述呼叫建立请求消息至少包括被叫方号码；发送查问消息到所述归属位置寄存器，所述查问消息至少包括所述被叫方号码；从所述归属位置寄存器接收至少包括漫游号码的查问消息；发送呼叫建立请求消息到另一呼叫控制节点；以及请求从所述目录将所述被叫方号码映射为针对所述移动台的所述逻辑名。

[0012] 在本发明的一个实施例中，在第二呼叫控制节点中获得主叫方号码。例如针对收到的去往第二呼叫控制节点的呼叫建立请求消息来获得主叫方号码。在响应于从归属位置寄存器收到漫游号码而发送的呼叫建立消息中向第一呼叫控制节点提供主叫方号码。当收到呼叫建立请求消息时，第一呼叫控制节点提取主叫方号码并且确定主叫方号码是否包括指示了主叫方号码可以转译成逻辑名的前缀。如果主叫方号码包括这样的前缀，则在所述第一呼叫控制节点的请求下在目录中将它映射为针对主叫方的第二逻辑名。作为响应，目录将第二逻辑名返回到第一呼叫控制节点。在呼叫控制节点中的呼叫控制实体中执行呼叫建立请求消息和主叫方号码分析。

[0013] 在本发明的一个实施例中，在移动台的通信实体中确定无线局域网（WLAN）在移动台处的可用性。通信实体建立从所述移动台到连接至无线局域网的接入路由器的连接。通信实体经由所述接入路由器获得所述第一呼叫控制节点的标识。接入路由器例如是控制去往和来自 WLAN 的区域中移动台的分组数据服务接入的路由器。路由器也可以针对它所连接到的 WLAN 中的移动台来执行认证、鉴权和记账功能。

[0014] 在本发明的一个实施例中，通信系统包括无线局域网（WLAN）。

[0015] 在本发明的一个实施例中，移动通信系统包括全球移动通信系统（GSM）网络和通用移动电话系统（UMTS）网络中的至少一个

[0016] 在本发明的一个实施例中，第一和第二呼叫控制节点是移动服务交换中心服务器（MSS）。MSS 可以控制至少一个处理用户平面业务的媒体网关或者媒体代理。可以从公共交换电话网络（PSTN）或者其它呼叫控制节点接收用户平面业务作为电路交换连接，该电路交换连接在媒体网关中被转换成分组交换连接。在本发明的一个实施例中，第一和第二呼叫控制节点是移动服务交换中心（MSC）。

[0017] 在本发明的一个实施例中，移动台包括会话发起协议（SIP）用户代理。当在 WALN 的区域中，用户代理通过发送会话发起协议（SIP）注册消息到第一呼叫控制节点来执行位置注册。呼叫控制节点可以包括使用会话发起协议（SIP）信令来与用户代理通信的呼叫控制实体。呼叫控制实体可以使用电路交换信令如 ISDN 用户部分（ISUP）来与其它呼叫控制节点通信。如果主叫方和被叫方属于同一运营商的网络，则用户平面业务可以不转换成电路交换连接，但是可代之以通过分组数据将用户平面业务从主叫方移动台运送到被叫方移动台。在那一情况下，在 ISUP 信令消息中带有与主叫方和被叫方相关联的用户平面 IP 地址。

[0018] 在本发明的一个实施例中，主叫方建立请求消息是 ISDN 用户部分（ISUP）呼叫建

立请求消息。在本发明的一个实施例中，呼叫建立请求消息是会话发起协议 (SIP) 邀请消息或者一般而言是任何等 效的基于 IP 的语音呼叫建立请求消息。

[0019] 在本发明的一个实施例中，目录是轻型目录访问协议 (LDAP) 目录。使用 LDAP 协议来访问目录。

[0020] 在本发明的一个实施例中，移动台包括无线局域网终端。在本发明的一个实施例中，移动台包括订户标识模块 (SIM)。

[0021] 在本发明的一个实施例中，移动台是支持 WLAN 和许可频带无线连通性的多无线终端。许可频带无线连通性例如包括在已经为提供 2G 和 3G 服务的运营商所分配的无线频带上的全球移动通信系统 (GSM) 无线连通性和通用移动电信系统 (UMTS) 连通性。

[0022] 在本发明的一个实施例中，在呼叫控制节点内的呼叫控制实体是软件部件。在本发明的一个实施例中，在呼叫控制节点内的移动性实体是软件部件。在本发明的一个实施例中，在移动台节点内的通信实体是软件部件。这些部件中的各部件可以包括至少一个独立编译或者转译的程序模块。部件可以包括在处理器或者虚拟机如 Java 虚拟机中执行的多个进程或者线程。

[0023] 在本发明的一个实施例中，计算机程序存储于计算机可读介质上。计算机可读介质可以是可移动存储卡、磁盘、光盘或者磁带。

[0024] 在本发明的一个实施例中，术语呼叫也指代短消息。在这一实施例中，呼叫建立消息是短消息递送消息而呼叫控制实体是短消息递送实体。在这一情况下，漫游号码是用于递送短消息到第一呼叫控制实体的路由号码。

[0025] 在本发明的一个实施例中，DNS 被配置为使得使用同一完全限定域名 (FQDN) 如“sip.operator.com”来查询多个 MSC 服务器，其中“operator”代表运营商名而“sip”代表 SIP 注册器集。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 可以用轮循方式为充当 SIP 注册器的不同 MSC 服务器返回 IP- 地址。因此，在不同的注册时间可以从 DNS 提供不同的 IP 地址给双系统终端。

[0026] 从核心网络和补充服务观点来看，本发明的益处与 2G/3G 终端 和双系统终端的统一处理有关。在支持 WLAN 和许可频带接入的任何双系统终端情况下，对于运营商来说有可能为任何 GMSC 中的终端接收终止呼叫。订户编号由于终端是双系统终端的事实而不受影响。无论当前 VMSC 是否充当用于 WLAN 热点的 SIP 注册器或者当前 VMSC 是否只服务于 2G/3G 区域都可以使用从 HLR 获得的漫游号码将呼叫路由到正确的服务 VMSC。

[0027] 另外，有可能配置 DNS 使得使用同一完全限定域名 (FQDN) 来查询多个 MSC 服务器。当双系统终端经由 WLAN 注册到电路交换核心网络并且为 SIP 服务提供 FQDN 时，DNS 可以用轮循方式为充当 SIP 注册器的不同 MSC 服务器返回 IP- 地址。因此，在不同的注册时间可以从 DNS 提供不同的 IP 地址到双系统终端。

[0028] 另外，通过允许在收到的去往网关 MSS 的呼叫建立请求消息中使用 MSISDN 号码，有可能维持普通电路交换核心网络漫游机制，包括使用 HLR、VLR 和漫游号码分配。没有必要为 IP 多媒体子系统利用不同机制。这允许从电路交换核心网络使用传统补充服务。从补充服务的观点来看，以与许可频带无线服务区相似的方式来处理 WLAN 提供了更容易的服务部署和运营。

[0029] 此外，一些传统服务可能要求与传统服务有关的呼叫必须路由到语音服务器或者

集中式 IN 服务交换点 / 经由语音服务器或者集中式 IN 服务交换点进行路由。因此，能够在电路交换核心网元之间使用传统 ISUP 信令是有益的。

附图说明

[0030] 被包含用来提供对本发明的进一步理解并且构成本说明书一部分的附图图示了本发明的实施例，并且与描述一起有助于说明本发明的原理。在附图中：

[0031] 图 1 是图示了现有技术中与为双系统终端提供传统服务相关联的问题的框图；

[0032] 图 2 是图示了根据本发明的通信系统的框图；

[0033] 图 3 是图示了在本发明的一个实施例中从会话发起协议 (SIP) 用户代理 (UA) 到移动交换中心服务器 (MSS) 的位置更新的消息序列图；

[0034] 图 4 是图示了在本发明的一个实施例中在基于会话发起协议 (SIP) 的两个用户代理 (UA) 之间的移动台到移动台呼叫的消息序列图；

[0035] 图 5 是描绘了用于在通信系统中将通信路由到会话发起协议 (SIP) 用户代理的方法的一个实施例的流程图；以及

[0036] 图 6 是图示了本发明的一个实施例中的移动交换中心服务器 (MSS) 的框图。

[0037] 具体实施方式

[0038] 现在将具体考虑本发明的实施例，这些实施例的例子在附图中进行图示。

[0039] 图 2 是图示了根据本发明的通信系统的框图。该通信系统至少包括移动台 (MS) 200、服务 MSS 220、网关 MSS 222、归属位置寄存器 (HLR) 230、轻型目录访问协议 (LDAP) 目录 232、CAMEL 服务实体 (CSE) 216、基站控制器 (BSC) 210 和连接到基站收发器 (BTS) 的第一接入网络 218。MS 200 是经由 MSS 220 获得 SIP 连通性的具有 SIP 功能的用户代理。MS 200 是支持 WLAN 和许可频带无线连通性的多无线终端。在本发明的一个实施例中，MS 200 包括执行所有与通信有关的功能的通信实体（未示出）。WLAN 基站收发器 (BTS) 202 提供 WLAN 无线连通性，而 BTS 246 支持许可频带无线连通性。许可频带无线连通性例如可以基于 WCDMA 无线接入或者 TDMA 无线接入。服务 MSS 220 包括为服务 MSS 220 中当前注册的订户存储订户数据的访问位置寄存器 (VLR) 214。网关 MSS 222 具有通向公共交换电话网络 (PSTN) 240 和服务 MSS 220 的信令连接。网关 MSS 222 控制第一 MGW 242 而 MSS 220 控制第二 MGW 244。第一 MGW 242 连接到 PSTN 240 并且向 IP 分组提供到 / 从电路交换 E1/T1 的用户平面转换。第二 MGW 244 连接到 PSTN 240 并且向 IP 分组提供到 / 从电路交换 BSC 210 的用户平面转换。UMA 控制器 208 也可以提供通向第二 MGW 244 的电路交换连接。分别基于来自 MSS 222 和 MSS 220 的请求在第一 MGW 242 与第二 MGW 244 之间对分组进行路由。BSC 210 使用协议接口 250 来连接到 MSS 220。协议接口 250 例如是 GSM A/Gb- 接口或者 UMTS Iu- 接口。BSC 210 因此也可以是 UMTS 无线网络控制器。

[0040] 在图 2 中也有第二接入网络 206，该网络的信令平面经由非许可移动接入 (UMA) 控制器 208 连接到 MSS 220。第二接入网络 206 是基于 IP 的接入网络。UMA 控制器 208 以看似标准 RAN 的方式接口到 MSS 220 中。换言之，UMA 控制器 208 对 MSS 220 而言仿效了 BSC 210。经由会话边界控制器 (SBC) 203 也连接到第二接入网络 206 的是客户端设备 (CPE)，该 CPE 例如是接入路由器。WLAN 基站收发器 (BTS) 202 连接到 CPE 204。可以有经由 CPE 204 连接到第二接入网络 206 的多个 WLAN BTS。SBC 203 充当 SIP 代理并且向 MS 200 隐藏在

至少包括第二接入网络 206 的运营商网络内的地址空间。当在 MS 200 与连接到 PSTN 240 的订户之间有呼叫时，去往 / 来自 MS 200 的用户平面业务经由 SBC 203 去往第一 MGW 242。SBC 203 也可以执行标准的与防火墙有关的任务，比如分组过滤。LDAP 目录 232 用来执行将 SIPURI 转译成 ITU-T E.164 地址并且反之亦然。例如，LDAP 目录在服务 MSS 的请求下将主叫方 SIP URI 转译成主叫方 IMSI 并且在相应的响应消息中提供 IMSI。当 MS 200 在 MSS 220 中执行注册（换言之，初始位置更新过程）时，LDAP 目录向 MSS 220 提供订户信息，该信息通常无法经由从 MS 200 到 MSS 220 的 SIP 信令来获得，但是可在位置更新时或者在呼叫建立请求时经由 GSM A- 接口信令或者 UMTSIu- 接口信令来获得。这样的信息例如包括与 MS 200 SIP URI 相对应的 IMSI。该信息在 MSS 220 的请求下从 LDAP 目录 232 提供给 MSS220。

[0041] 在本发明的一个实施例中，运营商的网络使用单个 LDAP 目录，例如 LDAP 目录 232。当订户经由配备有 SIP 一接口的任何 MSS 注册时，可以访问同一 LDAP 目录。因此，无论询问 MSS 如何，LDAP 目录都是相同的。在本发明的一个实施例中有多个 LDPA 目录。

[0042] 图 3 是图示了在本发明的一个实施例中从会话发起协议 (SIP) 用户代理 (UA) 到移动交换中心服务器 (MSS) 的位置更新的消息序列图。在时刻 t_1，MS 200 确定经由 WLAN BTS 202 的 WLAN 接入是可用的并且确定应当经由 WALN 无线接入对去往 MS 200 和来自 MS 200 的通信进行路由。MS 200（换言之，SIP 用户代理）向 DNS 服务器 314 发送 DNS 询问消息，如箭头 301 所示。该 DNS 询问消息指明了 SIP 服务器完全限定域名 (FDQN)，该 FDQN 由 DNS 服务器 314 解析成至少一个 IP 地址。在图 3 中提供有针对 MSS 220 的单个 IP 地址。DNS 服务器 314 以向 MS 200 提供该 IP 地址的查询响应消息做出响应，如箭头 302 所示。由此，MS 200 向 MSS 220 发送 SIP 注册消息，如箭头 303 所示。该 SIP 注册消息至少带有 MS 200 的 SIP URI 以及用户代理 IP 地址以便由 MSS 220 用来向 MS 200 发送用户平面和信令平面分组。SIP 注册消息可以穿越 SBC（未示出），这会更改用户代理 IP 地址。当 MSS 220 收到 SIP 注册消息时，它向 LDAP 目录 232 发送 LDAP 搜索消息，如箭头 304 所示。该 LDAP 搜索消息至少包括针对 MS 200 的 SIP URI。响应于 LDAP 搜索消息，LDAP 目录 232 获得与 SIP URI 相关联的订户数据。LDAP 目录 232 向 MSS 220 发送 LDAP 搜索响应消息，如箭头 305 所示。该 LDAP 搜索响应消息至少包含与 MS 200 相关联的 IMSI。LDAP 搜索响应消息中所含其它参数可以包括与 MS 200 相关联的主叫方 E.164 地址 (MSISDN-A)、用户名以及与认证有关的参数如临时数和来自 MS 200 的预期认证响应。当收到 LDAP 搜索响应消息时，MSS 220 向 MS 200 发送 SIP 401 响应消息，如箭头 306 所示。SIP 401 响应消息包括 WWW- 认证 / 摘要报头，该报头又包括与运营商网络中的 SIP 服务相关联的字段 (realm)、运营商的域、从 LDPA 目录 232 接收的临时数以及在认证时所要使用的算法（通常是消息摘要 5(MD5)）。响应于收到 SIP 401 响应消息，MS 200 向 MSS 220 提供 SIP 注册消息，如箭头 307 所示。该 SIP 注 册消息包括认证 / 摘要报头，该报头包括与 MS 200 相关联的用户名、与运营商网络中的 SIP 服务相关联的字段、运营商的域、临时数、与 MSS 220 相关联的 URI 以及 MS 200 基于在 SIP 401 响应消息中接收的参数而生成的响应。在收到 SIP 注册消息时，MSS 220 对 MS 200 所生成的响应与从 LDAP 目录 232 收到的预期响应进行比较。

[0043] 响应于成功的认证，MSS 220 开始针对 HLR 230 执行位置更新。MSS 220 将 MS 200 的位置更新到与它相关联的 VLR 214。然而，在图 3 的情况下，VLR 214 被视为 MSS 220 的

部分而没有单独地示出。在本发明的一个实施例中，MSS 220 获得在来自 LDAP 目录 232 的 SIP 注册消息中没有提供的对于位置更新而言必需的所有 MS 200 参数。在成功的认证之后，MS 200 向 HLR 230 发送位置更新请求消息，如箭头 308 所示。该位置更新请求消息至少包括与 MS 200 相关联的 IMSI。响应于收到位置更新请求消息，HLR 230 向 MSS 220 发送至少一个插入订户数据消息，如箭头 309 所示。该插入订户数据消息提供与 MS 200 相关联的订户数据。该订户数据被更新到与 MSS 220 相关联的 VLR 214。MSS 220 确认该插入订户数据消息，如箭头 310 所示。当所有插入订户数据消息都已经被 MSS 220 确认时，HLR 230 向 MSS 220 发送位置更新响应消息，如箭头 311 所示。由此，MSS 220 向 MS 200 发送 SIP 200 OK 消息，如箭头 312 所示。

[0044] 图 4 是图示了在本发明的一个实施例中在基于会话发起协议 (SIP) 的两个用户代理 (UA) 之间的移动台到移动台呼叫的消息序列图。用户代理是主叫方移动台即 MS 200 而被叫方移动台即 MS 452。主叫方称为 A- 方而被叫方称为 B- 方，因此将字母 A 和 B 指定给与相应方相关联的相应网元和地址。MS 200 由 MSS 220 处理，因此该 MSS 也称为主叫方的 MSS(MSS-A)。MS 452 由 MSS 450 处理，因此该 MSS 也称为被叫方的 MSS(MSS-B)。起初在时刻 t1，MS 200 的用户决定向 MS 452 进行传出呼叫。主叫用户通过选择或者输入作为根据 RFC3261 的 SIP URI 的 SIP-URI-B 来指明被叫方。MS 200 向其中当前注册有 MS 200 的 MSS 220 发送 SIP 邀请消息，如箭头 401 所示。当收 到 SIP 邀请消息时，MSS 220 向 LDAP 目录 232 发送 LDAP 搜索请求消息，如箭头 402 所示。LDAP 搜索请求消息至少包括被叫方 SIP-URI-B。当 SIP-URI-B 由 LDAP 目录 232 获得时，它被转译成 E.164 地址，即 MSISDN-B。LDAP 目录 232 向 MSS 220 发送至少包括 MSISDN-B 的 LDAP 搜索响应消息，如箭头 403 所示。

[0045] 当收到 LDAP 搜索响应消息和 MSISDN-B 时，MSS 220 现在能够使用 MSC 服务器的路由装置而无需利用 IMS 路由装置将呼叫路由到 MS452。MSC 服务器的路由装置类似于 GSM/UMTS 核心网络中电路交换呼叫的路由装置。类似地，对于 MSS 220 来说有可能使用迎合电路交换呼叫的补充服务之需的服务功能。另外，对于 MSS 220 来说有可能使用迎合电路交换呼叫之需的计费功能。也应当注意，由于主叫方 E.164 号码 MSISDN-A 可从在位置更新过程中执行的 LDAP 目录询问中获得，所以有可能在提供补充服务时也使用 MSISDN-A。例如，如果向 CSE 216 发送询问则可以使用 MSISDN-A 和 MSISDN-B 来代替 SIP 名以查询主叫方和被叫方，以便发起 CAMEL 补充服务。CAMEL 补充服务只需检查 E.164 地址而不是 SIP URI。

[0046] MSS 220 向 HLR 230 发送包括 MSISDN-B 的发送路由指令 (SRI) 消息，如箭头 404 所示。当收到发送路由指令消息时，HLR 230 获得与被叫订户相关联的订户数据。HLR 230 知道其中注册有被叫订户的 MSC 服务器和 VLR，即 MSS 450。如箭头 405 所示，HLR 又通过发送提供漫游号码 (PRN) 消息来询问 MSS 450 以及其中的 VLR。该漫游号码也称为移动台漫游号码 (MSRN)。VLR 然后使用如箭头 406 所示的消息向 HLR 230 提供漫游号码。该漫游然后用来向 MSS 450 路由呼叫。HLR 在它对 MSS 220 的响应消息 407 中对与被叫订户相关联的数据以及漫游号码进行封装，该 MSS 将根据 GSM/UMTS 电路交换核心网络充当网关 MSC。MSS 220 然后使用漫游号码在朝着 MSS 450 的方向上对呼叫进行路由。MSS 220 发送向 MSS 450 转发的 ISUP 初始地址消息 (IAM) 并且开始等待来自 MSS 450 方向的 ACM 消息，如箭头 408 所示。该 ISUP IMA 消息例如包括主叫方 E.164 地址即 MSISDN-A 和被叫方 E.164 地址即 MSISDN-B。当从 MSS 220 收到 IAM 消息 408 时，MSS 450 向 LDAP 目录 232 发送 LDAP 搜索

请求消息，如箭头409所示。该LDAP搜索请求消息例如包括来自ISUP IAM消息的MSISDN-A和MSISDN-B参数。响应于该LDAP搜索请求消息，LDAP目录232将MSISDN-A和MSISDN-B映射为SIP-URI-A和SIP-URI-B。LDAP目录232发送包括SIP-URI-A和SIP-URI-B的LDAP搜索请求响应消息，如箭头410所示。在已经从LDAP搜索响应消息收到SIP URI之后，MSS 450向MS 452发送SIP邀请消息，如箭头411所示。该SIP邀请消息至少包括用来向MS 452发送用户平面和信令平面分组的SIP-URI-A和SIP-URI-B参数以及IP地址。该IP地址在位置更新信令过程中已经提供给MSS 450。该IP地址与MS 452直接相关联或者它涉及如下SBC，SIP信令消息经由该SBC发送到MS 452。MSS 450向MSS 220发送ISUP地址完成消息(ACM)，如箭头412所示。由此，MSS 220向MS 200发送SIP尝试消息，如箭头413所示。

[0047] 在本发明的一个实施例中，在MSS 220与MSS 450之间使用SIP信令。例如在这一情况下，呼叫建立消息是SIP邀请消息。即使在MSS 220与MSS 450之间使用SIP信令，仍有可能将MSISDN和漫游号码用于将呼叫路由到MS 200。这允许维持利用E.164号码而不是SIP名的传统补充服务和计费机制。

[0048] 在本发明的一个实施例中，与给定的MS相关联的用户平面和信令平面分组具有不同的IP地址。在本发明的一个实施例中，IP地址涉及通用分组无线系统(GPRS)网关GPRS支持节点(GGSN)内的分组数据协议上下文(PDP)。

[0049] 图5是描绘了用于在通信系统中将通信路由到会话发起协议(SIP)用户代理的方法的一个实施例的流程图。

[0050] 在步骤502，第一MSS等待来自MS的位置更新消息。如果没有收到消息，则该方法在步骤502继续。

[0051] 在步骤504，第一MSS将在来自MS的位置更新消息中接收的SIPURI映射为与MS相关联的IMSI。

[0052] 在步骤506，第一MSS向HLR发送位置更新请求。在该位置更新请求消息中指明了与MS相关联的IMSI。

[0053] 在步骤508，第二MSS接收发往MS的呼叫建立请求。该呼叫请求至少提供与MS相关联的MSISDN。

[0054] 在本发明的一个实施例中，呼叫建立请求仅提供与MS相关联的SIP URI。第二MSS将SIP URI映射为与MS相关联的MSISDN。

[0055] 在步骤510，第二MSS使用与MS相关联的MSISDN来询问HLR并且保留来自第一MSS的漫游号码以便将呼叫路由到MS。可以从与第一MSS有关联的访问位置寄存器保留漫游号码。

[0056] 在步骤512，第二MSS使用漫游号码将呼叫建立请求路由到第一MSS。

[0057] 在步骤514，第一MSS接收呼叫建立请求。在本发明的一个实施例中，第一MSS将与MS相关联的MSISDN映射为与MS相关联的SIPURI。

[0058] 在步骤516，第一MSS检验呼叫建立请求中的主叫方号码是否可以映射为与主叫方相关联的SIP URI。例如可以通过分析主叫方号码并且确定该号码是否包括指示了主叫方号码可以映射为SIP URI的前缀来执行该检验。

[0059] 图6是图示了本发明的一个实施例中的移动交换中心服务器(MSS)的框图。在图

6 中有移动交换中心服务器 (MSS)600。MSS 600 包括呼叫控制 (CC) 实体 602 和移动性管理实体 610。该呼叫控制实体与会话发起协议 (SIP) 实体 604 通信，该 SIP 实体又例如与移动台如图 2 中的移动台 200 通信。呼叫控制实体 602 也与用来访问归属位置寄存器的移动应用部分 (MAP) 实体通信。呼叫控制实体 602 也可以与 ISUP 实体通信以便建立、维护和释放呼叫。移动性管理实体 610 经由移动应用部分实体 606 与归属位置寄存器通信。在归属位置寄存器中更新移动台位置时使用移动性管理实体 610。经由会话发起协议实体 604 从移动台接收去往移动性管理实体 610 的注册请求。移动性管理实体 610 和呼叫控制实体 602 使用轻型目录访问协 议 (LDAP) 实体 612 来与目录通信。在本发明的一个实施例中，移动性管理实体 610 也包括访问位置寄存器。

[0060] 对于本领域技术人员不言而喻，随着技术的发展，本发明的基本思想可以用各种方式来实施。本发明及其实施例因此不限于上述例子；而代之以它们可以在权利要求书的范围内进行改变。

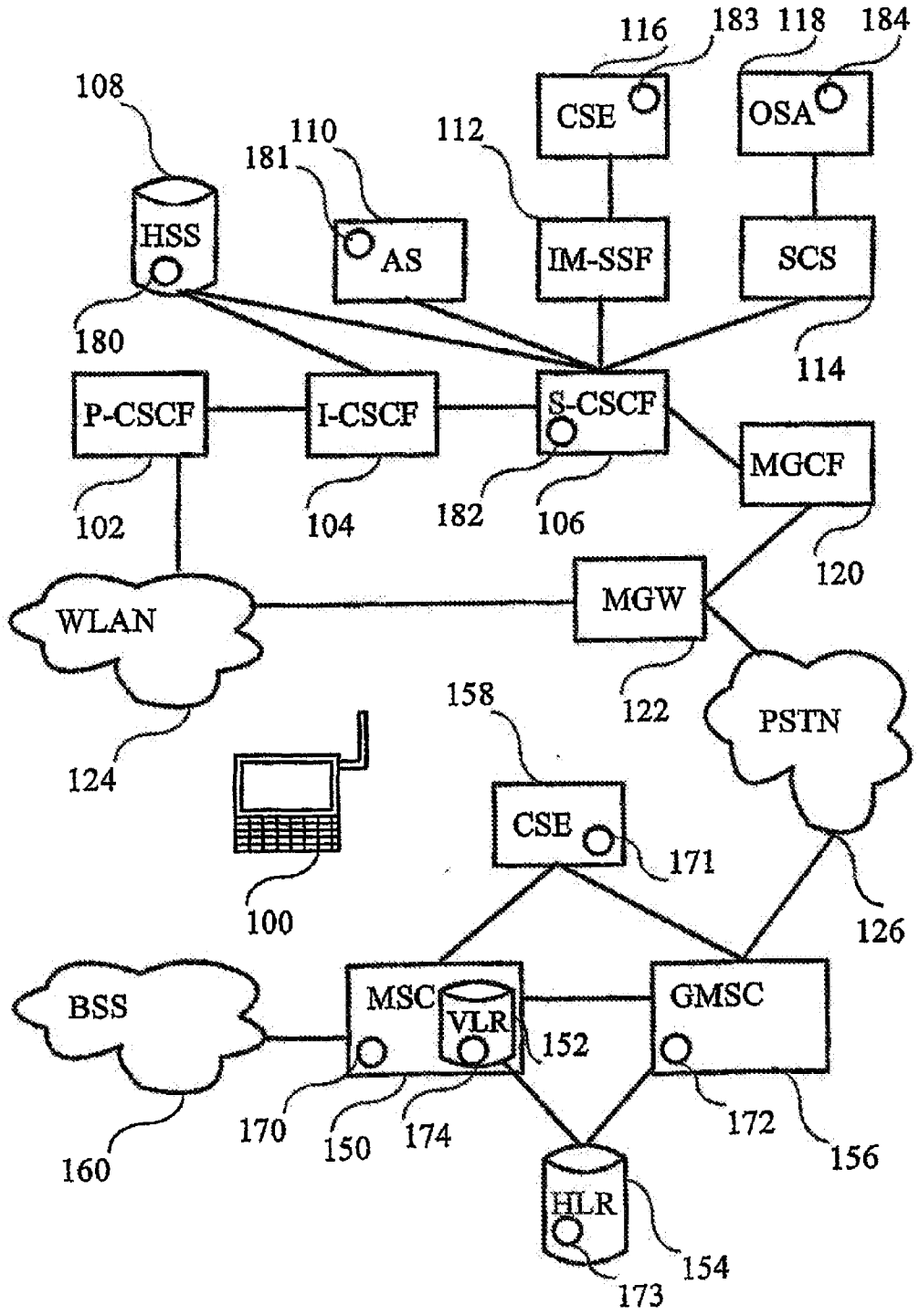


图 1 （现有技术）

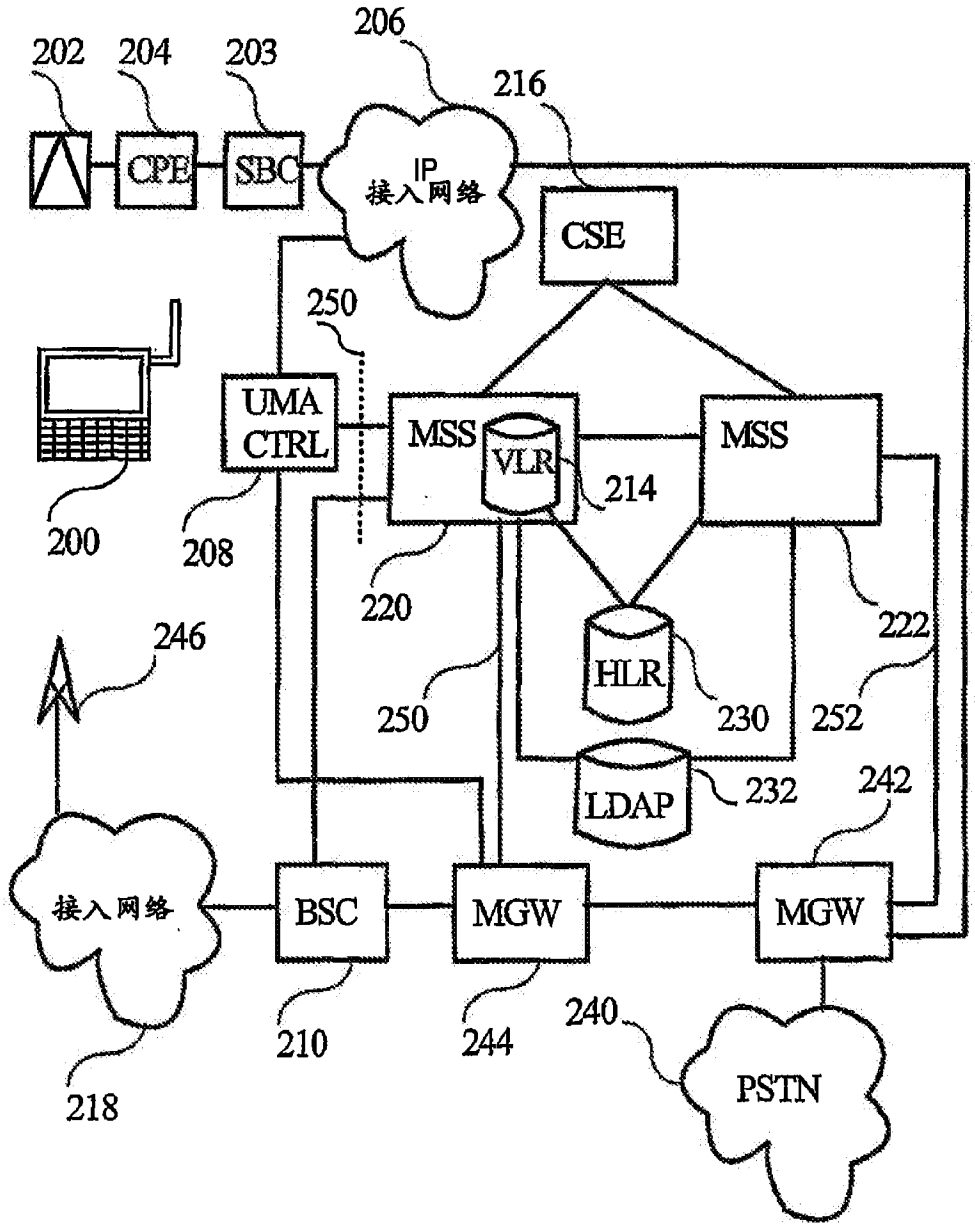


图 2

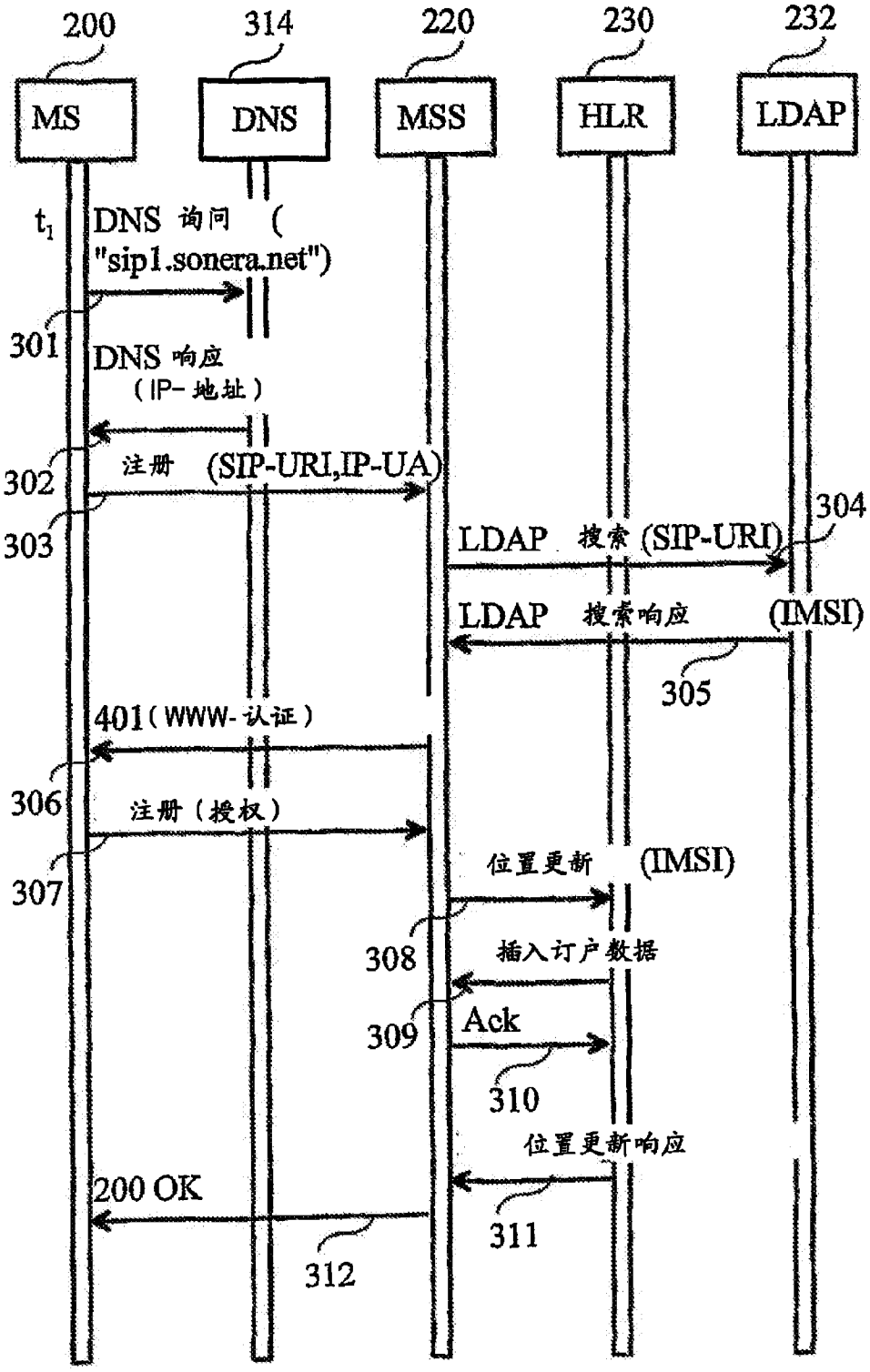


图 3

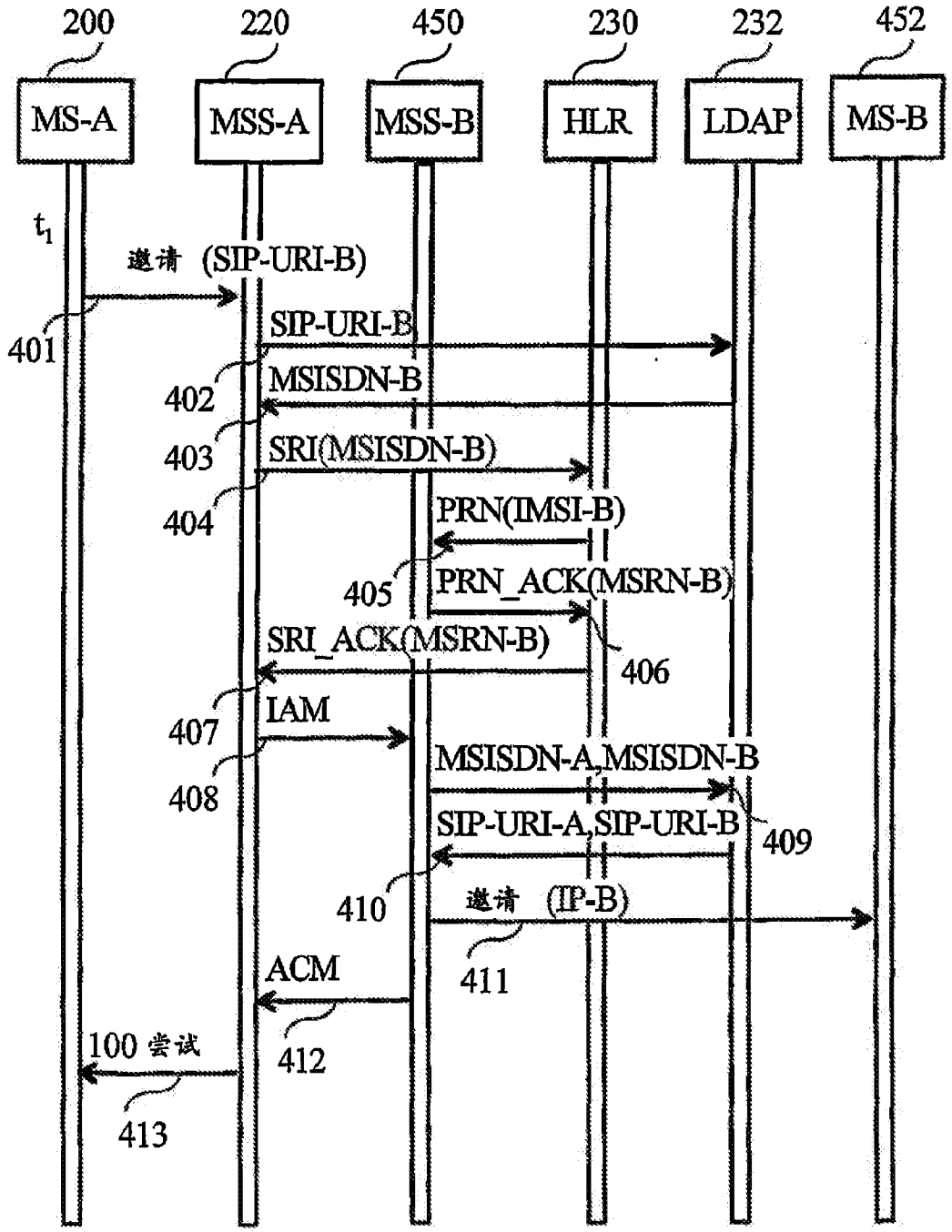


图 4

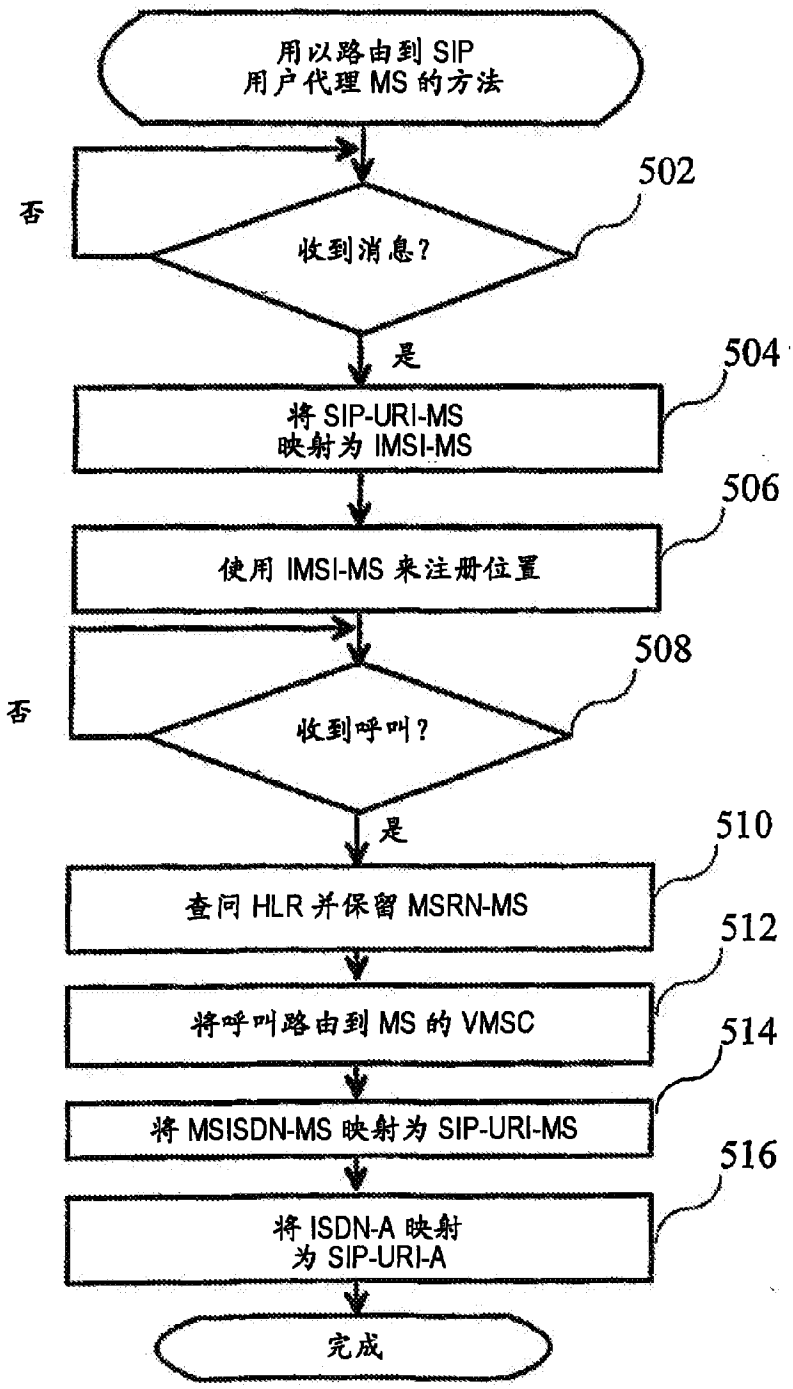


图 5

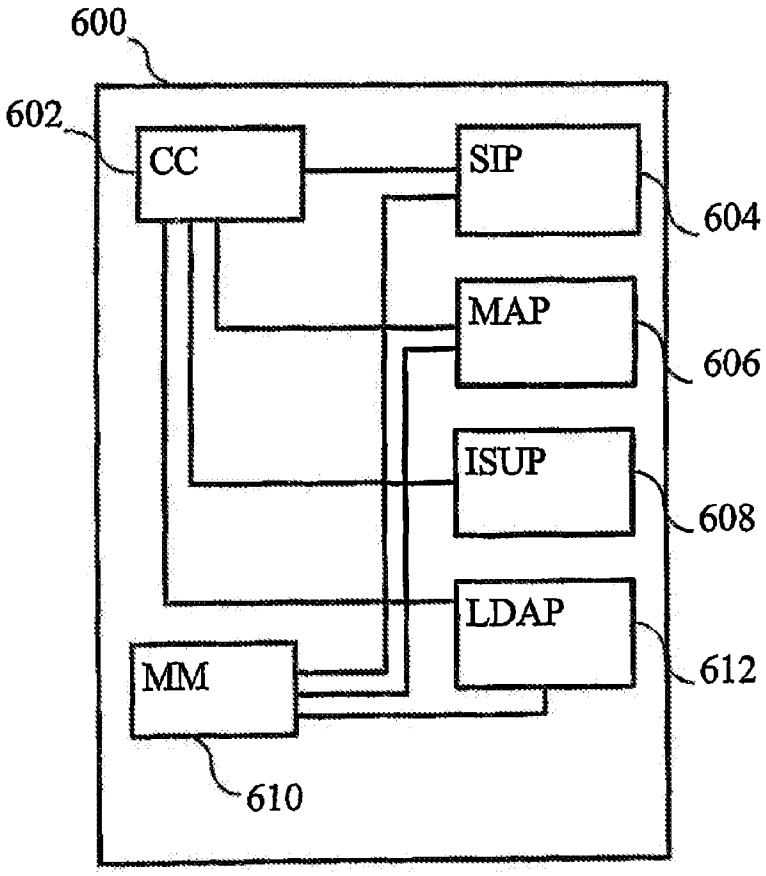


图 6

Espacenet

Bibliographic data: CN102484656 (A) — 2012-05-30

Method and apparatus for relaying packets

Inventor(s): ARI KERAENEN; JANI HAUTAKORPI; JOUNI MAEENPAEAE + (KERAENEN ARI, ; HAUTAKORPI JANI, ; MAEENPAEAE JOUNI)

Applicant(s): ERICSSON TELEFON AB L M + (ERICSSON TELEFON AB. L. M)

Classification: - international: ***H04L29/12***
- cooperative: **H04L29/12537; H04L61/2578; H04L61/2589**

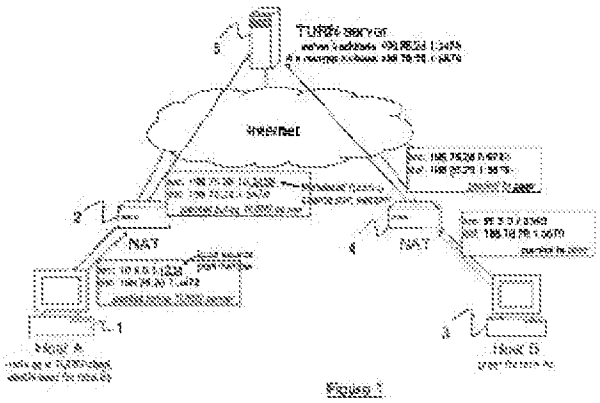
Application number: CN20098160227 20090629

Priority number (s): WO2009EP58129 20090629

Also published as: WO2011000405 (A1) US2012099599 (A1) US8611354 (B2) RU2012102911 (A) EP2449749 (A1) EP2449749 (B1) less

Abstract of CN102484656 (A)

Apparatus for relaying packets between a first host and a second host. The apparatus comprises a memory for registering for said first host; an address of the first host, a relayed address of the first host, an address of the second host, and an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier. The apparatus further comprises and one or both of : an outbound packet inspector for inspecting packets received from said first host and addressed to an address of the apparatus to determine whether or not they contain a registered outbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the second host; and an inbound packet inspector for inspecting packets received from said second host and addressed to said relayed address to determine whether or not they contain a registered inbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the first host.



(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102484656 A
(43)申请公布日 2012.05.30

(21)申请号 200980160227.X

(22)申请日 2009.06.29

(85)PCT申请进入国家阶段日
2011.12.29

(86)PCT申请的申请数据
PCT/EP2009/058129 2009.06.29

(87)PCT申请的公布数据
WO2011/000405 EN 2011.01.06

(71)申请人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩

(72)发明人 A·克拉南 J·豪塔科皮
J·马恩帕

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 姜冰 朱海煜

(51)Int.Cl.
H04L 29/12(2006.01)

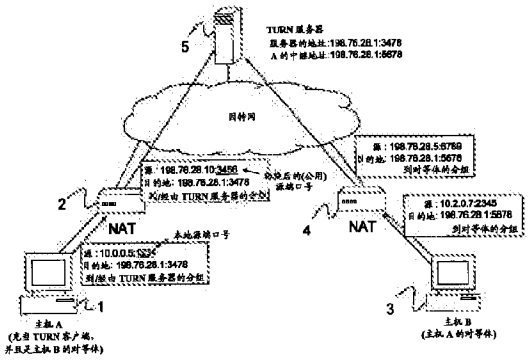
权利要求书 3 页 说明书 8 页 附图 6 页

(54)发明名称

用于中继分组的方法和设备

(57)摘要

用于中继第一主机和第二主机之间的分组的设备。该设备包括用于为所述第一主机登记第一主机的地址、第一主机的中继地址、第二主机的地址以及出站更高层标识符和/或入站更高层标识符的存储器。该设备还包括以下检验器的一个或两个:出站分组检验器,用于检验从所述第一主机接收的以及寻址到该设备的地址的分组,以确定它们是否包含登记的出站更高层标识符,以及如果是,则转发所述分组到第二主机的所述地址;以及入站分组检验器,用于检验从所述第二主机接收到的和寻址到所述中继地址的分组,以确定它们是否包含登记的入站更高层标识符,以及如果是,则转发所述分组到第一主机的所述地址。



CN 102484656 A

1. 一种用于在第一主机和第二主机之间中继分组的设备，所述设备包括：

存储器，用于为所述第一主机登记

所述第一主机的地址，

所述第一主机的中继地址，

所述第二主机的地址，以及

出站更高层标识符和 / 或入站更高层标识符；

以及以下检验器的一个或两个：

出站分组检验器，用于检验从所述第一主机接收的以及寻址到所述设备的地址的分组，以确定它们是否包含登记的出站更高层标识符，并且如果是，则用于转发所述分组到所述第二主机的所述地址；

入站分组检验器，用于检验从所述第二主机接收的以及寻址到所述中继地址的分组，以确定它们是否包含登记的入站更高层标识符，并且如果是，则用于转发所述分组到所述第一主机的所述地址。

2. 根据权利要求 1 的设备，所述出站分组检验器配置成用所述中继地址来替换要被转发到所述第二主机的分组的源地址字段中的所述第一主机的地址。

3. 根据权利要求 1 或 2 的设备，所述入站分组检验器配置成用所述第一主机的所述地址来替换要被转发到所述第一主机的分组的目的地地址字段中的所述中继地址，并且用所述设备的地址来替换那些分组的源地址字段中的所述第二主机的所述地址。

4. 根据上述权利要求中任一项的设备，所述入站分组检验器配置成传递包含所述入站更高层标识符的分组到所述第一主机，而不用附加的中继封装。

5. 根据上述权利要求中任一项的设备，其中，所述存储器配置成为所述第一主机附加地登记所述入站和出站更高层标识符或所述入站和出站更高层标识符中每个标识符的偏移位置，所述偏移位置标识分组内的关联更高层标识符的位置，并且所述出站和入站分组检验器配置成使用相应偏移位置来确定更高层标识符的存在。

6. 根据上述权利要求中任一项的设备，其中，所述存储器以及所述入站分组检验器和所述出站分组检验器或所述入站分组检验器和所述出站分组检验器中的每个检测器配置成使用所述入站和出站更高层标识符中的一个或两个来附加地处理所述第一主机和一个或多个另外主机之间分组的中继。

7. 根据上述权利要求中任一项的设备，其中，所述第一主机位于网络地址转换器之后，并且所述第一主机的所述地址是所述第一主机的经过 NAT 的地址。

8. 根据权利要求 7 引用权利要求 4 时的设备，其中所述附加的中继封装是根据使用中继穿越绕行 NAT 协议的封装。

9. 根据权利要求 7 或 8 的设备，还包括客户端终端登记单元，用于登记所述第一主机和任何另外主机，所述登记单元配置成使用所述使用中继穿越绕行 NAT，TURN，协议。

10. 一种配置成经由中继服务器与对等体终端交换分组的客户端终端，所述客户端终端包括：

中继单元，用于向所述中继服务器登记，以便被所述中继服务器分配中继地址；

标识确定单元，用于确定在与所述对等体终端交换的分组中要使用的入站更高层标识符；

标识符登记单元，用于连同所述中继地址、所述客户端终端的地址以及所述对等体终端的地址向所述中继服务器登记所述入站更高层标识符；

分组处理机，用于使用所述入站更高层标识符将从所述中继服务器接收的分组与所述对等体终端关联。

11. 根据权利要求 10 的客户端终端，所述标识确定单元配置成确定要在与所述对等体终端交换的分组中使用的出站更高层标识符，以及所述标识符登记单元配置成连同所述入站更高层标识符向所述中继服务器登记所述出站更高层标识符。

12. 根据权利要求 9 或 10 的客户端终端，所述标识确定单元配置成通过标识和使用以下协议参数中的一个参数来确定出站和 / 或入站更高层标识符：

主机身份标签，HIT；

同步源 (SSRC) 标识符；

安全参数索引 (SPI)；

TCP 端口号。

13. 根据权利要求 10 或 12 中任一项的客户端终端，所述中继单元配置成实现 NAT 穿越并且所述客户端终端的所述地址是经过 NAT 的地址。

14. 根据权利要求 13 的客户端终端，所述中继单元和所述标识符登记单元配置成使用使用中继穿越绕行 NAT，TURN，协议。

15. 根据权利要求 13 或 14 的客户端终端，还包括另外的分组处理机，用于如果所述标识确定单元不能确定入站更高层标识符、以及可选的出站更高层标识符，或 TURN 封装的分组从所述中继服务器被接收，则使用使用中继穿越绕行 NAT，TURN，封装来对于对等体终端发送和 / 或接收数据。

16. 根据权利要求 13 到 15 中任一项的客户端终端，所述中继单元配置成确定中继服务器是否支持基于更高层标识符的中继方法，以及如果否，则使用中继封装来发起与所述对等体终端的分组路由。

17. 一种在第一主机和第二主机之间发送分组的方法，所述方法包括：

代表所述第一主机在中继服务器进行登记

所述第一主机的地址，

所述第一主机的中继地址，

所述第二主机的地址，以及

出站更高层标识符和 / 或入站更高层标识符；

以及以下步骤中的一个或两个：

在所述中继服务器，检验从所述第一主机接收的以及寻址到所述中继服务器的地址的分组，以确定它们是否包含所述出站更高层标识符，以及如果是，则转发所述分组到所述第二主机的所述地址；

检验从所述第二主机接收的以及寻址到所述中继地址的分组，以确定它们是否包含所述入站更高层标识符，以及如果是，则转发所述分组到所述第一主机的所述地址。

18. 根据权利要求 17 的方法，其中，所述第一主机位于网络地址转换器之后。

19. 根据权利要求 18 的方法，使用使用中继穿越绕行 NAT，TURN，协议来实行所述登记步骤。

20. 根据权利要求 19 的方法，还包括如果从所述第二主机接收的分组不包含所述入站更高层标识符，则使用 TURN 封装来转发来自所述中继服务器的分组到所述第一主机。

用于中继分组的方法和设备

技术领域

[0001] 本发明涉及用于中继分组的方法和设备。它适用于实现网络地址转换 (NAT) 服务器的穿越并且特别适用于利用使用中继穿越绕行 NAT(Traversal Using Relays around NAT)(TURN) 协议的这种方法和设备。

背景技术

[0002] 网络地址转换 (NAT) 是在穿过业务路由装置时为了将给定地址空间重新映射到另一个的目的而修改数据报分组报头中的网络地址信息的过程。结合网络伪装（或 IP 伪装）来使用 NAT，网络伪装（或 IP 伪装）是一种隐藏整个地址空间的技术，地址空间通常由私有网络地址组成，其在另一个通常是公用地址空间中的单个 IP 地址后。在路由装置中实现这个机制，其使用状态转换表来将“隐藏”地址映射到单个地址，并且然后在出口重写外出的因特网协议 (IP) 分组，使得它们看上去是起始于路由器。在反向通信路径上，使用在转换表中存储的规则（“状态”）来将响应映射回起始 IP 地址。在没有新业务刷新其状态的短时间段之后，清除以这个方式建立的转换表规则。

[0003] 当然，网络地址转换的使用意味着因特网中的许多主机不能够被其它主机直接联系，因为它们位于阻止入站 (inbound) 连接的网络地址转换器 (NAT) 之后。不同的 NAT 穿越技术，例如，交互式连接性建立 (ICE)【参见 J. Rosenberg 的 Interactive Connectivity Establishment(ICE) :A Protocol for Network Address Translator(NAT)Traversal for Offer/Answer Protocols. draft-ietf-mmusicice-19（进行中的工作）2007 年 10 月】已经被开发以克服这个问题，但是对于某些种类的 NAT，在两个主机之间创建对等连接的唯一方式是通过对等体双方（包括 NAT 之后的一个对等体或多个对等体）都能够联系的节点来中继所有业务。

[0004] 使用中继穿越绕行 NAT(TURN)【参见 Traversal Using Relays around NAT(TURN) :Relay Extensions to Session Traversal Utilities for NAT(STUN). draft-ietf-behave-turn-15（进行中的工作）2009 年 2 月】允许主机（也就是 TURN 客户端）在 TURN 服务器登记“中继地址”(IP 地址和端口号的组合)，使得“通过”TURN 服务器和 TURN 客户端之间的 NAT 来建立会话（注意，在 NAT 之后的主机发起的连接，一般将引起通过 NAT 来建立会话，并且经由它，向其发起连接的节点能够发送分组给该主机）。由远程对等体发起的到中继地址的连接被 TURN 服务器中继到 TURN 客户端，使得其经过 NAT 中的穿孔 (punched hole)。TURN 客户端能够经由 TURN 服务器来发送数据给对等体，使得从对等体的观点来看，数据看起来是起始于中继地址。通过使用 TURN 服务器，甚至是对于最具限制性类型的 NAT，都能够在两个对等体之间建立通信路径。

[0005] 在从 TURN 服务器获得中继地址后，TURN 客户端需要通过经由 NAT 发送周期性的保持存活消息到 TURN 服务器来维持其在 NAT 中的状态。为了最小化保持存活消息的量，TURN 允许与不同对等体之间的多个连接再用相同的中继地址。因此，无论对等体的数量，仅要求一组保持存活消息。除了降低保持存活业务的量以外，这个方法还节约 TURN 服务器处

和 NAT 处的公用端口，允许它们服务更大数量的同时存在的用户。

[0006] 在多个对等体连接被复用到 TURN 客户端和 TURN 服务器之间的一个连接上的情况下，有必要提供一种机制，其允许 TURN 服务器和 TURN 客户端在它们交换的数据分组内标识对等体。为了这个目的，将服务器和客户端之间发送的数据封装在 TURN 消息内。

[0007] TURN 封装增加了每分组的开销并且减少了 TURN 服务器和客户端之间的链路上的最大传送单元 (MTU)。开销问题在受限带宽环境（例如，当使用蜂窝数据连接时）中特别严重，并且对于在多个小分组中发送的数据（例如，实时音频）也特别严重。更重要的也许是，封装阻止使用无修改操作系统内核协议栈来接收和发送数据。这至少导致性能问题，因为数据需要在内核和用户空间进程之间被来回发送。在受限操作系统（例如在移动设备中普遍使用的那些操作系统）的情况下，当然不可能将分组反馈回内核协议栈或在栈处理后捕获分组。TURN 封装在这类情况下不是可行选项。

[0008] 因特网 (IETF) 草案 -“Traversal Using Relays around NAT :Relay Extensions to Session Traversal Utilities for NAT(2007 年 7 月 8 日）”提供了一种避免封装的机制。这个机制利用“设定活动目的地”请求。然而，该机制不允许多个会话被复用到 TURN 服务器到客户端的链路上。

发明内容

[0009] 本发明的目的是允许不使用封装而在客户端和中继服务器之间发送分组，并且其减轻了已知解决方案的问题。

[0010] 根据本发明的第一方面，提供了用于在第一主机和第二主机之间中继分组的设备。该设备包括 :存储器，用于为所述第一主机登记第一主机的地址、第一主机的中继地址、第二主机的地址以及出站 (outbound) 更高层标识符和 / 或入站更高层标识符。该设备还包括以下检验器中的一个或两个 :

[0011] 出站分组检验器，用于检验从所述第一主机接收的以及寻址到该设备的地址的分组，以确定它们是否包含登记的出站更高层标识符，以及如果是，则转发所述分组到第二主机的所述地址 ;以及

[0012] 入站分组检验器，用于检验从所述第二主机接收的并且寻址到所述中继地址的分组，以确定它们是否包含登记的入站更高层标识符，以及如果是，则转发所述分组到第一主机的所述地址。

[0013] 本发明的实施例允许在第一主机和充当中继服务器的该设备之间发送分组，而不用在入站和出站方向中的一个或两个中进行封装。能够降低第一主机和该设备之间的链路上占用的带宽，同时允许将多个会话复用到该链路上。

[0014] 出站分组检验器（如果存在）可以配置成 :用所述中继地址来替换要被转发到所述第二主机的分组的源地址字段中的第一主机的地址。

[0015] 入站分组检验器（如果存在）可以配置成 :用第一主机的所述地址来替换要被转发到所述第一主机的分组的目的地地址字段中的所述中继地址，并且用该设备的地址来替换那些分组的源地址字段中的第二主机的所述地址。入站分组检验器可以配置成将包含所述入站更高层标识符的分组传递到所述第一主机，而不用附加的中继封装。

[0016] 存储器可以配置成为所述第一主机附加地登记所述入站和出站更高层标识符或

所述入站和出站更高层标识符中每个标识符的偏移位置，该偏移位置标识分组内的关联的更高层标识符的位置，并且出站分组检验器和入站分组检验器配置成使用相应偏移位置来确定更高层标识符的存在。

[0017] 存储器以及所述入站分组检验器和所述出站分组检验器或所述入站分组检验器和所述出站分组检验器中的每个检验器可以配置成：使用入站和出站更高层标识符中的一个或两个来附加地处理所述第一主机和一个或多个另外主机之间分组的中继。

[0018] 本发明适用于这样的情况，其中所述第一主机位于网络地址转换器之后，并且第一主机的所述地址是第一主机的经过 NAT 的 (NATed) 地址。在这个情况下，任何附加中继封装是根据使用中继穿越绕行 NAT 协议的封装。充当中继服务器的该设备可以包括用于登记所述第一主机和任何另外主机的客户端终端登记单元，该登记单元配置成使用所述使用中继穿越绕行 NAT(TRUN) 协议。

[0019] 根据本发明的第二方面，提供了配置成经由中继服务器来与对等体终端交换分组的客户端终端。该客户端终端包括用于向中继服务器登记以便被中继服务器分配中继地址的中继单元，以及用于确定在与所述对等体终端交换的分组中要使用的入站更高层标识符的标识确定单元。该终端还包括标识符登记单元，用于连同所述中继地址、客户端终端的地址以及对等体终端的地址向所述中继服务器登记入站更高层标识符；并且包括分组处理机，用于使用所述入站更高层标识符将从所述中继服务器接收的分组与所述对等体终端关联。

[0020] 终端的标识符确定单元可以配置成确定在与所述对等体终端交换的分组中要使用的出站更高层标识符，其中所述标识符登记单元配置成连同入站更高层标识符向所述中继服务器登记出站更高层标识符。

[0021] 标识符确定单元可以配置成通过标识和使用以下协议参数之一来确定入站更高层标识符和 / 或出站更高层标识符：主机身份标签，HIT；同步源 (SSRC) 标识符；安全参数索引 (SPI)；TCP 端口号。

[0022] 中继单元可以配置成实现 NAT 穿越并且客户端终端的所述地址是经过 NAT 的地址。在这个情况下，中继单元和所述标识符登记单元可以配置成使用使用中继穿越绕行 NAT(TURN) 协议。可以提供另外的分组处理机，如果所述标识符确定单元不能确定从所述中继服务器接收了入站更高层标识符以及可选的、出站更高层标识符、或者 TURN 封装的分组，则该处理机用于使用使用中继穿越绕行 NAT(TURN) 封装来对于对等体终端发送和 / 或接收分组。

[0023] 中继单元可以配置成：确定中继服务器是否支持基于更高层标识符的中继方法，以及如果否，则使用中继封装来发起与所述对等体终端的分组路由。

[0024] 根据本发明的第三方面，提供了在第一主机和第二主机之间发送分组的方法。该方法包括代表第一主机在中继服务器登记第一主机的地址、第一主机的中继地址、第二主机的地址以及出站更高层标识符和 / 或入站更高层标识符。该方法还包括以下步骤中的一个或两个：

[0025] 在中继服务器，检验从所述第一主机接收的以及寻址到中继服务器的地址的分组，以确定它们是否包含所述出站更高层标识符，以及如果是，则将所述分组转发到第二主机的所述地址；以及

[0026] 检验从所述第二主机接收的以及寻址到所述中继地址的分组，以确定它们是否包含所述入站更高层标识符，以及如果是，则将所述分组转发到第一主机的所述地址。

[0027] 第一主机可位于网络地址转换器之后，在该情况下，可以使用使用中继穿越绕行NAT(TURN)协议来实行所述登记步骤。如果从第二主机接收的分组不包含所述入站更高层标识符，则可以使用TURN封装来转发从中继服务器向第一主机发送的分组。

附图说明

[0028] 图1示意性地示出涉及使用TURN的NAT穿越的网络通信情形；

[0029] 图2示出图1的网络情形中的以及与修改的TURN协议关联的登记信令；

[0030] 图3示意性地示出ESP分组格式；

[0031] 图4示出图1的网络情形中的分组中继；

[0032] 图5示意性地示出图1的网络情形中的TURN客户端和TURN服务器；

[0033] 图6是示出TURN服务器登记和分组中继过程的流程图；

[0034] 图7示意性地示出RTP分组格式；以及

[0035] 图8示意性地示出HIP分组格式。

具体实施方式

[0036] NAT穿越的问题已经在上面的TURN封装的上下文中被考虑。现在将描述对TURN的增强以及使用数据中继的其它NAT穿越方案。

[0037] 数据（其可能在其它情况下是TURN客户端和TURN服务器之间的TURN封装的对象）将经常在分组内的一贯位置处包括持续的更高层标识符(HLI)。这里建议在传输层协议之上利用这种HLI以替代TURN封装来复用/解复用分组。当TURN客户端想要不使用TURN封装来与对等体通信时，其首先检查TURN服务器以确定TURN服务器是否支持这里描述的HLI机制。如果是，则TURN客户端在TURN服务器登记一对HLI（一个入站和一个出站）。TURN服务器的HLI登记包含两个字节数组（每个HLI有一个），以及数组长度、偏移和对等体地址。对于入站业务，当TURN服务器接收到指向中继地址的分组时，它检查以查看分组数据是否匹配登记的入站HLI，以及如果其匹配，则它不用任何封装而将分组发送到TURN客户端，因为入站HLI将向TURN客户端独特地标识对等体地址。当TURN服务器接收到来自TURN客户端的分组时，它检查以查看分组数据是否匹配登记的出站HLI，以及如果其匹配，则分组被发送到对于该出站HLI被登记的对等体地址（通过NAT向TURN客户端分配公用地址，即客户端的“经过NAT的”的地址，其作为在TRUN服务器处接收的分组的源地址而被包括，并根据正常TURN行为，被转变为中继地址）。

[0038] HLI能够是其值和位置在数据被发送或接收之前就已知的任何字节数组。数组的长度和其偏移（即在传输层报头之后的多少字节HLI开始）能够在（由TURN客户端）向TURN服务器登记HLI时定义。例如，在UDP封装的ESP[RFC3948]的情况下，SPI值能够作为HLI来使用。如果TCP在UDP上进行隧道化并且通过TURN服务器来中继，则潜在HLI的另一个示例将是TCP端口号。实时传输协议(RTP)的同步源标识符是HLI的另一个示例。

[0039] TURN服务器用TURN封装将（从对等体）发送到中继地址的不匹配登记的HLI的分组转发到TURN客户端。从TURN客户端到达TRUN服务器的不包含对于任何登记的HLI

的匹配的任何数据分组将被假定为是 TURN 封装的。这个行为允许包括新的功能性的 TURN 服务器与遗留 TURN 客户端兼容，且对于不包括可用 HLI 的业务是可用的。

[0040] 如果与某一协议关联的数据仅仅需要在 TURN 客户端和单个对等体之间交换，则不同于其它并发中继协议的协议报头中的任何恒定字段都是足够的。例如，对于这个目的，协议版本号或神奇 cookie(magic cookie) 值能是足够的。“神奇 cookie”值（在这个上下文中）是协议报头中的恒定值，用于在相同的流中区分某些协议消息和与其它协议关联的消息。例如，STUN【RFC5389】(TURN 和 ICE 使用的协议）在所有消息中携带这个种类的标识符。

[0041] 另一方面，如果 TURN 客户端与多个对等体交换使用相同协议的消息，则需要对于每个对等体都不同的标识符。许多协议在每个分组中都具有用于数据的源和 / 或目的地的某一标识符（例如，HIP 发送方和接收方 HIT 或 RTP 同步源）。对其它协议，通过组合多个协议字段中的信息来生成 HLI 是必要的。

[0042] 通常 TURN 客户端隐含地知道出站 HLI 的值，因为其是起始分组和生成更高层消息的实体。如果外部协议栈（例如操作系统提供的 IPsec) 被使用并且栈生成用作 HLI 的值，则客户端可能需要从栈中查询或从发送的分组中查找该值。

[0043] 如果 TURN 客户端事先知道对等体的 HLI 值（例如，其是恒定协议字段或某些对等体总是使用相同的值），则在 TURN 服务器登记 HLI 之前不需要附加信令。例如，在 HIP 信令业务的情况下，因为 HLI 是根据主机身份来计算的，所以甚至在彼此联系之前，主机就知道将在 HIP 报头中使用的主机身份标签 (HIT)。因此，HIT 能够用作 HLI，而不用任何附加信令。然而如果 HLI 事先不为 TURN 客户端所知，则 TURN 客户端需要从协议信令中或自动地从第一接收的分组中学习 HLI 值。当然该信令（假定其通过 TURN 服务器并且不经由某一其它中继，例如 SIP 服务器或 HIP 中继服务器）或第一分组肯定是 TURN 封装的。作为示例，考虑使用 IKE[RFC4306] 或 HIP 设立的 IPsec 安全关联。主机协商将被插入到每个加密的 ESP 分组的开始处的 SPI 值。因此，在发送任何数据之前，TURN 客户端学习对等体的 SPI 值，其能够用作 HLI。描述的方法不要求对等体中对于 HLI 的任何支持，或甚至是对正常 TURN 的支持。确实要求对等体中的 HLI 支持的备选方法涉及 TURN 客户端（使用例如新的 STUN/TURN 消息）向对等体显式询问 HLI 的值。

[0044] 为了说明所建议的实现 TURN 而不一定要求 TURN 封装的方法，考虑 UDP 封装的 ESP 的情况。图 1 示意性地示出在 NAT2 之后的 TURN 客户端（主机 A)1。对等体（主机 B)3 也在 NAT4 之后，并且希望使用 UDP 封装的 ESP 来与主机 A 通信。这通过使用 TURN 服务器（或中继）5 来实现。图 1 示出在网络中的各种点处的分组中包括的示范源 (src) 和目的 (dst) IP 地址和端口号。图 2 示出与这个情形关联的信令。支持 HLI 扩展的 TURN 客户端首先使用标准 TURN 分配请求（步骤 1) 来在 TURN 服务器进行登记。客户端在请求消息中包括 HLI-SUPPORTED 参数，以测试 TRUN 服务器是否支持这个扩展。如果服务器支持 HLI 中继，则其用分配 OK 消息来响应（步骤 2)。然而如果 TURN 服务器不支持 HLI 中继，则其拒绝请求并且客户端能够不用扩展而向服务器登记或尝试某一其它 TURN 服务器。HLI-SUPPORTED 参数具有“要求理解”【RFC5389】的类型，使得如果（遗留）TURN 服务不认识它，则其拒绝请求。图 1 中的主机中的一个或两个可位于多个 NAT 之后。这并不改变中继过程的原理。

[0045] 接着，主机协商 IPsec 安全关联。为了这个目的，它们能够使用例如 HIP 或

IKE。协商能够通过 TURN 服务器或者使用某一其它中继服务（例如 HIP 中继服务器【id-hip-nat-traversal：参见 Basic HIP Extensions for Traversal of Network Address Translators. draft-ietf-hip-nat-traversal-06（进行中的工作）. 2009 年 3 月】）或对等覆盖网络来进行。如果在 IPsec 信令中涉及 TURN 服务器，则信令消息在 TURN 服务器和客户端之间是 TURN 封装的，除非已经为信令协议设定 HLI。

[0046] TURN 客户端然后请求对等体的“准许”并且包括应该针对所有中继数据被检查的入站和出站 HLI（步骤 3）。TURN 服务器用准许 OK 来响应（步骤 4）。准许是正常 TURN 行为的一部分并且通过仅允许具有登记准许的对等体使用中继地址来增加安全。HLI 登记被搭载于标准准许登记过程上。因为客户端将使用 UDP 封装的 ESP，所以其登记（在地址 198.76.28.5 :6789 处）对等体的 SPI 值作为 HLI。在图 1 的示例中，入站 SPI 是‘0xA1B2C3D4”且出站 SPI 是“0xB2C3D4E5”。因为 SPI 总是在 ESP 包的前四个字节中，所以这两个参数都是四个字节长并且在 UDP 报头 (HLI 偏移是 0) 后立即开始。在 TURN 客户端，IPsec SA 中的对等体地址被设定成 TURN 服务器的地址，使得 IPsec 栈将以该对等体为目的地的 ESP 分组发送到 TURN 服务器。图 3 示出 ESP 的分组格式。

[0047] 图 4 示出在 TURN 客户端和对等体之间的 ESP 分组的交换（图中更低层的消息序列）并且其不要求 TURN 封装。当对等体发送不匹配登记的 HLI 的分组时（在这个示例中，除了 ESP 以外的东西，例如，NAT 穿越连接性检查消息或信令协议消息），用 TURN 封装来将数据转发到客户端（图 4 中的上层序列）。客户端能够通过封装响应并且在封装元数据中用信号通知对等体的地址来答复消息。当 TURN 服务器中继响应时，它移除 TURN 封装。在接收响应之后，对等体发送 UDP 封装的 ESP 分组，其具有匹配登记的 HLI 的 SPI。TURN 服务器检测到匹配并且不用任何封装来转发分组。TURN 客户端的 IPsec 栈接收数据并且相应地处理它。当使用 IPsec 的程序发送数据回对等体时，IPsec 栈自动发送数据（仅具有 UDP 封装）到 TURN 服务器。TURN 服务器检测到数据匹配登记的 HLI 并且将数据转发到其地址对于该 HLI 被登记的对等体。将容易明白的是，当利用这里描述的方法时，所交换的分组中的大部分不要求 TURN 封装。

[0048] 虽然上述方法使用简单的字节数组来匹配数据到准许，但是能实现更复杂的转发规则。例如，能用字节掩码来扩大字节数组并且允许对复用连接进行比特级检查。同样，不是只是单一的转发规则，而是 TURN 客户端能添加都匹配某一对等体地址的多个规则。甚至考虑了数据中的多个字节 / 比特位置的逻辑运算也能用于选择规则。这会使得以下成为可能：例如，不用封装而转发所有的分组到 TURN 客户端，除了涉及 NAT 穿越连接性检查的分组（以及对于其实际发送方地址信息是必要的分组）。

[0049] 图 5 示意性地示出配置成实现上面描述的方法的 TURN 服务器 5 和客户端终端 1（或 UE）（其中，在这些两个实体之间插入有 NAT）。在 UE 1 内，提供 NAT 穿越单元 6，其任务是向 TURN 服务器登记 UE，以便向 UE 分配中继地址。提供 HLI 确定单元 7 以确定对于朝向给定对等体的入站流和出站流二者都适当的 HLI。一旦被确定，这些 HLI 将被传给 HLI 登记单元 8，其向 TURN 服务器与对等体的地址相关联登记 HLI。登记详情还被传给分组处理机 9，其使用 HLI 以及对等体的地址来确定对于外出分组是否要求 TURN 封装，并且正确地路出进入分组到更高层。

[0050] 图 5 还示出 TURN 服务器 5。这包括客户端终端登记单元 10 以及关联存储器 11，

用于为 UE 1 登记 HLI 关联。入站分组检验器 12 配置成查验寻址到中继地址的分组以标识登记的入站 HLI，并且不用 TURN 封装来转发这类分组到 UE。出站分组检验器 13 配置成标识从 UE 接收的分组中的登记的出站 HLI，并且相应地将分组路由到对等体的目的地地址。当然将领会的是，TURN 服务器将并行为不同 UE（并且也潜在地为相同的 UE）处理多个 HLI 登记。

[0051] 图 6 是示出基于 HLI 的分组处理过程中的主要步骤的流程图。过程在步骤 100 开始，且在步骤 200，UE 向 TURN 服务器登记自身以获得中继地址。这个登记可以在用户决定发起会话之前发生。假定情况如此，在步骤 300 用户经由 UE 发起与对等体的会话。这个步骤可以响应于从对等体接收会话发起消息（例如，使用 TURN 封装经由 TURN 服务器或经由某一其它中继服务器来接收）。在步骤 400，UE 然后确定会话的入站 IILI 和出站 IILI，并且在步骤 500 向 TURN 服务器与对等体的地址关联登记这些。在这个登记步骤的完成之后，在步骤 600 和 700，UE 和 TURN 服务器处理数据（如所描述的），以避免 UE 和 TURN 服务器之间的 TURN 封装。并行执行步骤 600 和 700。

[0052] 以下小节示出 HLI 中继如何与除了 ESP 以外的某些示例协议一起使用。然而列举不是穷举的，并且本领域技术人员将领会所描述的方法适用于大量不同的协议。

[0053] 实时传输协议 (RTP)

[0054] RTP【RFC3550 :RTP :A Transport Protocol for Real-Time Applications. RFC3550. 2003 年 7 月】分组以固定报头开始，如图 7 中所示出的。用于标记来自不同源的流的 SSRC 字段包含随机数，要求该随机数在 RTP 会话内是全局独特的。当将 RTP 与 HLI 中继一起使用时，TURN 客户端设定其出站 IILI 以匹配它自己的 SSRC（其与某一对等体一起使用），并且设定其入站 HLI 来匹配对等体的 SSRC。

[0055] 主机身份协议 (HIP)

[0056] HIP【RFC5201 :Host Identity Protocol. RFC5201. 2008 年 4 月】分组报头逻辑上是 IPV6 扩展报头并且在图 8 中示出其格式。发送方和接收方主机身份标签 (HIT) 标识通信端点并且因此对于 HLI 是合适的。使用 HLI 中继的 TURN 客户端设定出站 HLI 以使“接收方的 HIT”匹配对等体的 HIT 并且设置入站 HLI 以使“发送方的 HIT”匹配对等体的 HIT。

[0057] 在 TCP 分组被封装在 UDP 中的情况下，TCP 端口号还可以用作 HLI。

[0058] 根据上面的讨论将明白，基于 HLI 的中继移除或降低 TURN 客户端和服务器之间的 TURN 封装所造成的带宽开销。同样，因为不需要在 TURN 客户端和服务器处添加或移除封装报头，处理开销也降低了。此外，由于没有封装要求，所以原生 (native) 操作系统栈能够用于处理中继数据。该解决方案与现有 TURN 客户端后向兼容并且不要求来自对等体的 HLI 支持。

[0059] 这里描述的扩展 TURN 服务器不是协议有关的，并且基于 HLI 的中继对于通过 UDP 携带的并且包含能够用于复用连接的足够标记的任何协议都是能够被实现的。甚至在协议不提供这类标记的情况下，如果不要求复用多个连接（例如，使用通过 TURN 服务器的仅单一连接），则能够使用具有零长度的 HLI 以使得 TURN 封装是不必要的。

[0060] 向 TURN 服务器登记的 IILI 可以更一般地被认为是规则集合。例如，在分组中不存在单个、独特的标识符的情况下，可指定例如“如果 HLI_1 在位置 1 处并且 HLI_2 在位置 2 中但是没有 HLI_3 在位置 3 中，则分组匹配中继规则 / 准许”的规则集合并且将其向 TURN

服务器登记。

[0061] 本领域技术人员将领会，可对上面描述的实施例进行各种修改，而不背离本发明的范围。例如，本方法可以应用于除了 TURN 以外的中继协议（并且其使用中继分组的封装），例如 SOCKS 5(IETF RFC

[0062] 1928)，并且实际上适用于例如目前指定的 TURN 协议的进一步增强。某些实施例可允许 TURN 服务器或者某一其它基于网络的节点来确定要用于会话的 HLI。在这个情况下，该确定节点可将 HLI 发信号通知到 TURN 客户端，并且如果节点自身不是 TURN 服务器，则还发信号通知到 TURN 服务器。本领域技术人员还将领会的是，这里描述的中继机制不仅对于 NAT 穿越是适用的。它例如能适用于客户端利用中继服务器以便维持匿名的情形。本领域技术人员还将领会，通过将这个基于 HLI 的方法应用在入站方向和出站方向中的仅一个而不是两个中，就可以实现益处。

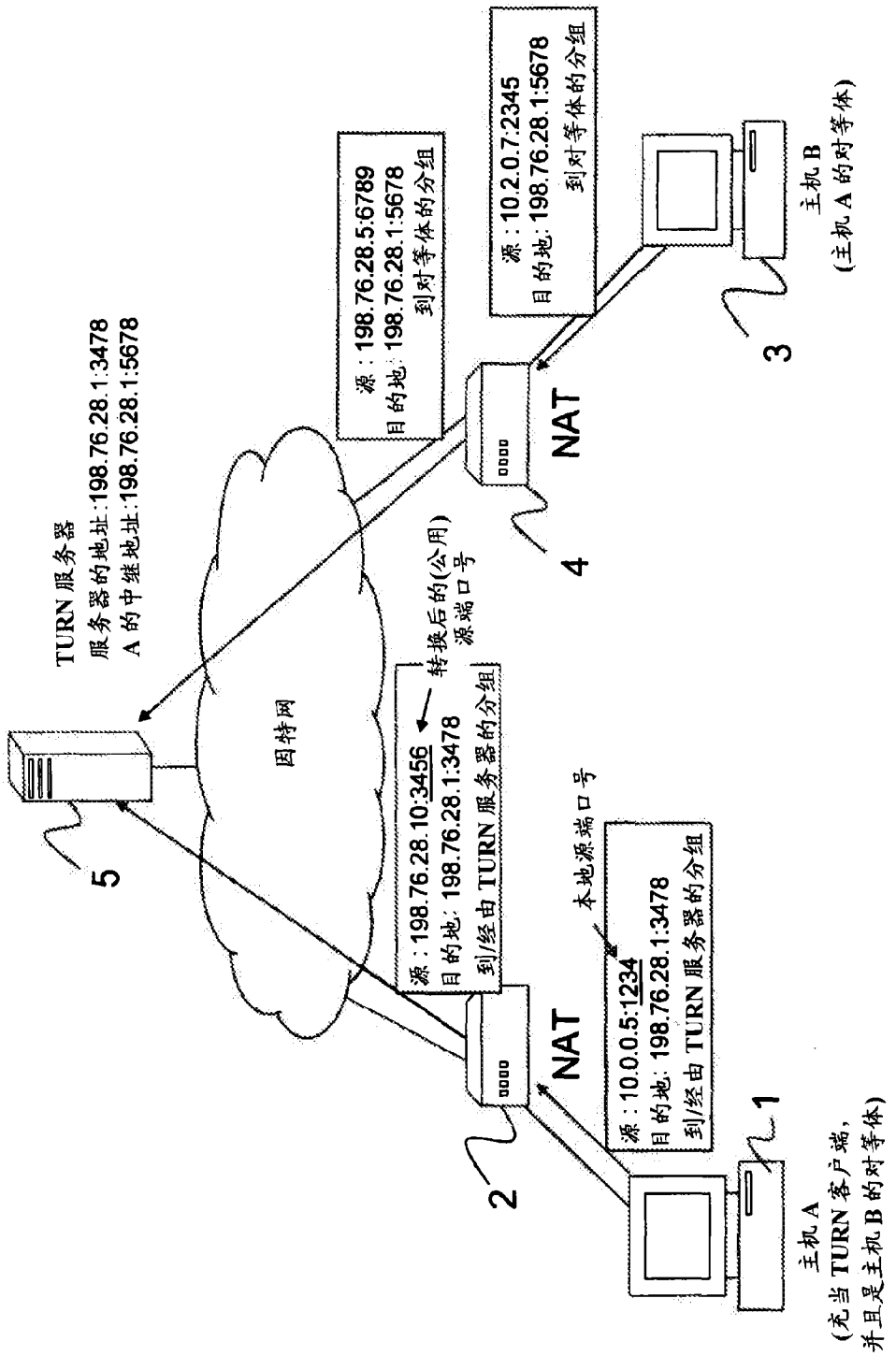


图 1

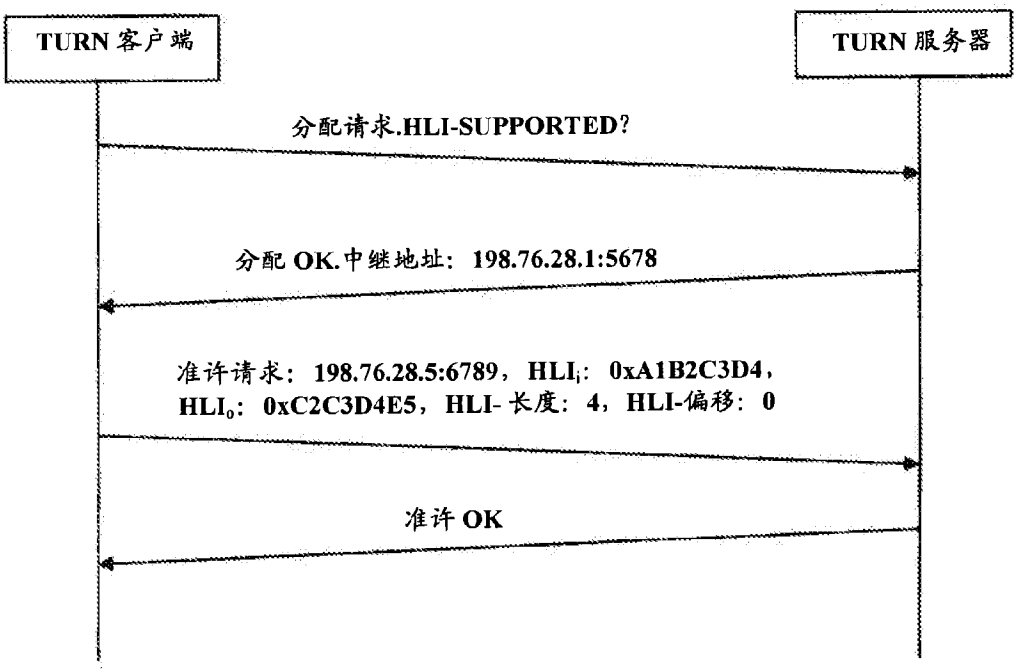


图 2

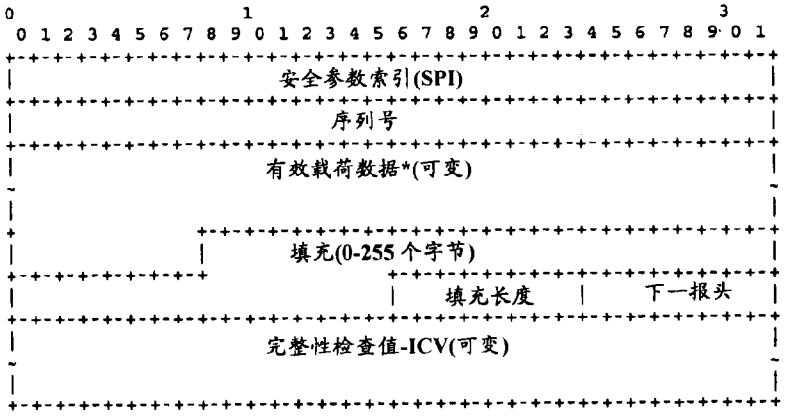


图 3

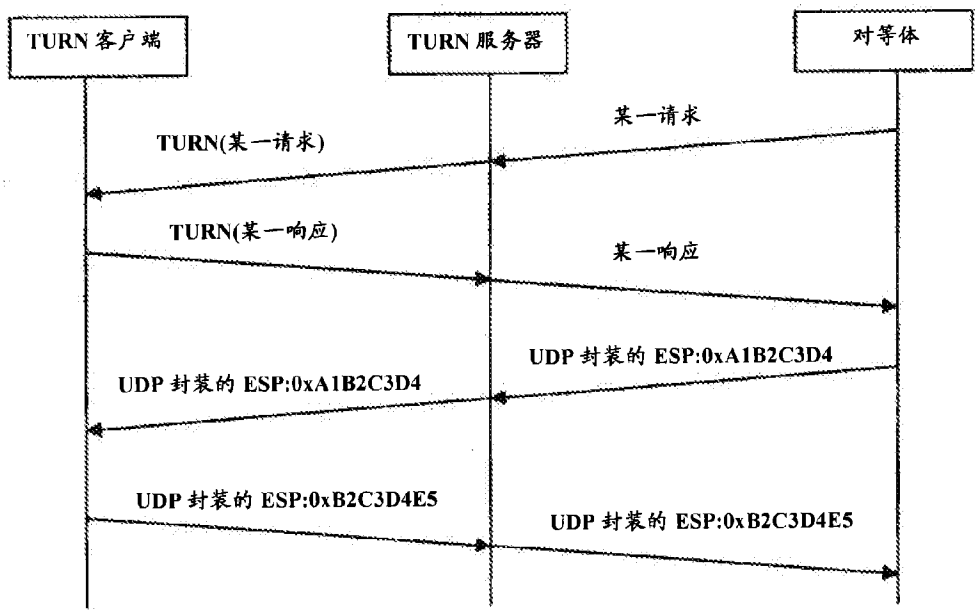


图 4

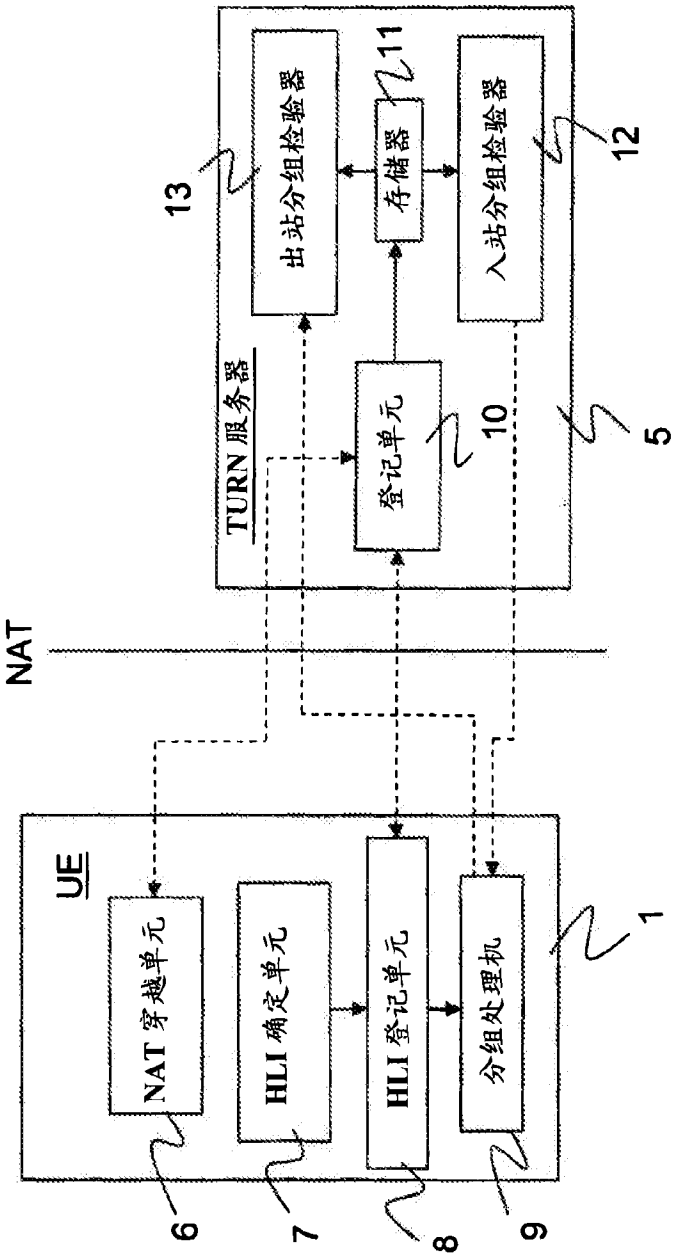


图 5

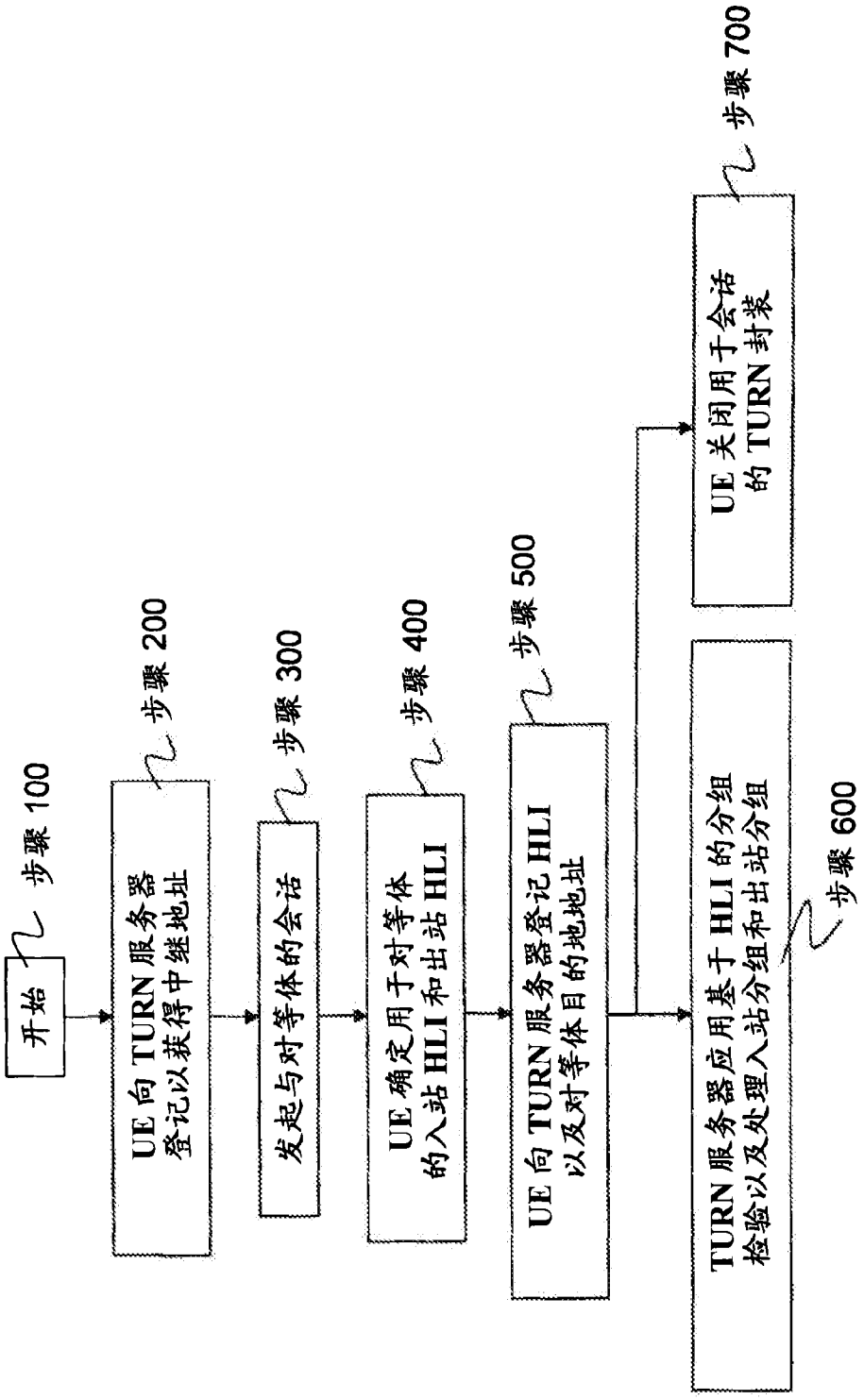


图 6

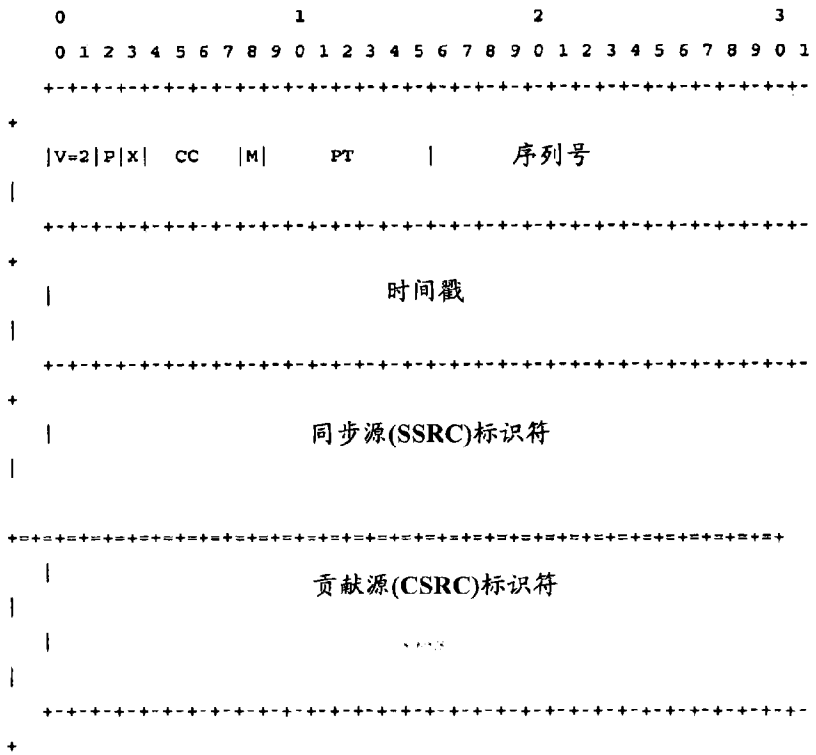


图 7

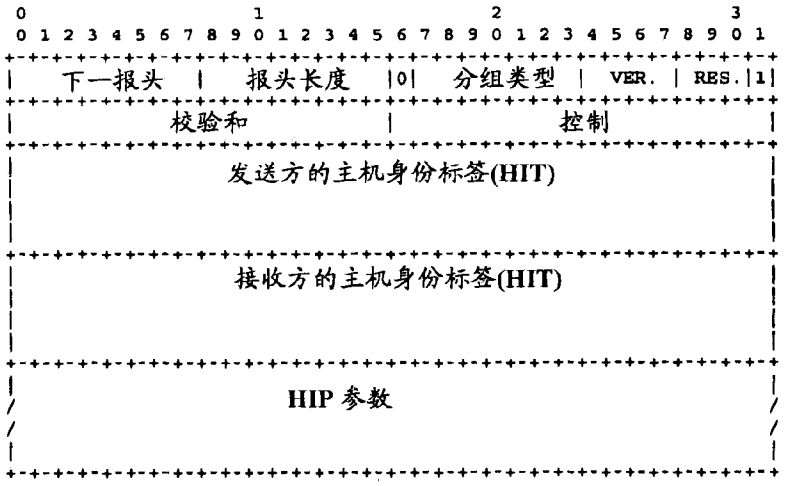


图 8

Espacenet

Bibliographic data: CN101095329 (B) — 2012-10-10

Distributed voice network

Inventor(s): GERALD LEBIZAY ± (LEBIZAY GERALD)

Applicant(s): INTEL CORP ± (INTEL CORP)

Classification: **- international:*H04L29/06***
- cooperative: G06Q20/102; H04L29/06027; H04L65/103; H04L65/104; H04L65/1043; H04L65/607

Application number: CN2005845760 20051229

Priority number(s): WO2005US47679 20051229 ; US20040027915 20041230

Also published as: CN101095329 (A) WO2006072099 (A1) US2012250624 (A1) US8605714 (B2) US2010008345 (A1) US8204044 (B2) US2006146797 (A1) US7593390 (B2) TWI307592 (B) GB2437666 (A) GB2437666 (B) DE112005003306 (T5) CN102833232 (A) less

Abstract of CN101095329 (B)

A method and apparatus (114, 116) that receives an IP packet and encapsulates the packet with an IP header. Further, time-domain multiplexed voice data is received and converted into VoIP packets. Still further, Signaling System (7) (SS7) compliant signals are decoded. The decoded (SS7) signals are received and encapsulated prior to transmission to a telephony device (102).

(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101095329 B
(45)授权公告日 2012.10.10

(21)申请号 200580045760.3

(22)申请日 2005.12.29

(30)优先权数据
11/027,915 2004.12.30 US

(85)PCT申请进入国家阶段日
2007.07.02

(86)PCT申请的申请数据
PCT/US2005/047679 2005.12.29

(87)PCT申请的公布数据
WO2006/072099 EN 2006.07.06

(73)专利权人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 G·利比扎伊

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 曾祥夌 魏军

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
Newman, P..In search of the all-IP mobile network.IEEE Communications Magazine12 42.2004,12(42),S3-S8.

Morand,L. et al..Global mobility approach with Mobile IP in "all IP" networks.IEEE International Conference on Communications, 20024.2002,42075-2079.

A.Dutta et al..Realizing mobile wireless Internet telephony and streamingmultimedia testbeb.Computer Communications27 8.2004,27(8),725-738.

审查员 胡延

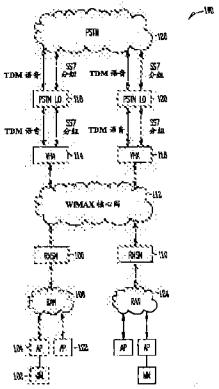
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

分布式语音网络

(57)摘要

一种接收IP分组并封装分组与IP首标的方法及设备(114,116)。此外,时域复用语音数据被接收并转换为VoIP分组。此外,对符合信令系统(7)(SS7)的信号解码。已解码(SS7)信号被接收,并在传送给电话装置(102)之前被封装。



CN 101095329 B

1. 一种用于语音通信的装置，包括：

封装电路，接收具有第一 IP 首标的 IP 分组，并在所述分组前面附加第二 IP 首标；

基于 IP 的语音 VoIP 电路，接收时域复用语音数据，并把所述数据转换为 VoIP 分组；

信令电路，对符合 7 号信令系统 SS7 的信号解码；以及

控制电路，用于

从所述信令电路接收已解码 SS7 信号，并把所述已解码 SS7 信号传递给所述封装电路，以便传送给电话装置；以及

从所述 VoIP 电路接收 VoIP 分组，并把所述 VoIP 分组传递给所述封装电路，以便传送给所述电话装置。

2. 如权利要求 1 所述的装置，其特征在于，所述封装电路、VoIP 电路、信令电路和控制电路被实施为与存储装置进行数据通信的微处理器。

3. 如权利要求 1 所述的装置，其特征在于：

所述封装电路被实施为第一刀片，所述 VoIP 电路被实施为第二刀片，所述信令电路被实施为第三刀片，以及所述控制电路被实施为第四刀片；以及

所述第一、第二、第三和第四刀片相互进行数据通信。

4. 如权利要求 3 所述的装置，其特征在于，所述第一、第二、第三和第四刀片经由局域网进行通信。

5. 如权利要求 3 所述的装置，其特征在于，所述第四刀片还配置成维护涉及移动电话装置的电话号码、移动 IP(MIP) 地址和转交地址的数据库。

6. 如权利要求 3 所述的装置，其特征在于，所述第一刀片包括到 IP 网络的接口。

7. 如权利要求 3 所述的装置，其特征在于，所述第二刀片包括到传送时域复用语音数据的网络的接口。

8. 如权利要求 3 所述的装置，其特征在于，所述第三刀片包括到 SS7 网络的接口。

9. 一种用于语音通信的系统，包括：

封装电路，接收具有第一 IP 首标的 IP 分组，并在所述分组前面附加第二 IP 首标；

基于 IP 的语音 VoIP 电路，接收时域复用语音数据，并把所述数据转换为 VoIP 分组；

计费电路，配置成测量所述系统的使用的持续时间和类型，以及使这类测量与用户帐户相关；

信令电路，对符合 7 号信令系统 SS7 的信号解码；以及

控制电路，用于

从所述信令电路接收已解码 SS7 信号，并把所述已解码 SS7 信号传递给所述封装电路，以便传送给电话装置；以及

从所述 VoIP 电路接收 VoIP 分组，并把所述 VoIP 分组传递给所述封装电路，以便传送给所述电话装置。

10. 如权利要求 9 所述的系统，其特征在于，所述封装电路、VoIP 电路、信令电路、计费电路和控制电路被实施为与存储装置进行数据通信的微处理器。

11. 如权利要求 9 所述的系统，其特征在于：

所述封装电路被实施为第一刀片，所述 VoIP 电路被实施为第二刀片，所述信令电路被实施为第三刀片，以及所述控制电路和计费电路被共同实施为第四刀片；以及

所述第一、第二、第三和第四刀片相互进行数据通信。

12. 如权利要求 11 所述的系统，其特征在于，所述第一、第二、第三和第四刀片经由局域网进行通信。

13. 如权利要求 11 所述的系统，其特征在于，所述第四刀片还配置成维护涉及移动电话装置的电话号码、移动 IP(MIP) 地址和转交地址的数据库。

14. 如权利要求 11 所述的系统，其特征在于，所述第一刀片包括到 IP 网络的接口。

15. 如权利要求 11 所述的系统，其特征在于，所述第二刀片包括到传送时域复用语音数据的网络的接口。

16. 如权利要求 11 所述的系统，其特征在于，所述第三刀片包括到 SS7 网络的接口。

分布式语音网络

技术领域

[0001] 本发明的实施例涉及在移动无线宽带网络上实现的基于 IP 的语音技术。

背景技术

[0002] 基于 IP 的语音 (VoIP) 技术允许各方通过分组交换 IP 网络进行口头通信。VoIP 技术在不断地普及，并且根据某些因素，可提供可与公共交换电话网 (PSTN) 相比的声音质量。

[0003] 不断普及的还有无线移动网络。无线移动网络允许装置链接到网络，无需物理导电线路在装置与网络之间传送数据。此外，这类网络通过允许装置以对于无线移动网络域外部的网络单元或节点透明的方式改变接入点来允许移动性。

[0004] 尽管 VoIP 技术和无线移动网络的普及性不断增长，但是对于基于因特网的当前 VoIP 服务没有移动客户装置。阻碍这类移动装置的进步的一个因素涉及找出用以在表现为保持单一 IP 地址的同时可允许移动装置在大地理区域漫游（因而可能在域之间来回移动）的简单方案。用户数据报协议 (UDP) 通过使用包含两个连接端点的 IP 地址和端口号的四元组对连接进行索引。改变这四个号码中的任一个使连接被中断和丢失。因此，重要的是，该装置表现为在地理上漫游的同时保持相同的 IP 地址。解决这个问题的困难随着允许装置在其中漫游的地理区域增大而增加。

[0005] 通过上述明显看到，需要一种方案，通过该方案，可允许无线 IP 电话装置在地理上的大区域、如都市区域漫游。希望这种方案比较简单地实现为在现有无线网络上的重叠。还希望这种方案易于与 PSTN 互连。

附图说明

[0006] 图 1 说明在其中采用语音归属代理的一个实施例的网络环境。

[0007] 图 2 说明根据本发明的一个实施例构成语音归属代理的协议栈。

[0008] 图 3 说明图 2 所示的协议栈的移动 IP 层所采用的隧道技术方案。

[0009] 图 4 说明根据本发明的一个实施例发起 VoIP 电话呼叫的方法。

[0010] 图 5 说明根据本发明的一个实施例执行 VoIP 电话呼叫的方法。

[0011] 图 6 说明根据本发明的一个实施例在其中可实施语音归属代理的硬件环境。

具体实施方式

[0012] 图 1 说明网络环境 100，在其中，可允许一个或多个移动节点 102 在地理上的大区域、例如在都市区域进行漫游。移动节点 102 经由数字传输（通常以 2 至 6GHz 许可频带，其中典型信道带宽的范围是从 1.5 至 20MHz）与接入点 104 通信。诸如由参考标号 104 标识的接入点（在本文中又称作基站）接收来自移动节点的传输，并把传输传递给关联区域接入网 106 中的网络单元。根据一个实施例，区域接入网 106 是一种有线网络（即，物理线路互连构成区域接入网的各个单元），它是一般的基于分组的接入网，例如以太网网络、IP/

MPLS 网络或 ATM 网络。接入点 104 与移动节点 102 之间的传输符合电气和电子工程师协会 (IEEE)802.16 标准信号，IEEE std.802.16-2001，2001 年发布，以及以后的版本（以下称作 IEEE 802.16 标准或 IEEE 802.16e 标准）。互连符合 IEEE 802.16e 标准的接入点（如 104）的区域接入网 106 称作 WiMAX 网络。

[0013] 在 WiMAX 区域接入网 106 的外围是无线电网络服务节点 108。无线电网络服务节点 108 提供其它 WiMAX 区域局域网、如参考标号 124 标识的 WiMAX 网络之间的路由选择和控制。各区域接入网 106 和 124 包括无线电网络服务节点 (108,110)，它把区域接入网 106 或 124 耦合到互连所有区域接入网 106 和 124 的 WiMAX 核心网 112。虽然 WiMAX 核心网 112 在图 1 中表示为互连两个 WiMAX 网络 106 和 124，但是 WiMAX 核心网 112 原则上可互连任何数量的区域接入网。

[0014] WiMAX 核心网 112 可以是普通 IP 网络，由常见的 IP 网络单元组成，例如允许高速数据传递的光纤网单元。因此，WiMAX 核心网 112 可直接与因特网（图 1 中未示出）互连。

[0015] 在 WiMAX 核心网 112 的外围是一个或多个语音归属代理 114 和 116。存在与各 WiMAX 区域接入网 106 和 124 关联的语音归属代理 114 或 116。下面详细论述语音归属代理 114 或 116 的结构或者由其制订的方法。简言之，语音归属代理是允许 WiMAX 核心网（例如核心网 112）与公共交换电话网 (PSTN)126 之间的 VoIP 综合的网络单元。另外，语音归属代理提供允许移动节点（例如移动节点 102）从一个 WiMAX 区域接入网（例如网络 106）漫游到另一个（例如 124）的功能性。

[0016] 虽然图 1 描绘了与各区域接入网 106 或 124 关联的单个语音归属代理 114 或 116，但是不止一个语音归属代理可与给定区域接入网关联。因此，虽然参考标号 114 和 116 在本文中用作表示单个语音归属代理，但是各参考标号 114 和 116 可理解为表示服务于它们相应的 WiMAX 区域接入网 106 和 124 的一组语音归属代理。

[0017] 各语音归属代理 114 和 116 把 WiMAX 核心网 112 与公共交换电话网 126 的本地局 118 或 120 接口。公共交换电话网 126 采用由国际电信联盟 (ITU) 电信标准化部门 (ITU-T) 定义的、称作 7 号信令系统 (SS7) 的带外信令方案。带外信令方案对于呼叫控制采用与用于承载呼叫本身的内容（例如语音数据）不同的物理路径。因此，如图 1 所示，语音归属代理用作两个分开的接口：用于作为时域复用数字语音数据来传送的语音数据的接口，以及用于作为 SS7 分组来传送的 SS7 控制信号的接口。

[0018] 诸如由参考标号 102 标识的移动节点之类的移动节点可被实施为电话手机（以与蜂窝电话相似的方式），可被实施为个人数字助理，或者可被实施为另一个移动计算装置。一旦上电，移动节点就向最接近的可用接入点进行初始传输。在传输时，接入点为移动节点分配管理信道，它向接入点标识移动节点。接入点和移动节点可在范围从一至五或十英里的距离上与另一个进行通信。给定这种区域的大小，其它移动节点可位于其中。因此，接入点可与数百个移动节点进行通信。管理信道的使用允许接入节点区分不同的接入点。

[0019] WiMAX 区域接入网中的各接入点具有标识它的 IP 地址。但是，这个 IP 地址仅在接入点所在的区域接入网（又称作域）中才起作用。因此，接入点可直接向它所在的区域接入网中的另一个接入点发送数据。为了把数据导向另一个域中的接入点，服务于接入点所在的特定域的无线电网络服务节点必须用作中间件。

[0020] 如上所述，在移动节点上电期间，为了建立管理信道并对用户鉴权，对基站进行初

始传输。此后，移动节点与服务于移动节点所在的域的语音归属代理进行初始通信。这个通信标记登记过程的开始，移动节点通过它来通知语音归属代理关于移动节点在哪一个域中。作为响应，语音归属代理对移动节点分配称作移动 IP(MIP) 地址的 IP 地址。语音归属代理还记录移动节点的转交地址。即使移动节点移动到它在其中与另一个接入点或者完全与另一个 WiMAX 区域接入网进行通信的地理区域，移动节点的 MIP 地址也不改变。另一方面，转交地址标识移动节点与之通信的域，因而在移动节点从一个区域接入网漫游到另一个区域接入网时会改变。

[0021] 语音归属代理可对移动节点分配不止一个 IP 地址。例如，移动节点可具有分配给它的用于传送语音数据的一个 IP 地址以及分配给它的用于传送信令数据的另一个 IP 地址。为了简单起见，本公开以下列假设继续进行：各移动节点在登记期间具有分配给它的单一 IP 地址。

[0022] 在登记时，语音归属代理更新它维护的数据库。数据库可包含与移动节点所支持的特征（呼叫等待、语音邮件等）有关的信息。数据库经过更新以便关联用来标识移动节点的电话号码、分配给移动节点的 MIP 地址以及移动节点所在的域（即，移动节点的转交地址）。

[0023] WiMAX 区域接入网 106 或 124 采用称作隧道技术的技术。利用这个技术，在给定 WiMAX 域 106 或 124 服务的地理区域内的移动节点的移动对于该域外部的网络单元或节点是透明的。因此，例如，WiMAX 域 106 外部的网络节点无法知道移动节点 102 是否正与接入点 104 或接入点 122 进行通信。域 106 外部的网络单元仅需要知道，移动节点 102 处于域 106 中以便与移动节点 102 通信。因此，每当移动节点（例如移动节点 102）从一个域移动到另一个域时，移动节点向它先前登记所用的语音归属代理重新登记。作为响应，语音归属代理更新其数据库，以便把新的转交地址（即，移动节点与之通信的域的网络地址）与该移动节点关联。

[0024] 前面的论述集中于语音归属代理 114 或 116 工作的网络环境。以下论述简要地提供组成语音归属代理 114 或 116 的协议层。

[0025] 图 2 说明语音归属代理 114 或 116 执行的协议栈 200。从图 2 中可以看到，协议栈 200 包括移动 IP(MIP) 层 202，它提供符合诸如“IP 移动性支持”(C. Perkins, ed., IETF RFC 2002, 1996 年 10 月）中所述的标准之类的工业公认 MIP 标准的功能性。MIP 层 202 提供的功能性可用于栈 200 的上层 204-210。

[0026] MIP 层提供以上所述的隧道技术功能性。图 3 说明接收具有 IP 首标 302 的分组 300 的 MIP 层 202。IP 首标 302 在其 32 位目标 IP 地址字段中包含分配给具体移动节点的 MIP 地址，因而称作 IP 首标 $_{MIP}$。对接收这种分组 300 进行响应，MIP 层 202 把分组 300 附接到第二 IP 首标 304。第二 IP 首标采用 MIP 地址标识的具体移动节点的转交地址，因而称作 IP 首标 $_{CareOf}$。因此，WiMAX 核心网 112 观察第二 IP 首标 304，并按照第二 IP 首标 304 来路由分组 300，表示分组 300 被路由到适当的域 106 或 124。在由移动节点接收之前，第二 IP 首标 304 被去掉。

[0027] 参照图 3 所述的隧道技术的作用在于，各移动节点接收包含在登记过程中分配给它的 MIP 地址的 IP 分组。因此，各移动节点可在保留登记过程中分配给它的 IP 地址的同时漫游 - 甚至在域之间漫游。

[0028] 隧道技术的许多层可用于图 1 所示的网络环境 100。例如，各 WiMAX 区域接入网 106 和 124 可采用隧道技术，使得设置在域外部的单元仅需要把 IP 分组送往适当域，以便让分组到达预期移动节点。

[0029] 再来看图 2，可以看到，协议栈 200 还包括提供基于 IP 的语音功能性的 VoIP 层 204，基于 IP 的语音功能性可符合工业公认 VoIP 标准，诸如 IETF RFC 1889 定义的实时传输协议 (RTP) 和 / 或 IETF RFC 2326 定义的实时流式传播协议 (RTSP)。简言之，VoIP 层 204 接收 VoIP 分组，并把那些分组变换为用于公共交换电话网 (PSTN) 118 和 120 的时域复用数字语音数据，反过来也是一样。如下面所述，在移动节点的用户与 PSTN 的用户之间的论述的上下文中，VoIP 层 204 把时域复用数字数据转换为 VoIP 分组。VoIP 分组包含分配给具体移动节点的 MIP 地址。VoIP 分组被传递给 MIP 层 202，MIP 层 202 把 VoIP 分组附接到包含具体移动节点的转交地址的 IP 首标。

[0030] 协议栈 200 还包括会话发起协议层 206，它提供可能符合工业公认标准、如 IETF RFC 3261 的 SIP 功能性。简言之，SIP 层 206 提供用于创建、修改和终止与一个或多个参与方的通信会话的应用层控制功能性。例如，SIP 层 206 包含发信号通知移动节点关于另一方希望与其通信的功能性。

[0031] 协议栈 200 还包括与 PSTN 接口的层 210。层 210 包括把时域复用语音数据转换为 IP 分组的媒体网关 (MGW)。它还包括 SS7 接口，SS7 接口接收 SS7 信号，对信号解码，以及把所提取信息传递给语音归属代理控制平面 208。

[0032] 语音归属代理控制平面 208 协调其它层的动作。它在主要网关与 VoIP 层 204 之间协调通信，并且还在 SS7 接口与 SIP 层 206 之间协调通信。例如，语音归属代理控制平面 208 可从 SS7 接口 210 接收表明需要到具体电话号码的连接的信号。作为响应，控制平面 208 调用 SIP 平面 206 向对应于该电话号码的移动节点发送 SIP 邀请消息。类似地，控制平面 208 在具体时隙中接收语音数据，并且把数据转发给 VoIP 层，用于转换为 VoIP 分组以及用于传递给具体移动节点（这样，维持语音路径）。

[0033] 前面的论述简要提供组成语音归属代理 114 或 116 的协议层 202-210。与关于呼叫发起和呼叫执行的语音归属代理 114 或 116 的操作相关的论述如下。这个论述总体（与基于逐层相对）描述语音归属代理的操作，并提供语音归属代理的操作的高级综合视图。

[0034] 图 4 描绘在对移动节点发起电话呼叫的过程中语音归属代理 114 或 116 的操作。该过程可由 PSTN 的用户或者由语音归属代理 114 或 116 服务的移动节点的用户发起。如果该过程由 PSTN 的用户发起，则语音归属代理 114 或 116 接收表明希望与具体电话号码标识的移动节点进行电话呼叫的 SS7 信号，如操作 400 中所示。电话号码从 SS7 信号中提取（操作 400）。SS7 信号被转换为邀请消息（操作 400），它是表明希望通信会话的 SIP 消息。因此，在操作 400 完成时，语音归属代理 114 或 116 已经构造送往具体电话号码的邀请消息。

[0035] 另一方面，该过程可能由语音归属代理 114 或 116 服务的移动节点发起。当移动节点发起电话呼叫时，移动节点把送往所选电话号码的 SIP 邀请消息发送给语音归属代理 114 或 116。这个 SIP 邀请消息由语音归属代理接收，如操作 402 所示。

[0036] 无论 SIP 邀请消息被接收（如移动节点发起电话呼叫时的情况）还是被语音归属代理创建（如 PSTN 的用户发起电话呼叫时的情况），操作流程随后进入操作 404。在操作

404 中，语音归属代理查询数据库以标识与嵌入邀请消息的电话号码关联的 MIP 地址和转交地址。

[0037] 如果在操作 404 中标识的电话号码对应于由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 采用参照图 3 所述的隧道技术向移动节点发送 SIP 邀请消息（操作 406）。

[0038] 如果在操作 404 中标识的电话号码对应于不是由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 向服务于与被邀请移动节点对应的域的语音归属代理 114 或 116 发送 SIP 邀请消息（操作 408）。

[0039] 如果电话号码表明，电话号码表示由 PSTN 服务的电话装置，则邀请消息被转换为 SS7 信号，以便在 PSTN 上发起电话呼叫（操作 410）。

[0040] 在已经发送邀请消息（通过 SIP 邀请消息或者通过 SS7 信号）之后，语音归属代理 114 或 116 等待对邀请消息的响应，如操作 412 所示。如果被邀请电话装置的用户希望应答电话呼叫，则表明这种希望的响应由语音归属代理 114 或 116 接收（操作 412）。如果响应从移动节点始发，则响应可通过 SIP 确认 (ack) 消息的形式到达语音归属代理 114 或 116。另一方面，如果响应从 PSTN 电话装置始发，则响应可通过可被转换为 SIP ack 消息的 SS7 信号的形式到达语音归属代理 114 或 116。

[0041] 在响应被接收之后，它被转发给发起方（操作 414）。如果电话呼叫的发起方为移动节点，则转发操作包括使用 MIP 层 202 把响应发送给移动节点，以便采用参照图 3 所述的隧道技术。另一方面，如果电话呼叫的发起方是 PSTN 上的电话装置，则响应被转换为 SS7 信号，并通过 SS7 接口 210 导向到 PSTN。

[0042] 最后，假定在操作 412 接收的响应表明被邀请移动节点的用户希望参与通信会话（即希望应答呼叫），则建立邀请与被邀请装置之间的语音路径（操作 416）。建立语音路径可包括把来自 PSTN 本地局 118 或 120 的时域复用语音数据中的具体时隙与具体 MIP 地址关联（反之亦然）。另外，还可包括把移动节点的 MIP 地址与服务于具体移动节点的语音归属代理 114 或 116 的转交地址或地址关联。

[0043] 在已经建立 VoIP 会话之后（如图 4 所示），各方可相互通话。在各方通话时，语音归属代理 114 或 116 接收 VoIP 分组或者来自 PSTN 的时域复用语音数据，如图 5 的操作 500 所示。如果语音归属代理接收来自 PSTN 的时域复用语音数据，则这种数据被转换为 VoIP 分组，如上所述。

[0044] 随后，如操作 502 所示，VoIP 分组或语音数据沿图 4 的操作 416 中建立的语音通路发送。在向移动节点发送 VoIP 分组的情况中，这可表示把所接收 VoIP 分组发送给服务于移动节点的语音归属代理 114 或 116，或者可表示采用参照图 3 所述的隧道技术把所接收 VoIP 分组直接发送给移动节点。在向 PSTN 上的电话装置发送语音数据的情况中，操作 502 包括把 VoIP 数据转换为时域复用数字语音数据，并把这种语音数据插入到适当的时隙，使得 PSTN 交换设备把数据路由到适当的位置。

[0045] 前面的论述涉及电话呼叫的发起和执行期间的语音归属代理的操作。以下论述从系统级的角度陈述在图 1 所示的网络环境 100 的上下文中的电话呼叫的发起和执行。

[0046] 在 PSTN 电话装置（呼叫的发起方）与移动节点（呼叫的应答方）之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理 114 或 116 接收表明希望与对应于给定

电话号码的移动装置进行通信会话的 SS7 信号。语音归属代理提取电话号码，并创建送往被邀请移动节点的 MIP 地址的 SIP 邀请消息。（如果被邀请移动节点不可用，则呼叫可被重新路由到语音邮件服务。）

[0047] 通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。同时，语音归属代理 114 或 116 向邀请电话装置发送产生回铃音的 SS7 信号。

[0048] 如果移动节点的用户接受该呼叫，则 SIP 确认消息被发送给语音归属代理 114 或 116。语音归属代理 114 或 116 把 SIP 确认消息转换为 SS7 信号，并建立语音路径。这时，PSTN 电话装置和移动节点的用户开始通话。

[0049] 在两个移动节点（在不同的域中）之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理接收来自邀请移动节点的 SIP 邀请消息。SIP 邀请消息被送往与预期移动节点对应的电话号码。作为响应，语音归属代理把 SIP 邀请消息转发给服务于被邀请移动节点所在的域的语音归属代理。后一个语音归属代理向被邀请移动节点的 MIP 地址发送响应。

[0050] 通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。此外，邀请移动节点的 IP 地址包含在 SIP 邀请消息中。

[0051] 如果被邀请移动节点的用户接受该呼叫，则 SIP 确认消息被发送给服务于被邀请移动节点所在的域的语音归属代理 114 或 116。作为响应，语音归属代理 114 或 116 把 SIP 确认消息转发给服务于邀请移动节点所在的域的语音归属代理 114 或 116。后一个语音归属代理 114 或 116 把 SIP 确认消息转发到邀请移动节点的 MIP 地址。SIP 确认消息包含被邀请节点的 IP 地址。

[0052] 语音通信这时可通过两种方式之一进行。首先，移动节点可相互通信而无需语音归属代理的介入。这是可行的，因为通过 SIP 邀请和确认消息，各移动节点知道另一个的 IP 地址。但是，如果移动节点中的任一个漫游到不同的域，则两个移动节点之间的连接将丢失。

[0053] 其次，语音路径可在两个语音归属代理之间延伸。这个方案允许移动节点中任一个从一个域漫游到另一个域。

[0054] 图 6 描绘其中可实施语音归属代理 114 或 116 的硬件环境。该环境包括四个刀片 600、602、604 和 606。各刀片包含它自己的计算环境，其中包括处理器、存储器以及提供对网络接口或存储装置的访问的输入 / 输出模块（例如，控制集线器和 I/O 总线）。各刀片 600-606 可经由局域网、例如经由以太网集线器进行通信。刀片 600-606 可被实施为可安装在机架中的薄板。

[0055] 各刀片可专用于执行先前所述的控制平面功能或数据平面功能的各种小方面。例如，刀片 602 可执行与 MIP 层 202 相关的功能。这个刀片 602 还执行在接收到 VoIP 分组并且需要被路由到另一个语音归属代理或者移动节点时所需的路由功能性，如上所述。刀片 602 包括允许在其中运行的软件 / 固件与 WiMAX 核心网 112 进行通信的网络接口。

[0056] 刀片 604 可执行以上参照图 2 中所述的 VoIP 层 204 所描述的 VoIP 功能性。刀片 604 包括允许在其中运行的软件 / 固件与来自 PSTN 的时域复用数字语音数据交互的时域复用接口。

[0057] 刀片 606 可对 SS7 信号解码，并把所提取内容发送给驻留在刀片 600 上的 SS7 应用层功能性。刀片 606 包括允许在其中运行的软件 / 固件与来自 PSTN 本地局的 SS7 分组交互的 SS7 接口。

[0058] 刀片 600 可执行如上所述的语音归属代理控制平面功能性。为此，该刀片包括存储装置（以便维护为执行这种功能性所必需的数据库）。刀片 600 还执行 SS7 子系统的 SIP 功能性和应用层功能性。在一个实施例中，刀片 600 执行计费例程。计费例程可根据逐个用户或逐个帐户来跟踪给定用户连接到网络的时间量、用户消耗的业务量、用户消耗的服务的类型（本地呼叫、长途呼叫等）或者用户消耗的带宽。所跟踪信息可存储在数据库中，以及可从其中产生定期帐单。

[0059] 本发明的实施例可通过硬件、固件和软件其中之一或者它们的组合来实现。本发明的实施例还可实现为存储于机器可读媒体中的指令，所述指令可由至少一个处理器读取和运行，以便执行本文所述的操作。机器可读媒体可包括用于存储或传送机器（例如计算机）可读形式的信息的任何机构。例如，机器可读媒体可包括：只读存储器 (ROM)，随机存取存储器 (RAM)，磁盘存储媒体，光存储媒体，闪速存储装置，电、光、声或其它形式的传播信号（例如载波、红外信号、数字信号等），等等。

[0060] 摘要是根据要求摘要以允许读者确定技术公开的性质和要点的 37C.F.R. 第 1.72(b) 节来提供的。应当理解，它的提供并不是用于限制或解释权利要求的范围或含意。

[0061] 在前面的详细描述中，各种功能有时集中到单一实施例中，用于简化本公开。这种公开的方法不应解释为反映了要求其权益的主题的实施例要求超过各权利要求中明确陈述的特征的意图。相反，如以下权利要求所反映的那样，本发明主题在于少于单个公开实施例的全部特征。因此，以下权利要求由此结合到详细描述中，其中各权利要求本身代表单独的优选实施例。

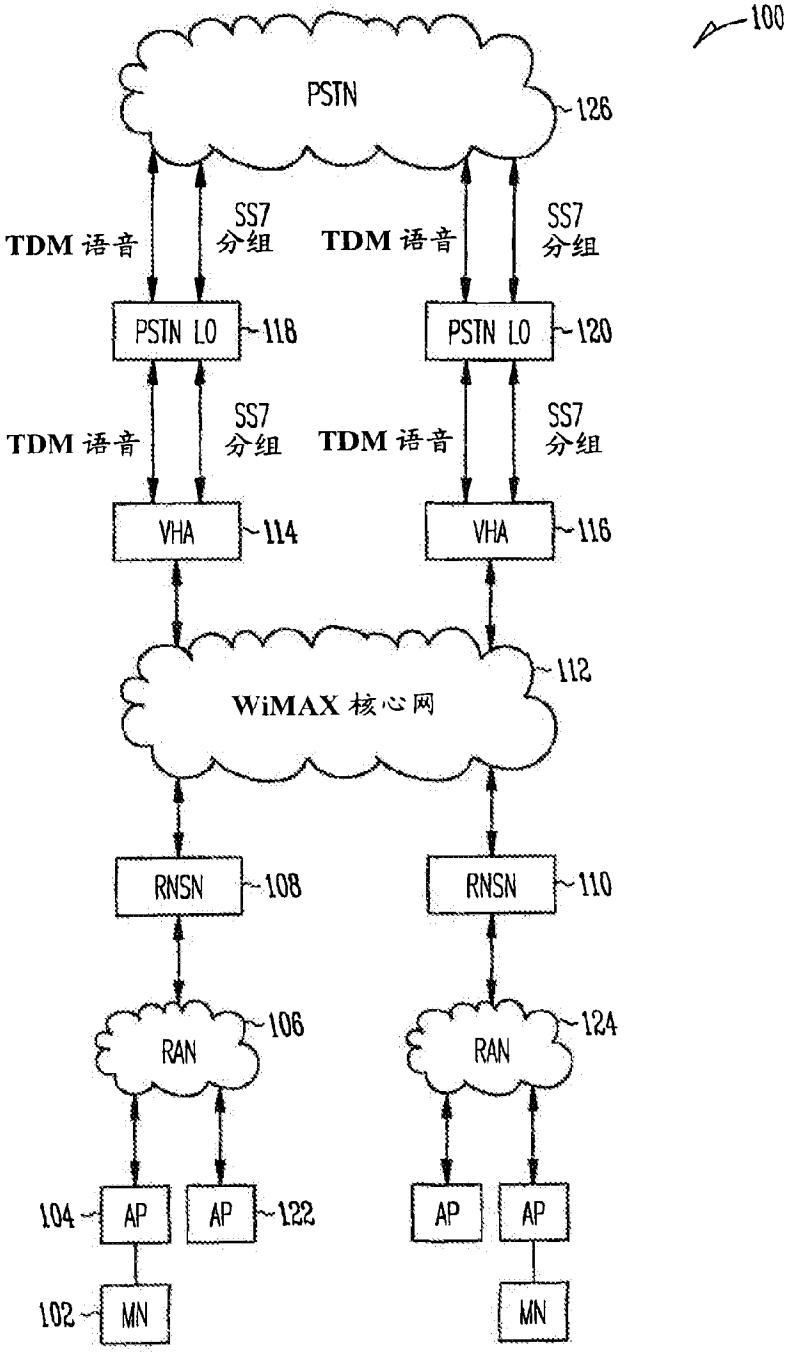


图 1

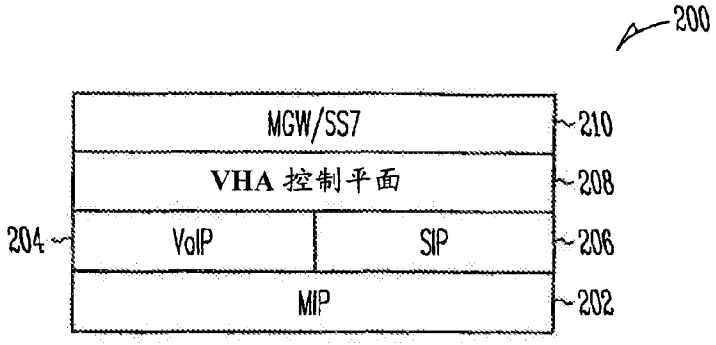


图 2

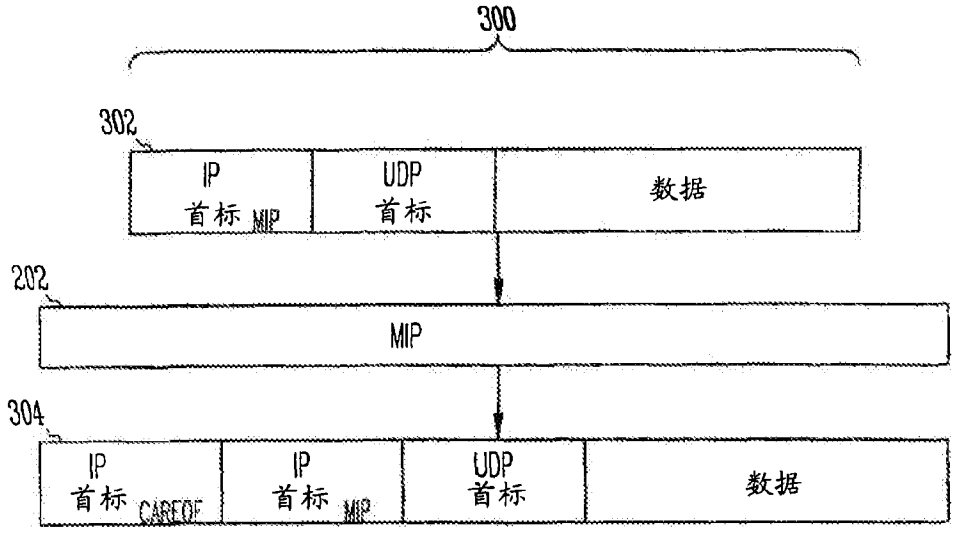


图 3

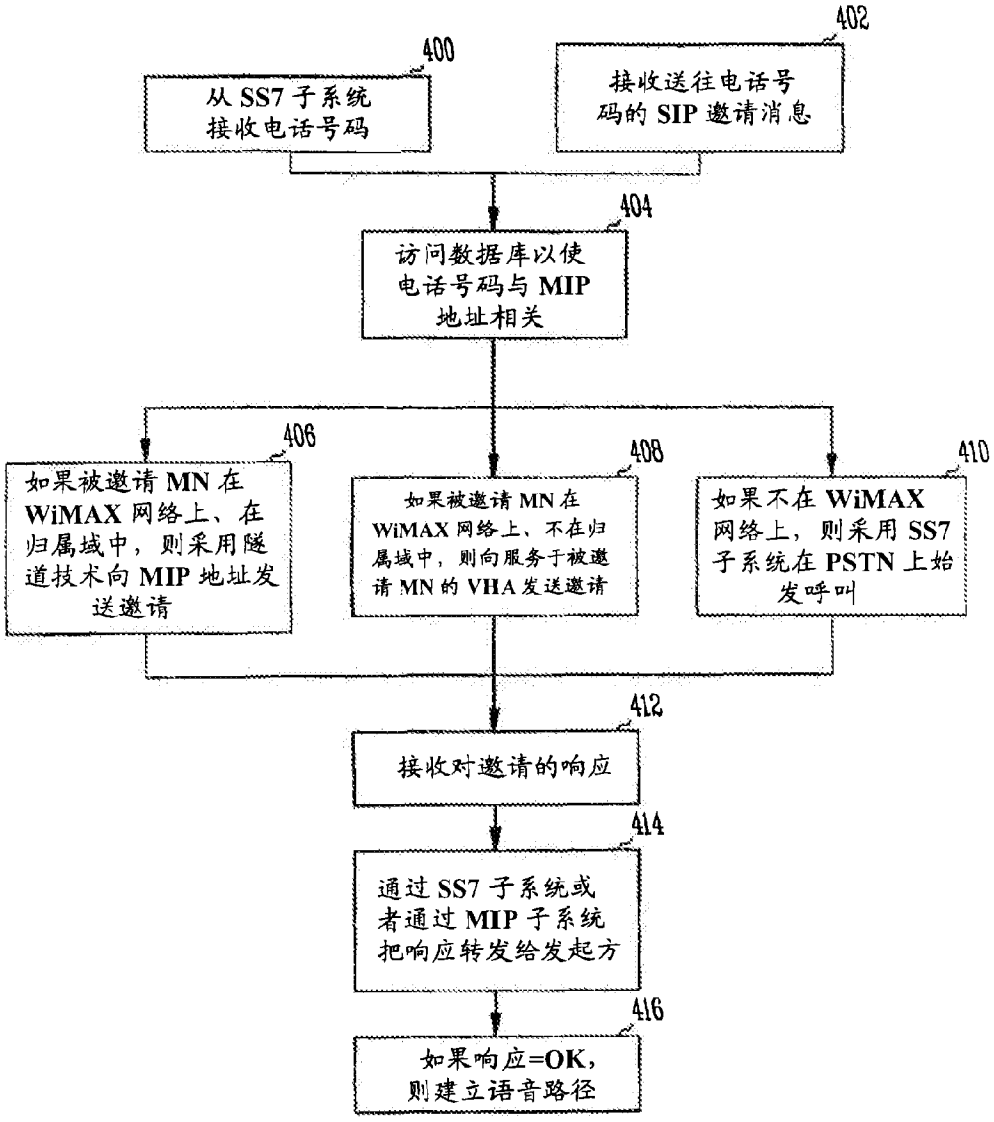


图 4

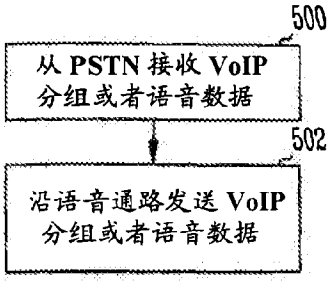


图 5

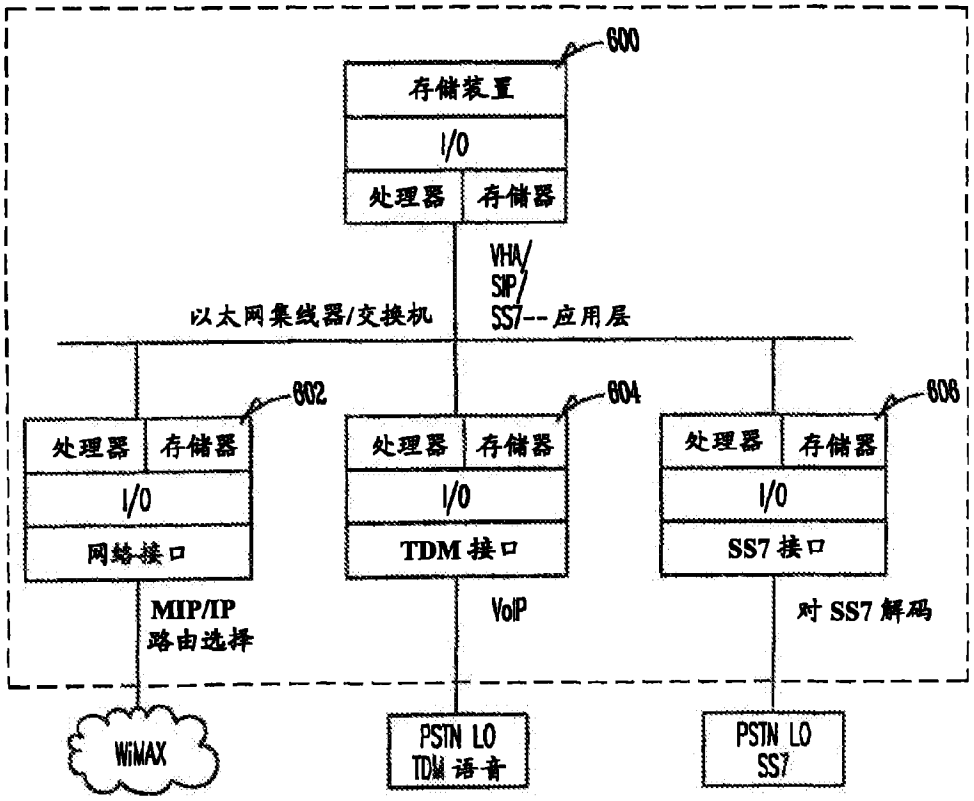


图 6

Espacenet

Bibliographic data: CN102833232 (A) — 2012-12-19

Distributed voice network

Inventor(s): LEBIZAY GERALD + (LEBIZAY GERALD)

Applicant(s): INTEL CORP + (INTEL CORPORATION)

Classification: - international:***H04L29/06; H04L29/12***
- cooperative: **G06Q20/102; H04L29/06027; H04L65/103; H04L65/104; H04L65/1043; H04L65/607**

Application number: CN20121277853 20051229

Priority number (s): US20040027915 20041230

Also published as: WO2006072099 (A1) US2012250624 (A1) US8605714 (B2) US2010008345 (A1) US8204044 (B2) more

Abstract of CN102833232 (A)

A method and apparatuses (114, 116) that receives an IP packet and encapsulates the packet with an IP header. Further, time-domain multiplexed voice data is received and converted into VoIP packets. Still further, Signaling System (7) (SS7) compliant signals are decoded. The decoded (SS7) signals are received and encapsulated prior to transmission to a telephony device (102).

(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102833232 A
(43)申请公布日 2012.12.19

(21)申请号 201210277853.0

(22)申请日 2005.12.29

(30)优先权数据
11/027,915 2004.12.30 US

(62)分案原申请数据
200580045760.3 2005.12.29

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 G.利比扎伊

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 柯广华 李家麟

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)

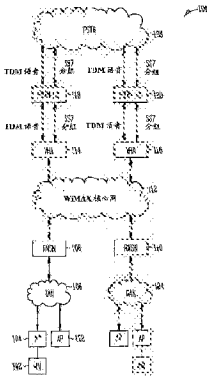
权利要求书 4 页 说明书 7 页 附图 4 页

(54)发明名称

分布式语音网络

(57)摘要

一种接收IP分组并封装分组与IP首标的方法及设备(114,116)。此外,时域复用语音数据被接收并转换为VoIP分组。此外,对符合信令系统(7)(SS7)的信号解码。已解码(SS7)信号被接收,并在传送给电话装置(102)之前被封装。



CN 102833232 A

1. 一种由一个或多个网络单元执行的用于建立第一通信装置和第二通信装置之间的英特网 - 协议(IP)通信会话的方法,所述方法包括 :

接收来自所述第一通信装置的邀请所述第二通信装置参与 IP 通信会话的请求,所述第二通信装置由网络标识符在所述请求中标识 ;

使所述网络标识符与所述第二通信装置的移动 IP (MIP)地址和第二 IP 地址相关,所述第二 IP 地址表明所述第二通信装置到无线接入网的附连点或所述第二通信装置正在其中进行操作的无线接入网的域的转交地址 ;及

发送邀请到所述第二通信装置的所述 MIP 地址,所述邀请包括所述第一通信装置的 MIP 地址和第一 IP 地址,

其中,所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP 地址来建立用于与所述第二通信装置的 IP 通信会话的 IP 连接。

2. 权利要求 1 的方法,还包括 :

接收来自所述第二通信装置的对于所述邀请的响应 ;

修改所述响应以包括包括所述第二通信装置的所述 MIP 地址的第一 IP 首标和包括所述第二 IP 地址的第二 IP 首标 ;及

转发所修改的响应到所述第一通信装置 ;

其中,在收到所修改的响应后,所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP 地址来建立用于与所述第二通信装置的所述 IP 通信会话的所述 IP 连接。

3. 权利要求 2 的方法,其中,所述第一 IP 地址表明所述第一通信装置到所述无线接入网的附连点或所述第一通信装置正在其中进行操作的所述无线接入网的域的转交地址。

4. 权利要求 3 的方法,其中,发送到所述第二通信装置的所述 MIP 地址的所述邀请当所述第二通信装置正在不同的域中进行操作时包括所述第一通信装置的所述转交地址或包括所述附连点。

5. 权利要求 2 的方法,其中,所述英特网 - 协议通信会话是基于 IP 的视频和语音通信会话,

其中,在收到所修改的响应后,所述第一通信装置配置成建立与所述第二通信装置的对等 IP 连接,所述对等 IP 连接包括除去所述网络单元的通信路径 ;及

其中,所述第一和第二通信装置中的至少一个是无线或移动通信装置。

6. 一种配置成建立第一通信装置和第二通信装置之间的英特网 - 协议(IP)通信会话的网络单元,所述网络单元配置成 :

接收来自所述第一通信装置的邀请所述第二通信装置参与 IP 通信会话的请求,所述第二通信装置由网络标识符在所述请求中标识 ;

使所述网络标识符与所述第二通信装置的移动 IP (MIP)地址和第二 IP 地址相关,所述第二 IP 地址表明所述第二通信装置到无线接收网的附连点或所述第二通信装置正在其中进行操作的无线接入网的域的转交地址 ;及

发送邀请到所述第二通信装置的所述 MIP 地址,所述邀请包括所述第一通信装置的 MIP 地址和第一 IP 地址 ;

其中,所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP

地址来建立用于与所述第二通信装置的 IP 通信会话的 IP 连接。

7. 权利要求 6 的网络单元，还配置成：

接收来自所述第二通信装置的对所述邀请的响应；

修改所述响应以包括包括所述第二通信装置的所述 MIP 地址的第一 IP 首标和包括所述第二 IP 地址的第二 IP 首标；及

转发所修改的响应到所述第一通信装置；

其中，在收到所修改的响应后，所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP 地址来建立用于与所述第二通信装置的所述 IP 通信会话的所述 IP 连接。

8. 权利要求 7 的网络单元，其中，所述第一 IP 地址表明所述第一通信装置到所述无线接入网的附连点或所述第一通信装置正在其中进行操作的所述无线接入网的域的转交地址；及

其中，发送到所述第二通信装置的所述 MIP 地址的所述邀请当所述第二通信装置正在不同的域中进行操作时包括所述第一通信装置的所述转交地址或包括所述附连点。

9. 权利要求 7 的网络单元，其中，所述英特网 - 协议通信会话是基于 IP 的视频和语音通信会话，

其中，在收到所修改的响应后，所述第一通信装置配置成建立与所述第二通信装置的对等 IP 连接，所述对等 IP 连接包括除去所述网络单元的通信路径；及

其中，所述第一和第二通信装置中的至少一个是无线通信装置。

10. 权利要求 9 的网络单元，包括：

接口电路，接收来自所述第一通信装置的邀请所述第二通信装置参与所述 IP 通信会话的所述请求并发送所述邀请到所述第二通信装置的所述 MIP 地址；及

处理电路，使所述网络标识符与所述第二通信装置的所述 MIP 地址和所述第二 IP 地址相关。

11. 一种由一个或多个网络单元执行的用于建立第一通信装置和第二通信装置之间的基于 IP 的语音 (VoIP) 通信会话的方法，所述方法包括：

接收来自所述第一通信装置的邀请所述第二通信装置参与 VoIP 会话的请求，所述第二通信装置由网络标识符在所述请求中标识；

使所述网络标识符与所述第二通信装置的移动 IP (MIP) 地址和第二 IP 地址相关，所述第二 IP 地址表明所述第二通信装置到无线接入网的附连点或所述第二通信装置位于其中的所述无线接入网的域的转交地址；

发送邀请到所述第二通信装置的所述 MIP 地址，所述邀请包括所述第一通信装置的 MIP 地址和第一 IP 地址；

接收来自所述第二通信装置的对所述邀请的响应；

修改所述响应以包括包括所述第二通信装置的所述 MIP 地址的第一 IP 首标和包括所述第二 IP 地址的第二 IP 首标；及

转发所修改的响应到所述第一通信装置；

其中，在收到所修改的响应后，所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP 地址来建立用于与所述第二通信装置的 VoIP 会话的 IP 连接。

12. 权利要求 11 的方法，其中，所述第一 IP 地址表明所述第一通信装置到所述无线接入网的附连点。

13. 权利要求 11 的方法，其中，所述第一 IP 地址表明所述第一通信装置位于其中的所述无线接入网的域的转交地址；及

其中，发送到所述第二通信装置的所述 MIP 地址的所述邀请当所述第二通信装置位于不同的域中时包括所述第一通信装置的所述转交地址。

14. 权利要求 11 的方法，其中，所述邀请是按照会话发起协议（SIP）来配置的 SIP 邀请消息，

其中，对所述邀请的响应是 SIP 确认消息，及

其中，所述 SIP 邀请消息包括标识所述第一通信装置的主叫 ID 信息。

15. 权利要求 11 的方法，其中，所述邀请是参与所述 VoIP 会话的邀请，及

其中，所述响应表明所述第二通信装置接受参与所述 VoIP 会话的所述邀请。

16. 权利要求 11 的方法，其中，在收到所修改的响应后，所述第一通信装置配置成建立用于与所述第二通信装置的 VoIP 通信的对等 IP 连接，所述对等 IP 连接包括不包括所述一个或多个网络单元的通信路径。

17. 权利要求 11 的方法，其中，在收到所修改的响应后，所述第一通信装置配置成使用隧道技术来建立所述 IP 连接，用于与所述第二通信装置的 VoIP 通信。

18. 权利要求 11 的方法，其中，所述第一通信装置位于由第一网络单元服务的第一域中，及

其中，当所述网络标识符与所述无线接入网的第二域相关时，所述方法包括转发所述邀请到正在服务所述第二域的第二网络单元，所述第二通信装置位于所述第二域中。

19. 权利要求 11 的方法，其中，在收到所修改的响应后，所述第一通信装置配置成建立用于与所述第二通信装置的 VoIP 通信的 IP 连接，所述 IP 连接包括包括一个或多个网络单元的通信路径以允许所述第一和第二通信装置中的至少一个在域间漫游。

20. 权利要求 11 的方法，还包括：

确定所述第一通信装置是否已改变了到所述网络的附连点；及

重新定义所述第一 IP 地址以标识所改变的附连点。

21. 一种配置成建立第一通信装置和第二通信装置之间的基于 IP 的语音（VoIP）通信会话的网络单元，所述网络单元配置成：

接收来自所述第一通信装置的邀请所述第二通信装置参与 VoIP 会话的请求，所述第二通信装置由网络标识符在所述请求中标识；

使所述网络标识符与所述第二通信装置的移动 IP（MIP）地址和第二 IP 地址相关，所述第二 IP 地址表明所述第二通信装置到无线接入网的附连点或所述第二通信装置位于其中的所述无线接入网的域的转交地址；

发送邀请到所述第二通信装置的所述 MIP 地址，所述邀请包括所述第一通信装置的 MIP 地址和第一 IP 地址；

接收来自所述第二通信装置的对所述邀请的响应；

修改所述响应以包括包括所述第二通信装置的所述 MIP 地址的第一 IP 首标和包括所述第二 IP 地址的第二 IP 首标；及

转发所修改的响应到所述第一通信装置；

其中，在收到所修改的响应后，所述第一通信装置配置成使用所述第二通信装置的所述 MIP 地址和所述第二 IP 地址来建立用于与所述第二通信装置的 VoIP 会话的 IP 连接。

22. 权利要求 21 的网络单元，其中，所述第一 IP 地址表明所述第一通信装置到所述无线接入网的附连点。

23. 权利要求 21 的网络单元，其中，所述第一 IP 地址表明所述第一通信装置位于其中的所述无线接入网的域的转交地址；及

其中，发送到所述第二通信装置的所述 MIP 地址的所述邀请当所述第二通信装置位于不同的域中时包括所述第一通信装置的所述转交地址。

24. 权利要求 21 的网络单元，其中，所述邀请是按照会话发起协议(SIP)配置的 SIP 邀请消息，

其中，对所述邀请的所述响应是 SIP 确认消息，及

其中，所述 SIP 邀请消息包括标识所述第一通信装置的主叫 ID 信息。

25. 权利要求 21 的网络单元，其中，所述邀请是参与所述 VoIP 会话的邀请，及

其中，所述响应表明所述第二通信装置接受参与所述 VoIP 会话的所述邀请。

26. 权利要求 21 的网络单元，其中，在收到所修改的响应后，所述第一通信装置配置成建立用于与所述第二通信装置的 VoIP 通信的对等 IP 连接，所述对等 IP 连接包括不包括所述网络单元的通信路径。

27. 权利要求 21 的网络单元，其中，在收到所修改的响应后，所述第一通信装置配置成使用隧道技术来建立所述 IP 连接，用于与所述第二通信装置的 VoIP 通信。

28. 权利要求 21 的网络单元，其中，所述网络单元是第一网络单元，

其中，所述第一通信装置位于由所述第一网络单元服务的第一域中，及

其中，当所述网络标识符与所述无线接入网的第二域相关时，所述第一网络单元配置成转发所述邀请到正在服务所述第二域的第二网络单元，所述第二通信装置位于所述第二域中。

29. 权利要求 21 的网络单元，其中，在收到所修改的响应后，所述第一通信装置配置成建立用于与所述第二通信装置的 VoIP 通信的 IP 连接，所述 IP 连接包括包括一个或多个网络单元的通信路径以允许所述第一和第二通信装置中的至少一个在域间漫游。

分布式语音网络

技术领域

[0001] 本发明的实施例涉及在移动无线宽带网络上实现的基于 IP 的语音技术。

背景技术

[0002] 基于 IP 的语音 (VoIP) 技术允许各方通过分组交换 IP 网络进行口头通信。VoIP 技术在不断地普及，并且根据某些因素，可提供可与公共交换电话网 (PSTN) 相比的声音质量。

[0003] 不断普及的还有无线移动网络。无线移动网络允许装置链接到网络，无需物理导电线路在装置与网络之间传送数据。此外，这类网络通过允许装置以对于无线移动网络域外部的网络单元或节点透明的方式改变接入点来允许移动性。

[0004] 尽管 VoIP 技术和无线移动网络的普及性不断增长，但是对于基于因特网的当前 VoIP 服务没有移动客户装置。阻碍这类移动装置的进步的一个因素涉及找出用以在表现为保持单一 IP 地址的同时可允许移动装置在大地理区域漫游（因而可能在域之间来回移动）的简单方案。用户数据报协议 (UDP) 通过使用包含两个连接端点的 IP 地址和端口号的四元组对连接进行索引。改变这四个号码中的任一个使连接被中断和丢失。因此，重要的是，该装置表现为在地理上漫游的同时保持相同的 IP 地址。解决这个问题的困难随着允许装置在其中漫游的地理区域增大而增加。

[0005] 通过上述明显看到，需要一种方案，通过该方案，可允许无线 IP 电话装置在地理上的大区域、如都市区域漫游。希望这种方案比较简单地实现为在现有无线网络上的重叠。还希望这种方案易于与 PSTN 互连。

附图说明

[0006] 图 1 说明在其中采用语音归属代理的一个实施例的网络环境。

[0007] 图 2 说明根据本发明的一个实施例构成语音归属代理的协议栈。

[0008] 图 3 说明图 2 所示的协议栈的移动 IP 层所采用的隧道技术方案。

[0009] 图 4 说明根据本发明的一个实施例发起 VoIP 电话呼叫的方法。

[0010] 图 5 说明根据本发明的一个实施例执行 VoIP 电话呼叫的方法。

[0011] 图 6 说明根据本发明的一个实施例在其中可实施语音归属代理的硬件环境。

具体实施方式

[0012] 图 1 说明网络环境 100，在其中，可允许一个或多个移动节点 102 在地理上的大区域、例如在都市区域进行漫游。移动节点 102 经由数字传输（通常以 2 至 6GHz 许可频带，其中典型信道带宽的范围是从 1.5 至 20MHz）与接入点 104 通信。诸如由参考标号 104 标识的接入点（在本文中又称作基站）接收来自移动节点的传输，并把传输传递给关联区域接入网 106 中的网络单元。根据一个实施例，区域接入网 106 是一种有线网络（即，物理线路互连构成区域接入网的各个单元），它是一般的基于分组的接入网，例如以太网网络、IP/

MPLS 网络或 ATM 网络。接入点 104 与移动节点 102 之间的传输符合电气和电子工程师协会 (IEEE)802.16 标准信号，IEEE std.802.16-2001，2001 年发布，以及以后的版本（以下称作 IEEE 802.16 标准或 IEEE 802.16e 标准）。互连符合 IEEE 802.16e 标准的接入点（如 104）的区域接入网 106 称作 WiMAX 网络。

[0013] 在 WiMAX 区域接入网 106 的外围是无线电网络服务节点 108。

[0014] 无线电网络服务节点 108 提供其它 WiMAX 区域局域网、如参考标号 124 标识的 WiMAX 网络之间的路由选择和控制。各区域接入网 106 和 124 包括无线电网络服务节点 (108,110)，它把区域接入网 106 或 124 耦合到互连所有区域接入网 106 和 124 的 WiMAX 核心网 112。虽然 WiMAX 核心网 112 在图 1 中表示为互连两个 WiMAX 网络 106 和 124，但是 WiMAX 核心网 112 原则上可互连任何数量的区域接入网。

[0015] WiMAX 核心网 112 可以是普通 IP 网络，由常见的 IP 网络单元组成，例如允许高速数据传递的光纤网单元。因此，WiMAX 核心网 112 可直接与因特网（图 1 中未示出）互连。

[0016] 在 WiMAX 核心网 112 的外围是一个或多个语音归属代理 114 和 116。存在与各 WiMAX 区域接入网 106 和 124 关联的语音归属代理 114 或 116。下面详细论述语音归属代理 114 或 116 的结构或者由其制订的方法。简言之，语音归属代理是允许 WiMAX 核心网（例如核心网 112）与公共交换电话网 (PSTN)126 之间的 VoIP 综合的网络单元。另外，语音归属代理提供允许移动节点（例如移动节点 102）从一个 WiMAX 区域接入网（例如网络 106）漫游到另一个（例如 124）的功能性。

[0017] 虽然图 1 描绘了与各区域接入网 106 或 124 关联的单个语音归属代理 114 或 116，但是不止一个语音归属代理可与给定区域接入网关联。因此，虽然参考标号 114 和 116 在本文中用作表示单个语音归属代理，但是各参考标号 114 和 116 可理解为表示服务于它们相应的 WiMAX 区域接入网 106 和 124 的一组语音归属代理。

[0018] 各语音归属代理 114 和 116 把 WiMAX 核心网 112 与公共交换电话网 126 的本地局 118 或 120 接口。公共交换电话网 126 采用由国际电信联盟 (ITU) 电信标准化部门 (ITU-T) 定义的、称作 7 号信令系统 (SS7) 的带外信令方案。带外信令方案对于呼叫控制采用与用于承载呼叫本身的内容（例如语音数据）不同的物理路径。因此，如图 1 所示，语音归属代理用作两个分开的接口：用于作为时域复用数字语音数据来传送的语音数据的接口，以及用于作为 SS7 分组来传送的 SS7 控制信号的接口。

[0019] 诸如由参考标号 102 标识的移动节点之类的移动节点可被实施为电话手机（以与蜂窝电话相似的方式），可被实施为个人数字助理，或者可被实施为另一个移动计算装置。一旦上电，移动节点就向最接近的可用接入点进行初始传输。在传输时，接入点为移动节点分配管理信道，它向接入点标识移动节点。接入点和移动节点可在范围从一至五或十英里的距离上与另一个进行通信。给定这种区域的大小，其它移动节点可位于其中。因此，接入点可与数百个移动节点进行通信。管理信道的使用允许接入节点区分不同的接入点。

[0020] WiMAX 区域接入网中的各接入点具有标识它的 IP 地址。但是，这个 IP 地址仅在接入点所在的区域接入网（又称作域）中才起作用。因此，接入点可直接向它所在的区域接入网中的另一个接入点发送数据。为了把数据导向另一个域中的接入点，服务于接入点所在的特定域的无线电网络服务节点必须用作中间件。

[0021] 如上所述，在移动节点上电期间，为了建立管理信道并对用户鉴权，对基站进行初

始传输。此后，移动节点与服务于移动节点所在的域的语音归属代理进行初始通信。这个通信标记登记过程的开始，移动节点通过它来通知语音归属代理关于移动节点在哪一个域中。作为响应，语音归属代理对移动节点分配称作移动 IP(MIP) 地址的 IP 地址。语音归属代理还记录移动节点的转交地址。即使移动节点移动到它在其中与另一个接入点或者完全与另一个 WiMAX 区域接入网进行通信的地理区域，移动节点的 MIP 地址也不改变。另一方面，转交地址标识移动节点与之通信的域，因而在移动节点从一个区域接入网漫游到另一个区域接入网时会改变。

[0022] 语音归属代理可对移动节点分配不止一个 IP 地址。例如，移动节点可具有分配给它的用于传送语音数据的一个 IP 地址以及分配给它的用于传送信令数据的另一个 IP 地址。为了简单起见，本公开以下列假设继续进行：各移动节点在登记期间具有分配给它的单一 IP 地址。

[0023] 在登记时，语音归属代理更新它维护的数据库。数据库可包含与移动节点所支持的特征（呼叫等待、语音邮件等）有关的信息。数据库经过更新以便关联用来标识移动节点的电话号码、分配给移动节点的 MIP 地址以及移动节点所在的域（即，移动节点的转交地址）。

[0024] WiMAX 区域接入网 106 或 124 采用称作隧道技术的技术。利用这个技术，在给定 WiMAX 域 106 或 124 服务的地理区域内的移动节点的移动对于该域外部的网络单元或节点是透明的。因此，例如，WiMAX 域 106 外部的网络节点无法知道移动节点 102 是否正与接入点 104 或接入点 122 进行通信。域 106 外部的网络单元仅需要知道，移动节点 102 处于域 106 中以便与移动节点 102 通信。因此，每当移动节点（例如移动节点 102）从一个域移动到另一个域时，移动节点向它先前登记所用的语音归属代理重新登记。作为响应，语音归属代理更新其数据库，以便把新的转交地址（即，移动节点与之通信的域的网络地址）与该移动节点关联。

[0025] 前面的论述集中于语音归属代理 114 或 116 工作的网络环境。以下论述简要地提供组成语音归属代理 114 或 116 的协议层。

[0026] 图 2 说明语音归属代理 114 或 116 执行的协议栈 200。从图 2 中可以看到，协议栈 200 包括移动 IP(MIP) 层 202，它提供符合诸如“IP 移动性支持”(C. Perkins, ed., IETF RFC 2002, 1996 年 10 月）中所述的标准之类的工业公认 MIP 标准的功能性。MIP 层 202 提供的功能性可用于栈 200 的上层 204-210。

[0027] MIP 层提供以上所述的隧道技术功能性。图 3 说明接收具有 IP 首标 302 的分组 300 的 MIP 层 202。IP 首标 302 在其 32 位目标 IP 地址字段中包含分配给具体移动节点的 MIP 地址，因而称作 IP 首标 $_{MIP}$。对接收这种分组 300 进行响应，MIP 层 202 把分组 300 附接到第二 IP 首标 304。第二 IP 首标采用 MIP 地址标识的具体移动节点的转交地址，因而称作 IP 首标 $_{CareOf}$。因此，WiMAX 核心网 112 观察第二 IP 首标 304，并按照第二 IP 首标 304 来路由分组 300，表示分组 300 被路由到适当的域 106 或 124。在由移动节点接收之前，第二 IP 首标 304 被去掉。

[0028] 参照图 3 所述的隧道技术的作用在于，各移动节点接收包含在登记过程中分配给它的 MIP 地址的 IP 分组。因此，各移动节点可在保留登记过程中分配给它的 IP 地址的同时漫游 - 甚至在域之间漫游。

[0029] 隧道技术的许多层可用于图 1 所示的网络环境 100。例如，各 WiMAX 区域接入网 106 和 124 可采用隧道技术，使得设置在域外部的单元仅需要把 IP 分组送往适当域，以便让分组到达预期移动节点。

[0030] 再来看图 2，可以看到，协议栈 200 还包括提供基于 IP 的语音功能性的 VoIP 层 204，基于 IP 的语音功能性可符合工业公认 VoIP 标准，诸如 IETF RFC 1889 定义的实时传输协议 (RTP) 和 / 或 IETF RFC 2326 定义的实时流式传播协议 (RTSP)。简言之，VoIP 层 204 接收 VoIP 分组，并把那些分组变换为用于公共交换电话网 (PSTN) 118 和 120 的时域复用数字语音数据，反过来也是一样。如下面所述，在移动节点的用户与 PSTN 的用户之间的论述的上下文中，VoIP 层 204 把时域复用数字数据转换为 VoIP 分组。VoIP 分组包含分配给具体移动节点的 MIP 地址。VoIP 分组被传递给 MIP 层 202，MIP 层 202 把 VoIP 分组附接到包含具体移动节点的转交地址的 IP 首标。

[0031] 协议栈 200 还包括会话发起协议层 206，它提供可能符合工业公认标准、如 IETF RFC 3261 的 SIP 功能性。简言之，SIP 层 206 提供用于创建、修改和终止与一个或多个参与方的通信会话的应用层控制功能性。例如，SIP 层 206 包含发信号通知移动节点关于另一方希望与其通信的功能性。

[0032] 协议栈 200 还包括与 PSTN 接口的层 210。层 210 包括把时域复用语音数据转换为 IP 分组的媒体网关 (MGW)。它还包括 SS7 接口，SS7 接口接收 SS7 信号，对信号解码，以及把所提取信息传递给语音归属代理控制平面 208。

[0033] 语音归属代理控制平面 208 协调其它层的动作。它在主要网关与 VoIP 层 204 之间协调通信，并且还在 SS7 接口与 SIP 层 206 之间协调通信。例如，语音归属代理控制平面 208 可从 SS7 接口 210 接收表明需要到具体电话号码的连接的信号。作为响应，控制平面 208 调用 SIP 平面 206 向对应于该电话号码的移动节点发送 SIP 邀请消息。类似地，控制平面 208 在具体时隙中接收语音数据，并且把数据转发给 VoIP 层，用于转换为 VoIP 分组以及用于传递给具体移动节点（这样，维持语音路径）。

[0034] 前面的论述简要提供组成语音归属代理 114 或 116 的协议层 202-210。与关于呼叫发起和呼叫执行的语音归属代理 114 或 116 的操作相关的论述如下。这个论述总体（与基于逐层相对）描述语音归属代理的操作，并提供语音归属代理的操作的高级综合视图。

[0035] 图 4 描绘在对移动节点发起电话呼叫的过程中语音归属代理 114 或 116 的操作。该过程可由 PSTN 的用户或者由语音归属代理 114 或 116 服务的移动节点的用户发起。如果该过程由 PSTN 的用户发起，则语音归属代理 114 或 116 接收表明希望与具体电话号码标识的移动节点进行电话呼叫的 SS7 信号，如操作 400 中所示。电话号码从 SS7 信号中提取（操作 400）。SS7 信号被转换为邀请消息（操作 400），它是表明希望通信会话的 SIP 消息。因此，在操作 400 完成时，语音归属代理 114 或 116 已经构造送往具体电话号码的邀请消息。

[0036] 另一方面，该过程可能由语音归属代理 114 或 116 服务的移动节点发起。当移动节点发起电话呼叫时，移动节点把送往所选电话号码的 SIP 邀请消息发送给语音归属代理 114 或 116。这个 SIP 邀请消息由语音归属代理接收，如操作 402 所示。

[0037] 无论 SIP 邀请消息被接收（如移动节点发起电话呼叫时的情况）还是被语音归属代理创建（如 PSTN 的用户发起电话呼叫时的情况），操作流程随后进入操作 404。在操作

404 中，语音归属代理查询数据库以标识与嵌入邀请消息的电话号码关联的 MIP 地址和转交地址。

[0038] 如果在操作 404 中标识的电话号码对应于由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 采用参照图 3 所述的隧道技术向移动节点发送 SIP 邀请消息（操作 406）。

[0039] 如果在操作 404 中标识的电话号码对应于不是由语音归属代理 114 或 116 服务的域，则语音归属代理 114 或 116 向服务于与被邀请移动节点对应的域的语音归属代理 114 或 116 发送 SIP 邀请消息（操作 408）。

[0040] 如果电话号码表明，电话号码表示由 PSTN 服务的电话装置，则邀请消息被转换为 SS7 信号，以便在 PSTN 上发起电话呼叫（操作 410）。

[0041] 在已经发送邀请消息（通过 SIP 邀请消息或者通过 SS7 信号）之后，语音归属代理 114 或 116 等待对邀请消息的响应，如操作 412 所示。如果被邀请电话装置的用户希望应答电话呼叫，则表明这种希望的响应由语音归属代理 114 或 116 接收（操作 412）。如果响应从移动节点始发，则响应可通过 SIP 确认 (ack) 消息的形式到达语音归属代理 114 或 116。另一方面，如果响应从 PSTN 电话装置始发，则响应可通过可被转换为 SIP ack 消息的 SS7 信号的形式到达语音归属代理 114 或 116。

[0042] 在响应被接收之后，它被转发给发起方（操作 414）。如果电话呼叫的发起方为移动节点，则转发操作包括使用 MIP 层 202 把响应发送给移动节点，以便采用参照图 3 所述的隧道技术。另一方面，如果电话呼叫的发起方是 PSTN 上的电话装置，则响应被转换为 SS7 信号，并通过 SS7 接口 210 导向到 PSTN。

[0043] 最后，假定在操作 412 接收的响应表明被邀请移动节点的用户希望参与通信会话（即希望应答呼叫），则建立邀请与被邀请装置之间的语音路径（操作 416）。建立语音路径可包括把来自 PSTN 本地局 118 或 120 的时域复用语音数据中的具体时隙与具体 MIP 地址关联（反之亦然）。另外，还可包括把移动节点的 MIP 地址与服务于具体移动节点的语音归属代理 114 或 116 的转交地址或地址关联。

[0044] 在已经建立 VoIP 会话之后（如图 4 所示），各方可相互通话。在各方通话时，语音归属代理 114 或 116 接收 VoIP 分组或者来自 PSTN 的时域复用语音数据，如图 5 的操作 500 所示。如果语音归属代理接收来自 PSTN 的时域复用语音数据，则这种数据被转换为 VoIP 分组，如上所述。

[0045] 随后，如操作 502 所示，VoIP 分组或语音数据沿图 4 的操作 416 中建立的语音通路发送。在向移动节点发送 VoIP 分组的情况中，这可表示把所接收 VoIP 分组发送给服务于移动节点的语音归属代理 114 或 116，或者可表示采用参照图 3 所述的隧道技术把所接收 VoIP 分组直接发送给移动节点。在向 PSTN 上的电话装置发送语音数据的情况中，操作 502 包括把 VoIP 数据转换为时域复用数字语音数据，并把这种语音数据插入到适当的时隙，使得 PSTN 交换设备把数据路由到适当的位置。

[0046] 前面的论述涉及电话呼叫的发起和执行期间的语音归属代理的操作。以下论述从系统级的角度陈述在图 1 所示的网络环境 100 的上下文中的电话呼叫的发起和执行。

[0047] 在 PSTN 电话装置（呼叫的发起方）与移动节点（呼叫的应答方）之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理 114 或 116 接收表明希望与对应于给定

电话号码的移动装置进行通信会话的 SS7 信号。语音归属代理提取电话号码，并创建送往被邀请移动节点的 MIP 地址的 SIP 邀请消息。（如果被邀请移动节点不可用，则呼叫可被重新路由到语音邮件服务。）

[0048] 通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。同时，语音归属代理 114 或 116 向邀请电话装置发送产生回铃音的 SS7 信号。

[0049] 如果移动节点的用户接受该呼叫，则 SIP 确认消息被发送给语音归属代理 114 或 116。语音归属代理 114 或 116 把 SIP 确认消息转换为 SS7 信号，并建立语音路径。这时，PSTN 电话装置和移动节点的用户开始通话。

[0050] 在两个移动节点（在不同的域中）之间的电话呼叫的上下文中，流程如下进行。最初，语音归属代理接收来自邀请移动节点的 SIP 邀请消息。SIP 邀请消息被送往与预期移动节点对应的电话号码。作为响应，语音归属代理把 SIP 邀请消息转发给服务于被邀请移动节点所在的域的语音归属代理。后一个语音归属代理向被邀请移动节点的 MIP 地址发送响应。

[0051] 通过语音归属代理和各种 WiMAX 域的隧道技术能力，SIP 邀请消息到达被邀请移动节点，被送往移动节点的 MIP 地址。在 SIP 邀请消息内，嵌入了主叫 ID 信息。因此，标识邀请电话装置的消息可在被邀请移动节点上显示。此外，邀请移动节点的 IP 地址包含在 SIP 邀请消息中。

[0052] 如果被邀请移动节点的用户接受该呼叫，则 SIP 确认消息被发送给服务于被邀请移动节点所在的域的语音归属代理 114 或 116。作为响应，语音归属代理 114 或 116 把 SIP 确认消息转发给服务于邀请移动节点所在的域的语音归属代理 114 或 116。后一个语音归属代理 114 或 116 把 SIP 确认消息转发到邀请移动节点的 MIP 地址。SIP 确认消息包含被邀请节点的 IP 地址。

[0053] 语音通信这时可通过两种方式之一进行。首先，移动节点可相互通信而无需语音归属代理的介入。这是可行的，因为通过 SIP 邀请和确认消息，各移动节点知道另一个的 IP 地址。但是，如果移动节点中的任一个漫游到不同的域，则两个移动节点之间的连接将丢失。

[0054] 其次，语音路径可在两个语音归属代理之间延伸。这个方案允许移动节点中任一个从一个域漫游到另一个域。

[0055] 图 6 描绘其中可实施语音归属代理 114 或 116 的硬件环境。该环境包括四个刀片 600、602、604 和 606。各刀片包含它自己的计算环境，其中包括处理器、存储器以及提供对网络接口或存储装置的访问的输入 / 输出模块（例如，控制集线器和 I/O 总线）。各刀片 600-606 可经由局域网、例如经由以太网集线器进行通信。刀片 600-606 可被实施为可安装在机架中的薄板。

[0056] 各刀片可专用于执行先前所述的控制平面功能或数据平面功能的各种小方面。例如，刀片 602 可执行与 MIP 层 202 相关的功能。这个刀片 602 还执行在接收到 VoIP 分组并且需要被路由到另一个语音归属代理或者移动节点时所需的路由功能性，如上所述。刀片 602 包括允许在其中运行的软件 / 固件与 WiMAX 核心网 112 进行通信的网络接口。

[0057] 刀片 604 可执行以上参照图 2 中所述的 VoIP 层 204 所描述的 VoIP 功能性。刀片 604 包括允许在其中运行的软件 / 固件与来自 PSTN 的时域复用数字语音数据交互的时域复用接口。

[0058] 刀片 606 可对 SS7 信号解码，并把所提取内容发送给驻留在刀片 600 上的 SS7 应用层功能性。刀片 606 包括允许在其中运行的软件 / 固件与来自 PSTN 本地局的 SS7 分组交互的 SS7 接口。

[0059] 刀片 600 可执行如上所述的语音归属代理控制平面功能性。为此，该刀片包括存储装置（以便维护为执行这种功能性所必需的数据库）。刀片 600 还执行 SS7 子系统的 SIP 功能性和应用层功能性。在一个实施例中，刀片 600 执行计费例程。计费例程可根据逐个用户或逐个帐户来跟踪给定用户连接到网络的时间量、用户消耗的业务量、用户消耗的服务的类型（本地呼叫、长途呼叫等）或者用户消耗的带宽。所跟踪信息可存储在数据库中，以及可从其中产生定期帐单。

[0060] 本发明的实施例可通过硬件、固件和软件其中之一或者它们的组合来实现。本发明的实施例还可实现为存储于机器可读媒体中的指令，所述指令可由至少一个处理器读取和运行，以便执行本文所述的操作。机器可读媒体可包括用于存储或传送机器（例如计算机）可读形式的信息的任何机构。例如，机器可读媒体可包括：只读存储器 (ROM)，随机存取存储器 (RAM)，磁盘存储媒体，光存储媒体，闪速存储装置，电、光、声或其它形式的传播信号（例如载波、红外信号、数字信号等），等等。

[0061] 摘要是根据要求摘要以允许读者确定技术公开的性质和要点的 37C.F.R. 第 1.72(b) 节来提供的。应当理解，它的提供并不是用于限制或解释权利要求的范围或含意。

[0062] 在前面的详细描述中，各种功能有时集中到单一实施例中，用于简化本公开。这种公开的方法不应解释为反映了要求其权益的主题的实施例要求超过各权利要求中明确陈述的特征的意图。相反，如以下权利要求所反映的那样，本发明主题在于少于单个公开实施例的全部特征。因此，以下权利要求由此结合到详细描述中，其中各权利要求本身代表单独的优选实施例。

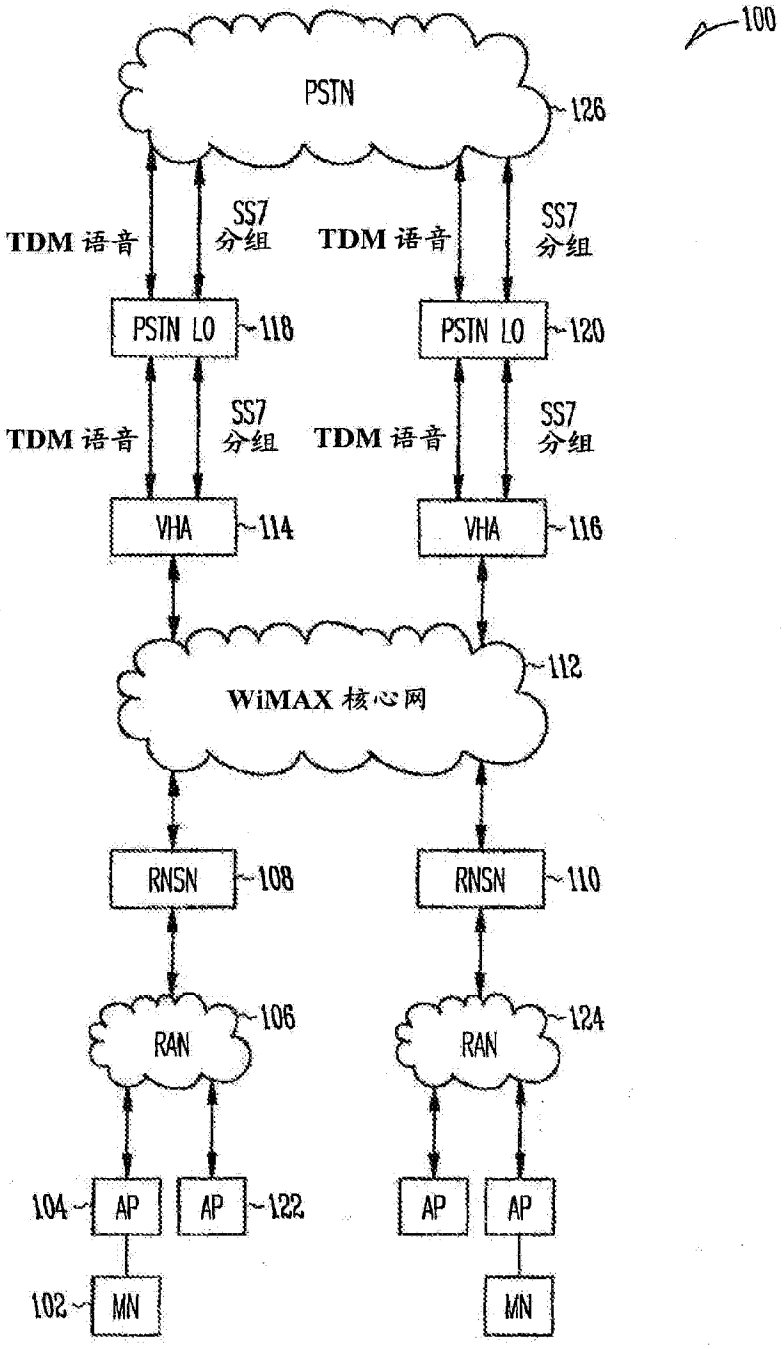


图 1

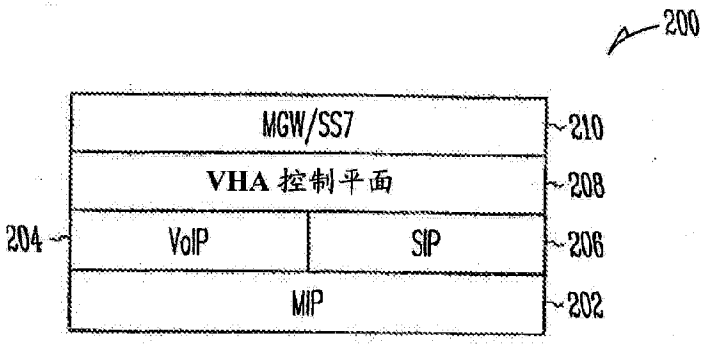


图 2

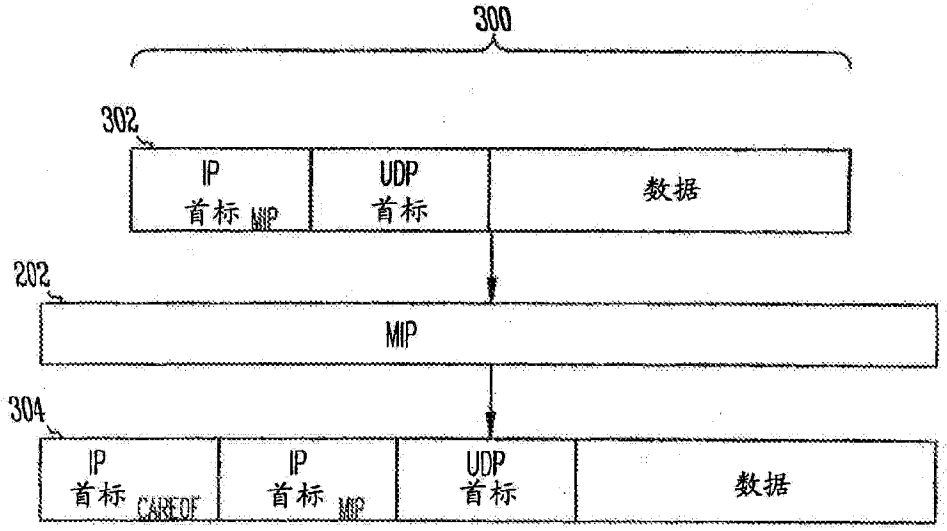


图 3

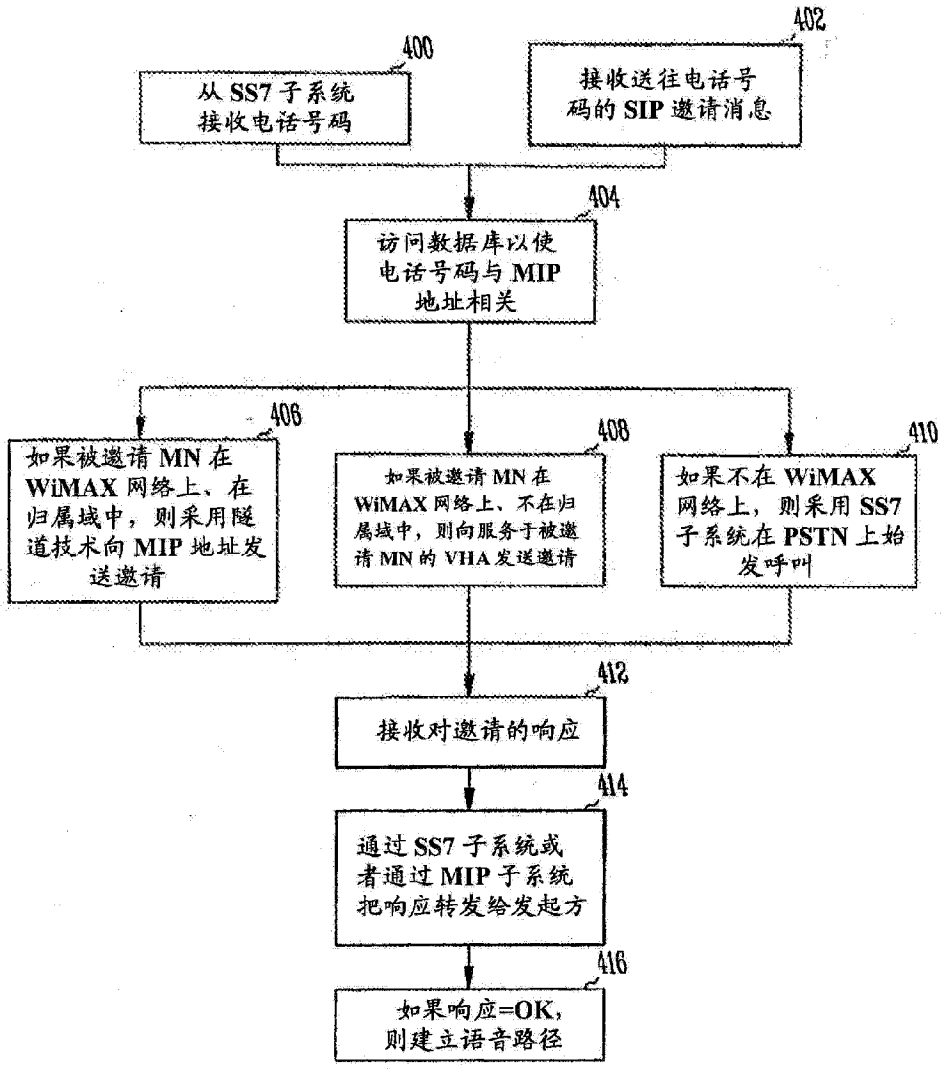


图 4

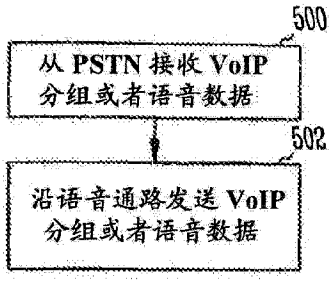


图 5

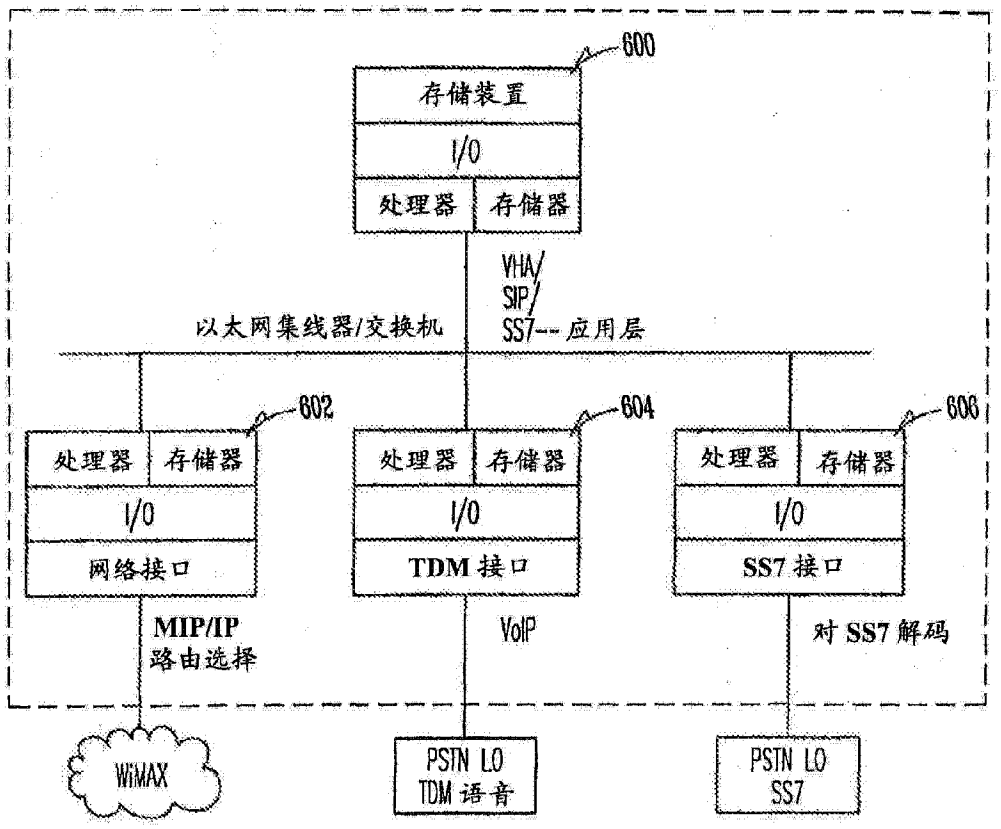


图 6

Espacenet

Bibliographic data: CN101005503 (B) — 2013-01-16

Method and data processing system for intercepting communication between a client and a service

Inventor(s): ANDRESS JIRI; VON KULESSA THOMAS; HEINE STEFAN ± (ANDRESS JIRI,HEINE STEFAN,VON KULESSA THOMAS, ; ANDRESS JIRI, ; VON KULESSA THOMAS, ; HEINE STEFAN)

Applicant(s): IBM ± (IBM)

Classification: - international: ***H04L29/06; H04L9/00***
- cooperative: **H04L63/08; H04L63/0884**

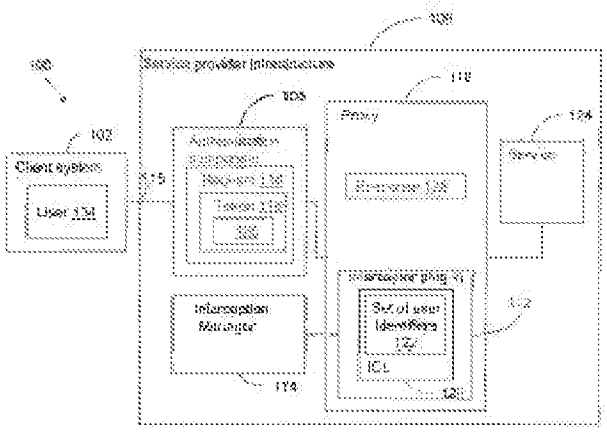
Application number: CN2007101788 20070116

Priority number (s): EP20060100369 20060116

Also published as: CN101005503 (A) US2007174469 (A1) US8024785 (B2)

Abstract of CN101005503 (A)

A method of monitoring communication between client-side and serveice, wherein the method includes a step of performancing user certification of the client-side user and a step of receiving requests from the client-side user via the service. The requests contains user special marks including unique user identifier. The user special marks can be allocated to the user requests thanks to user certification. If the unique user identifier equals to one user identifier of a group of unique user identifiers, the user requests are stored, wherein using the unique user identifier as key. The service sends answers relative to the requests, if the unique user identifier of the request is included in the group of unique user identifiers, storing copy thereof.



(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101005503 B
(45)授权公告日 2013.01.16

(21)申请号 200710001788.8

(22)申请日 2007.01.16

(30)优先权数据
06100369.5 2006.01.16 EP

(73)专利权人 国际商业机器公司
地址 美国纽约阿芒克

(72)发明人 托马斯·冯库莱萨 斯蒂芬·海因吉里·安德烈斯

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 黄小临 王志森

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/00(2006.01)

(56)对比文件
US 20030140151 A1,2003.07.24, 全文.
US 2002068582 A1,2002.06.06, 全文.

审查员 朱少华

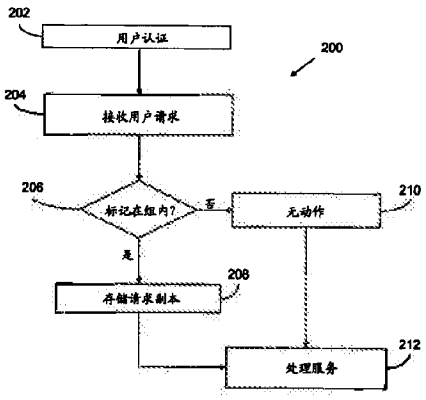
权利要求书 3 页 说明书 10 页 附图 5 页

(54)发明名称

用于侦听客户端和服务之间的通信的方法和数据处理系统

(57)摘要

提供了一种侦听客户端和服务之间的通信的方法，其中该方法包括执行所述客户端的用户的用户认证的步骤以及由所述服务从所述客户端的用户接收请求的步骤。所述请求包括用户特有标记，并且该用户特有标记包括唯一的用户标识符。该用户特有标记由于所述用户认证而能够被分配给所述用户的请求。如果所述唯一用户标识符等于一组唯一用户标识符的一个用户标识符，则存储所述请求的副本，其中，将所述唯一用户标识符用作密钥。所述服务发送与所述请求有关的响应，如果所述响应涉及的请求的唯一用户标识符被包括在这组唯一用户标识符中，则存储其副本。



CN 101005503 B

1. 一种侦听客户端 (102) 和服务 (124) 之间的通信的方法，所述方法包括：

执行所述客户端 (102) 的用户 (104) 的用户认证，将用户特有标记 (118) 添加到请求 (116) 中，所述用户特有标记 (118) 包括唯一的用户标识符 (126)，所述用户特有标记 (118) 由于所述用户认证而能够被分配给所述用户的所述请求 (116)；

在所述服务 (124) 处从所述客户端 (102) 的所述用户 (104) 接收请求 (116)，所述请求 (116) 包括用户特有标记 (118)；

如果所述唯一用户标识符 (126) 等于一组唯一用户标识符 (122) 的一个用户标识符，则使用所述唯一用户标识符 (126) 作为密钥来存储所述请求 (116) 的副本。

2. 如权利要求 1 所述的方法，所述方法还包括：

从所述服务 (124) 向所述客户端 (102) 发送响应 (128)，所述响应 (128) 与包括所述用户特有标记 (118) 的所述请求 (116) 有关，其中所述用户特有标记 (118) 包括所述唯一用户标识符 (126)；

如果所述唯一用户标识符 (126) 等于一组唯一用户标识符 (122) 的一个用户标识符，则使用所述唯一用户标识符 (126) 作为密钥来存储所述响应 (128) 的副本。

3. 如权利要求 2 所述的方法，其中，由认证组件 (108) 来执行所述用户认证，其中，所述认证组件 (108) 将所述用户特有标记 (118) 添加到所述请求 (116) 中，其中，侦听器插件 (112) 将所述唯一用户标识符 (126) 与所述一组唯一用户标识符 (122) 进行比较，其中，所述侦听器插件 (112) 被插入代理服务器 (110)，所述代理服务器 (110) 位于所述服务 (124) 和所述客户端 (102) 之间，其中，所述侦听器插件 (112) 包括侦听控制列表 (120)，所述侦听控制列表 (120) 包含所述一组唯一用户标识符 (122)，其中，所述侦听器插件 (112) 链接到侦听管理器 (114)，其中，所述请求 (116) 和所述响应 (128) 被存储在所述侦听管理器 (114) 上。

4. 如权利要求 3 所述的方法，其中，所述请求 (116) 和所述响应 (128) 被存储在消息队列 (402) 上，其中，所述消息队列 (402) 被包括在所述侦听器插件中，或者其中，所述请求 (116) 和所述响应 (128) 被存储在所述侦听器插件 (112、332) 上，由此，所述请求 (116) 和所述响应 (128) 通过加密的端到端通信 (338) 而被所述消息队列 (402) 或者从所述侦听器插件 (112、332) 传递到所述侦听管理器 (114、334)。

5. 如权利要求 3 所述的方法，其中，将所述侦听控制列表 (120) 永久存储在所述侦听管理器 (114、506) 上，并且其中，所述方法还包括：

在所述代理服务器 (502) 的启动之后，将所述侦听器插件 (504) 加载到所述代理服务器 (502) 中；

在所述代理服务器 (502) 的所述启动之后，将所述侦听控制列表从所述侦听管理器 (506) 加载到所述侦听器插件 (504) 中。

6. 如权利要求 3 所述的方法，所述方法包括：

利用更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表；

将所述更新的侦听控制列表加载到所述侦听器插件中。

7. 如权利要求 3 所述的方法，其中，从所述服务 (124) 或从所述代理服务器 (110) 的高速缓冲存储器接收所述响应 (128)。

8. 如权利要求 2 所述的方法，其中，以加密的方式将所述请求 (116) 和所述响应 (128)

与对应的唯一用户标识符 (126) 一起存储。

9. 如权利要求 3 所述的方法，其中，在所述侦听器插件 (332) 和所述侦听管理器 (334) 之间的所述链接 (338) 是加密的端到端通信。

10. 如权利要求 3 所述的方法，其中，所述认证组件 (314)、所述代理服务器 (316)、所述侦听器插件 (332)、所述侦听管理器 (334) 以及所述服务 (306) 是网络宿主环境的组件或服务提供商基础设施 (302) 的组件。

11. 如权利要求 3 所述的方法，其中，所述侦听管理器和所述侦听器插件采用加密方法来存储所述侦听控制列表。

12. 如权利要求 3 所述的方法，其中，所述侦听管理器 (334) 通过安全线路 (342) 链接到执法机构的网络，其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务的服务提供商的所选择的职员访问所述侦听控制列表。

13. 一种侦听客户端 (102) 和服务 (124) 之间的通信的数据处理系统，所述数据处理系统包括：

用于执行所述客户端 (102) 的用户 (104) 的用户认证并将用户特有标记 (118) 添加到请求 (116) 中的部件，所述用户特有标记 (118) 包括唯一的用户标识符 (126)，所述用户特有标记 (118) 由于所述用户认证而能够被分配给所述用户的所述请求 (116)；

用于在所述服务 (124) 处从所述客户端 (102) 的所述用户 (104) 接收请求 (116) 的部件；

用于如果所述唯一用户标识符 (126) 等于一组唯一用户标识符 (122) 的一个用户标识符，则使用所述唯一用户标识符 (126) 作为密钥来存储所述请求 (116) 的副本的部件。

14. 如权利要求 13 所述的数据处理系统，所述数据处理系统还包括：

用于从所述服务 (124) 向所述客户端 (102) 发送响应 (128) 的部件，所述响应 (128) 与包括所述用户特有标记 (118) 的所述请求 (116) 有关，所述用户特有标记 (118) 包括所述唯一用户标识符 (126)；

用于如果所述唯一用户标识符 (126) 等于一组唯一用户标识符 (122) 的一个用户标识符，则使用所述唯一用户标识符 (126) 作为密钥来存储所述响应 (128) 的副本的部件。

15. 如权利要求 14 所述的数据处理系统，其中，由认证组件 (108) 来执行所述用户认证，其中，所述认证组件 (108) 将所述用户特有标记 (118) 添加到所述请求 (116) 中，其中，侦听器插件 (112) 将所述唯一用户标识符 (126) 与所述一组唯一用户标识符 (122) 进行比较，其中，所述侦听器插件 (112) 被插入代理服务器 (110)，所述代理服务器 (110) 位于所述服务 (124) 和所述客户端系统 (102) 之间，其中，所述侦听器插件 (112) 包括侦听控制列表 (120)，所述侦听控制列表 (120) 包含所述一组唯一用户标识符 (122)，其中，所述侦听器插件 (112) 链接到侦听管理器 (114)，其中，所述请求 (116) 和所述响应 (128) 被存储在所述侦听管理器 (114) 上。

16. 如权利要求 15 所述的数据处理系统，其中，所述请求 (116) 和所述响应 (128) 被存储在消息队列 (402) 上，其中，所述消息队列 (402) 被包括在所述侦听器插件 (112、332) 中，或者其中，所述请求 (116) 和所述响应 (128) 被存储在所述侦听管理器 (114、334) 上，由此，将所述请求 (116) 和所述响应 (128) 通过加密的端到端通信 (338) 而从所述消息队

列 (402) 传递到所述侦听管理器 (114、334)。

17. 如权利要求 15 所述的数据处理系统，其中，所述侦听管理器 (114、506) 包括用于存储所述侦听控制列表 (120) 的部件，并且其中，所述数据处理系统还包括：

用于在所述代理服务器 (502) 的启动之后将所述侦听器插件 (504) 加载到所述代理服务器 (502) 中的部件；

用于在所述代理服务器 (502) 的所述启动之后将所述侦听控制列表 (120) 从所述侦听管理器 (506) 加载到所述侦听器插件 (504) 中的部件。

18. 如权利要求 15 所述的数据处理系统，所述数据处理系统包括：

用于通过更新的侦听控制列表来更新由所述侦听管理器保存的所述侦听控制列表的部件；

用于将所述更新的侦听控制列表加载到所述侦听器插件中的部件。

19. 如权利要求 15 所述的数据处理系统，其中，所述侦听管理器包括用于建立到执法机构的网络的安全网络连接的部件，并且其中，仅仅所述执法机构的职员被特许访问所述侦听控制列表以及存储在所述侦听管理器上的被侦听的响应和请求，并且其中，仅仅准许所述服务提供商的所选择的职员访问所述侦听控制列表。

用于侦听客户端和服务之间的通信的方法和数据处理系统

技术领域

[0001] 本发明一般地涉及一种用于侦听客户端和服务之间的通信的方法和数据处理系统，并且具体涉及一种用于侦听客户端和服务之间的嫌疑人的通信的方法和数据处理系统。

背景技术

[0002] 在大多数国家中，法律强制通信或服务提供商使得能够为象特务机关、刑事调查部门以及国家和国际犯罪打击和犯罪防范组织的执法机构侦听顾客的通信。因此，电信服务提供商必须提供电信和 IT 基础设施，以便使执法部门能够侦听语音和数据流量。基本上，必须确保以下主要原则：

[0003] 1. 该侦听对于其通信被侦听的人来说必须是不可见的和不可识别的。

[0004] 2. 该侦听对于服务提供商的职员来说必须是不可见的和不可识别的。

[0005] 3. 仅仅允许侦听合法确定的嫌疑人的通信。

[0006] 然而，传统的语音通信基于电路交换网络技术，并且在接入点处，侦听相当容易实现，基于分组交换技术的 IP 数据流量暴露了关于上述原则的障碍。通常使用的用于侦听数据流量的方法是在特定的侦听点记录若干用户会话的所有 IP 流量，随后进行过滤器分析，以便重新产生完整的用户会话。三个原因主要地说明这一实践的低效：需要存储、管理和分析巨量数据。此外，记录数据流量不一定记录到所有通信数据，因为分组交换网络可以使用不可预测的路由和节点。侦听不是实时的，并且可能影响法律问题，原因是存储比所需的更多的用户数据。

[0007] 因此，在互连交换机中，诸如公共交换电话网和公共陆地移动网络的电话网络中进行侦听。所述交换机被互连到与执法机构相连接的传达设备。交换机使用电话号码 (ISDN/MSISDN) 作为侦听依据。在交换机处侦听对于某个电话号码的呼入或呼出通话。该交换机复制通信内容。除了呼叫者和被叫者之间的传输之外，经由传达设备将数据传递给执法机构。

[0008] 在基于 TCP/IP 的网络中，侦听与电话网络非常相似。交换机与连接到执法机构的传达设备相连接。使用 IP 地址的源地址字段、IP 地址的目的地地址字段或者二者取代电话号码作为侦听依据。通常的实践是记录来自或去往给定 IP 地址的所有连接数据（但不一定是全部内容）。存在若干种类型的信息源，从该信息源中，例如从 IP 路由器日志文件、从 HTTP 服务器日志文件、从网络协议分析器或从动态流量过滤，可以提取通信数据记录。

[0009] 已经知道一些专利，其描述用于合法侦听分组无线网络的侦听方法和系统。那些仅适用于网络运营商，原因是他们需要与其核心网络的交换基础设施进行深入交互。最接近的 5 个专利列出如下：

[0010] 美国专利申请 US220/0049913A1 和 US220/0051457A1——侦听系统和方法——涉及一种用于在诸如通用分组无线服务 (GPRS) 或通用移动通信系统 (UMTS) 的分组网络中进行合法侦听的侦听系统和方法。

[0011] 名称为侦听方法和系统的美国专利申请US2002/0078384A1涉及一种侦听方法和系统，用于在诸如通用分组无线服务(GPRS)或通用移动通信系统(UMTS)的分组网络中进行合法侦听的侦听系统和方法。

[0012] 美国专利申请US2002/0068582A1——用于向执法机构报告信息的方法、系统和传达设备——涉及蜂窝对电信网络用户通信的监控，并且特别涉及一种用于向执法机构报告所监控的信息的方法、系统和传达设备。

[0013] 在名称为——用于使用基于实时内容的网络监控来检测和报告在线活动的系统和方法的美国专利申请2002/0128925中描述了关于监控的更普通的方法。其一般地涉及通过诸如因特网、万维网或公司局域网(LAN)的公共或专用网络报告在线活动的系统。该专利仅适用于基于URL的过滤，并且不进行整个用户会话。它明确排除了对诸如图像的特定内容类型的侦听，因此不适用于合法侦听。

[0014] 基于IP的侦听使用定义的IP地址来侦听来自或去往特定IP地址的通信。然而，如果用户不具有诸如由例如因特网接入提供商的第三方提供的动态分配的IP地址的公知/固定IP地址，则基于IP地址的侦听并不够。要利用这样的IP地址侦听的用户建立的应用程序会话将不会被记录到。基于IP的侦听可以记录特定应用程序或整个基础设施的所有通信。然而，对于大量应用程序/网站来说，将记录的数据量是巨大的。这些数据的管理和处理需要大量的努力和例如以大量数据存储设备形式的资源。由于在此情况中将侦听所有应用程序会话，因此隐私问题确实存在，并且法律方面确实适用。为了从所记录的数据中获得所感兴趣的应用程序会话的内容，必须进行过滤。由于这涉及大量数据，因此所述过滤是耗时和耗费资源的。

[0015] 此外，可以使用传输层安全协议(TLS)或安全套接字层(SSL)来加密通过IP地址侦听所记录的数据。对诸如HTTP网络服务器日志或应用程序日志的标准应用程序和基础设施日志的分析不包含通信的全部内容。为了获得全部应用程序会话内容，需要修改应用程序以实现所需的日志记录。

[0016] 因此，确实存在对于用于侦听数据流量的改进的方法和数据处理系统的需要。

发明内容

[0017] 根据本发明的实施例，提供了一种侦听客户端和服务之间的通信的方法，其中，该方法包括执行所述客户端的用户的用户认证的步骤，以及由所述服务从所述客户端的用户接收请求的步骤。所述请求包括用户特有标记(token)，并且该用户特有标记包括唯一的用户标识符。由于所述用户认证，可以将该用户特有标识符分配给用户的请求。如果该唯一用户标识符与一组唯一用户标识符中的一个用户标识符相等，则存储该请求的副本，其中，将该唯一用户标识符用作密钥。

[0018] 将用户特有标记添加到从客户端发送给服务的所有请求。用户特有标记包括唯一的用户标识符。通过使用该用户特有标记，可以识别该用户。检查所述唯一的用户标识符是否等于包括在一组唯一用户标识符中的一个用户标识符。如果是这种情况，则记录请求的副本，从而将用户标识符用作密钥以便识别该用户。因此，通过将包括在标记中的用户标识符和一组唯一用户标识符进行比较来窃听客户端和服务之间的通信。在这组唯一用户标识符中，包含可疑的并且将被窃听的所有用户的用户标识符。

[0019] 根据本发明的实施例，所述方法还包括将来自服务的响应发送给客户端的步骤，其中，所述响应与包括用户特有标记的请求有关，所述用户特有标记包括唯一的用户标识符。如果该唯一用户标识符等于一组唯一用户标识符中的一个用户标识符，则在所述方法的另一步骤中，将所述响应的副本与作为密钥的唯一用户标识符一起存储。

[0020] 因此，不仅仅侦听从客户端发送到服务的请求。从服务发送给客户端的响应也被侦听。如果响应与包括标记的请求有关、其中所述标记具有也包括在该组唯一用户标识符中的唯一用户标识符，则存储该响应的副本。

[0021] 当仅仅对于在该组唯一用户标识符中存储了其用户标识符的用户的请求和响应进行侦听时，所述方法尤其有利。所有其它用户不受根据本发明的方法影响。因此，根据本发明的方法满足仅仅允许侦听合法确定的人的通信的法律要求。此外，被侦听的人不会觉察到他或她已经被侦听。

[0022] 根据本发明的实施例，通过认证组件来执行用户认证，其中，认证组件将用户特有标记添加到所述请求中，其中，侦听器插件将唯一的用户标识符与一组唯一用户标识符进行比较，其中，该侦听器插件被插入代理服务器，其中，该代理服务器位于服务和客户端之间，其中，侦听器插件包括侦听控制列表，其中，侦听控制列表包含该组唯一用户标识符，其中，侦听器插件连接到侦听管理器，其中，将所述请求和响应存储在侦听管理器上。

[0023] 典型为服务提供商的基础设施的第一组件并且从客户端接收消息的认证组件对用户进行认证，并且将用户特有标记添加到所述请求中。如上所述，用户特有标记包括唯一的用户标识符。所述请求还被传递给位于服务和客户端之间的代理服务器。侦听器插件被插入包括侦听控制列表的代理服务器。侦听控制列表保存该组唯一用户标识符。针对该组唯一用户标识符检查被包括在消息的标记中的用户标识符。如果唯一用户标识符被包括在该组唯一用户标识符中，则将响应副本存储在侦听管理器上。因为可以简单地将侦听器插件插入代理服务器，所以使用侦听器插件识别是否从应该被侦听的用户发送请求特别有利。然而，这要求服务提供商的基础设施包括代理服务器。还有可能在另一组件中使用侦听器插件。例如，可以将侦听器插件集成到认证组件中，此外，使用容留该侦听器插件的分离组件也是可行的。然后，将把这一组件布置在认证组件和服务之间。

[0024] 根据本发明的实施例，将所述请求和响应存储在消息队列中，其中，在侦听器插件中比较该消息队列，或者其中，将所述请求和响应存储在侦听器插件中，由此通过加密的端到端通信将所述请求和响应从消息队列或从侦听器插件传递到侦听管理器。

[0025] 根据本发明的实施例，将侦听控制列表永久存储在侦听管理器上，并且在代理服务器启动之后将侦听器插件加载到代理服务器中，并且在该代理服务器启动之后，将侦听控制列表从侦听管理器加载到侦听器插件中。

[0026] 根据本发明的实施例，利用被加载到侦听器插件中的更新的侦听控制列表来更新侦听控制列表，从而刷新所存储的侦听控制列表。

[0027] 根据本发明的实施例，从服务或从代理服务器的高速缓冲存储器接收所述响应。

[0028] 根据本发明的实施例，以加密的方式将所述请求和响应与对应的唯一用户标识符一起存储。这确保了将不会向未被授权访问被侦听的响应和请求的任何人授予访问权。

[0029] 根据本发明的实施例，侦听器插件和侦听管理器之间的连接是加密的端到端通信。当将被侦听的响应和请求从侦听插件传递到侦听管理器时，这阻止未被授权访问被侦

听的请求和响应的任何人。

[0030] 根据本发明的实施例，认证组件、代理服务器、侦听器插件、侦听管理器和服务本身是网络宿主环境的组件或服务提供商的基础设施的组件。例如但不唯一的是，所述服务与提供服务的服务器或者设备盒有关。

[0031] 根据本发明的实施例，侦听管理器和侦听器插件采用加密方法来存储侦听控制列表。以加密的方式存储被侦听的请求和响应以及侦听控制列表的优点在于防止未被授权访问这些敏感数据中的任一个的任何人这么做。当法律要求未被授权的任何人都不能访问这些敏感数据中的任一个时，这特别有利。因此，根据本发明的方法满足法律所要求的必要条件。

[0032] 根据本发明的实施例，侦听管理器通过安全线路连接到执法机构的网络，其中，仅仅执法机构的职员被特许访问存储在侦听管理器上的侦听控制列表以及被侦听的响应和请求，并且其中，仅仅准许服务提供商的被选中的职员访问侦听控制列表。

[0033] 在另一方面，本发明涉及一种计算机程序产品，其包括用于执行根据本发明的方法的计算机可执行指令。

[0034] 在另一方面，本发明涉及一种侦听客户端和服务之间的通信的数据处理系统，其中，所述数据处理系统包括用于执行客户端的用户的用户认证的部件和用于在服务处从客户端的用户接收请求的部件，其中，所述请求包括用户特有标记，其中该用户特有标记包括唯一的用户标识符，其中，由于所述用户认证，可以将该用户特有标记分配给该用户。该数据处理系统还包括用于如果所述唯一的用户标识符与一组唯一用户标识符中的一个用户标识符相等则使用所述唯一的用户标识符作为密钥来存储所述请求和相关响应的副本。

附图说明

[0035] 下面，将仅仅参考附图、作为示例来更详细地描述本发明的优选实施例，在附图中：

[0036] 图 1 示出了连接到被适配为侦听通信的服务提供商的基础设施的客户端系统的方框图，

[0037] 图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图，

[0038] 图 3 在方框图中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端和服务之间的数据流量，

[0039] 图 4 示出了侦听设施的可扩充 (scalable) 设置的方框图，

[0040] 图 5 是示出在侦听器插件启动期间由各个组件处理的步骤的顺序图，

[0041] 图 6 是图示当侦听通信时各个组件的交互的顺序图，以及

[0042] 图 7 示出了图示当更新侦听控制列表时执行的步骤的顺序图。

具体实施方式

[0043] 图 1 示出了连接到被适配为侦听通信的服务提供商 106 的基础设施的客户端系统 102 的方框图 100。服务提供商基础设施 106 包括认证组件 108、代理服务器 110、侦听管理器 114 和服务 124。用户 104 登录到客户端系统 102 中。客户端系统 102 例如是诸如 PC、移动电话或 PDA 的、运行浏览器应用程序的设备，其连接到服务提供商基础设施 106。服务

提供商知晓用户 104，因此服务提供商准许用户 104 访问服务提供商基础设施 106。

[0044] 认证组件 108 从客户端 102 接收请求 116。在那里，将带有用户标识符 126 的标记 118 添加到请求 116 中。可以通过用户标识符 126 来识别用户 104。请求 116 被发送给服务 124。代理服务器 110 位于认证组件 108 和服务 124 之间，使得请求 116 在它到达服务 124 之间通过代理服务器 110。代理服务器 110 包括侦听器插件 112。在此示例中，侦听器插件 112 是被插入代理服务器 110 中的插件。侦听器插件 112 保存列出一组用户标识符 122 的侦听控制列表 (ICL)120。侦听器插件 112 从请求 116 读取用户标识符 126。如果用户标识符 126 被包括在侦听控制列表 120 中，则将请求 116 的副本与用户标识符 126 一起发送到侦听管理器 114，在那里，将请求 116 的副本与用户标识符 126 一起存储。

[0045] 服务 124 接收请求 116。服务 124 将响应 128 发送回客户端。当响应 128 通过代理服务器 110 时，侦听器插件 112 检查该响应是否与被侦听的请求有关。如果是这样，则将响应 128 的副本与用户标识符 126 一起存储在侦听管理器 114 中。响应 128 被进一步发送给客户端系统 102，使得用户最终接收到根据其请求 116 的响应 128。由此，用户不知道他可能已被侦听。

[0046] 图 2 示出了图示由根据本发明的方法执行的基本步骤的流程图 200。在步骤 202 中，执行客户端系统的用户的用户认证。在步骤 204 中，在侦听器插件处从客户端的用户接收请求，其中，该请求包括含有唯一用户标识符的用户特定标记，其中，由于所述用户认证，可以将用户特有标记分配给该用户的请求。在步骤 206 中，检查该唯一用户标识符是否被包括在一组唯一用户标识符中。如果是这种情况，则根据本发明的方法继续进行步骤 208，其中，存储所述请求的副本。否则，根据本发明的方法继续进行步骤 210，其中，不进一步考虑动作。在步骤 208 或 210 的处理之后，在步骤 212 中，将所述请求传递到所述服务，在那里它被处理。

[0047] 图 3 在方框图 300 中图示了用于侦听的组件如何扩展公共宿主环境以便侦听客户端 312 和服务提供商基础设施 302 之间的数据流量。概念服务提供商基础设施是非常笼统的术语，并且它应当被理解为：在此文档的语境中，它指的是在最广泛的意义上向用户提供通信服务的服务提供商的基础设施。如先前所述，服务提供商只需要通过使用认证组件来识别该用户的方式。下面，将专注于与通信服务提供商所提供的基础设施不同的服务提供商的基础设施。通常，通信服务提供商通过使用分配给客户端的动态 IP 地址来授权用户的访问，并且允许到 IP 网络的通信。另一方面，服务提供商具有固定 IP 地址以及被用来获得服务的公知域名，所述服务例如可以是在线银行服务或者在更广的意义上为相同 IP 网络上的网络服务。

[0048] 客户端 312 可以是具有浏览器应用程序的设备，所述设备经由网络 310 连接到也被称为服务提供商所在地 (premise) 的服务提供商基础设施 302。客户端 312 也可以是使用包括语音浏览器（例如 VoiceXML 浏览器）的交互式语音响应 (IVR) 系统的电话，其中，通过服务提供商基础设施 302 通过网络 310 向其提供服务。语音浏览器应用网络技术，以便使用户能够经由言语和双音多频 (DTMF) 的组合而从电话访问服务。

[0049] 网络 310 可以是由通信服务提供商提供的所有类型访问信道的代表实体。如上所述，服务提供商和通信服务提供商通常不是相同的。这意味着服务提供商不知道除了客户端的 IP 地址以外的用户细节。服务提供商不能在没有通信服务提供商的帮助的情况下识

别或认证用户。由于这一事实，诸如在线银行的由服务提供商所提供的大多数网络应用要求用户在访问所述服务时认证他们自己。

[0050] 服务提供商基础设施 302 通常由 3 个组件组成，它们是 HTTP 服务器 304、应用程序服务器 306 和目录服务 308。此外，服务提供商基础设施通常包括所谓的边缘组件 313，其包括认证组件 314 和代理服务器 316。

[0051] 客户端 312 经由连接 318 和 320，通过网络 310 而连接到服务提供商基础设施 302。在认证组件 314 处接收来自客户端 312 的请求。认证组件 314 经由连接 330，针对目录服务 308 验证证书。认证组件 314 仅仅将可被证实的请求经由连接 322、324 和 326 转发到代理服务器 316、HTTP 服务器 304 或应用程序服务器 306。

[0052] 认证组件 314 还将用户特有标记添加到请求中。该用户特有标记包括可用以唯一地识别用户的唯一的用户标识符。

[0053] 将所述请求继续传递到代理服务器 316。代理服务器 316 包括侦听器插件 332，其分析所述标记，并且针对在侦听控制列表中列出的一组用户标识符来检查用户标识符。如果在侦听控制列表中列出了所述用户标识符，则将该请求的副本存储在例如侦听器插件的高速缓冲存储器中。

[0054] 所述请求被进一步传递给 HTTP 服务器 304 和应用程序服务器 306，由此，将与目录服务 308 的连接 328 用于授权的目的和用户细节。从应用程序服务器 326 产生响应，所述响应随后经由 HTTP 服务器 304 和边缘组件 313 而被发送回客户端系统 312。如果以前请求过所述请求，那么也可以直接由代理服务器 316 部分或全部地产生所述请求。

[0055] 代理服务器 316 的侦听器插件 332 还分析所述响应是否与带有标记的用户标识符的请求有关，其中所述用户标识符也被包括在侦听控制列表中列出的一组用户标识符中。如果在侦听控制列表中列出了所述用户标识符，则将所述响应的副本存储在例如侦听器插件的存储器中。

[0056] 通常，以加密的方式将被侦听的请求和响应存储在侦听器插件的存储器中，使得服务提供商的未被授权的服务职员不能访问所述请求和响应。此外，出于相同的原因，以加密的方式存储该侦听控制列表。

[0057] 侦听管理器 334 经由连接 338 连接到代理服务器 316，并且可以直接与侦听器插件 332 通信。可以使用连接 338 来在侦听器插件 332 和侦听管理器 334 之间建立加密的端到端通信。例如，可以周期性地建立连接 338，然后，可以将存储在侦听器插件 332 的存储器中的请求和响应从侦听器插件 332 传递到侦听管理器 334。

[0058] 或者，可以永久地建立连接 338，并且可以将被侦听的响应和请求从侦听器插件 332 直接传送到侦听管理器 334，在侦听管理器 334 中，它们将以加密的方式而被永久存储。侦听控制列表也以加密的方式被存储在那里。

[0059] 此外，在侦听器插件和侦听管理器组件之间可以使用消息队列，以便提高可用性和适用性。在这么做的时候，实现了侦听器插件 332 和侦听管理器 334 之间的有保证的传送，并且在服务中断的情况下避免了数据丢失。

[0060] 侦听管理器 334 经由连接 342 与网络 340 通信。连接 342 最好也是永久或临时建立的加密的端到端连接。网络 340 由执法机构控制。可以将被侦听地响应和请求从侦听管理器传递到网络 340，以便由执法机构的授权职员作进一步分析。

[0061] 如之前已经提到的那样，将用户特有标记添加到从客户端接收的所有请求中，在该客户端上该用户特定标记所涉及的用户访问服务提供商所在地。利用被包括在该侦听控制列表中的用户标识符来检查该用户特有标记。服务提供商知道该用户标识符。因此，执法机构必须向帮助建立侦听控制列表的服务提供商的职员中的几个人授权，因为这些人必须提供用户特有标识符。

[0062] 图4示出了侦听设施的可扩充设置的方框图400。该设置基本上与如图3所述的相同，并且根据本发明的用于侦听用户请求和响应的方法也是相同的。将水平扩充(scaling)技术应用于认证组件314、代理服务器316和对应的侦听器插件332。消息队列402被置于侦听器插件332和侦听管理器334之间。在侦听器插件332和侦听管理器组件334之间使用消息队列402，以便如上所述提高可用性和适用性。

[0063] 图5是示出在侦听器插件504启动期间由各个组件(即代理服务器502、侦听器插件504和侦听管理器506)处理的步骤的顺序图500。在步骤508中，启动代理服务器502。侦听器插件504被加载到代理服务器中。它被插入代理服务器502。在步骤510中，侦听器插件将它自己初始化。它从侦听管理器506请求侦听控制列表，所述侦听控制列表被加载到侦听器插件504的存储器中。侦听器插件504将“准备工作”信号发送回代理服务器502。在步骤512中，完成代理服务器502的启动，并且该代理服务器将其状态设置为“准备工作”。

[0064] 图6是图示当侦听嫌疑用户的通信时各个组件(即客户端系统602、认证组件604、代理服务器606、服务608、侦听器插件610、侦听管理器612和执法机构(LEA)614)的交互的顺序图600。

[0065] 在步骤630中，客户端602将请求发送给认证组件604。认证组件604在步骤616中对用户进行认证，将带有用户标识符的用户特有标记添加到该请求中，并且在步骤632中将该请求发送给代理服务器606。在步骤634中，调用侦听器插件610。针对侦听控制列表检查用户标识符，并且如果它被保存在侦听控制列表中，则在步骤618中侦听该请求。在步骤636中，将该请求的副本发送到侦听器管理器612，所述侦听器管理器612在步骤620中存储该请求。在步骤638中，它被进一步发送给执法机构614，或者更准确地说，它被进一步发送给该机构的网络。在步骤640中，代理服务器606还将所述请求转发给服务608，在那里，在步骤622中，执行该服务自身。在步骤642中，将与所述请求有关的响应发送回代理服务器606。该代理服务器在步骤644中调用侦听器插件。在步骤624中，如果所述响应与被侦听的请求有关，那么它也被侦听。所述响应的副本被发送给侦听管理器612，在那里，在步骤628中将其存储。在步骤648中，它被进一步发送给执法机构614。代理服务器606还在步骤650中将所述响应转发到认证组件604，在步骤652中，将所述响应发送给客户端。用户在不知道他可能已经被侦听的情况下接收到该响应。

[0066] 图7示出了图示被执行以便更新侦听控制列表(ICL)的步骤的顺序图700。在步骤710中，授权的管理员702维护和更新存储在侦听管理器704上的侦听控制列表(ICL)。在步骤712中，分发更新的侦听控制列表。在步骤718中将该侦听控制列表发送到侦听器插件706。在步骤714中，更新的侦听控制列表刷新所存储的侦听控制列表。在步骤720中，将向侦听管理器704通知已经成功地进行了该更新的消息从侦听器插件706发送到侦听管理器704。在步骤716中，将更新信息发送给执法机构(LEA)708。在步骤722中，向LEA708

通知允许对侦听控制列表（ICL）的改变。

[0067] 参考标号列表

[0068]

100	方框图
102	客户端系统
104	用户
106	服务提供商基础设施
108	认证组件
110	代理服务器
112	侦听器插件
114	侦听管理器
116	请求
118	标记
120	侦听控制列表
122	一组用户标识符
124	服务
126	用户标识符
128	响应
200	流程图
202	用户认证
204	在侦听器插件处接收用户的请求
206	检查是否设置了标记
208	存储请求的副本
210	无动作
212	处理服务

300	方框图
302	服务提供商基础设施
304	HTTP 服务器
306	应用程序服务器
308	目录服务
310	网络
312	客户端

[0069]

313	边缘组件
314	认证组件
316	代理服务器
318	连接
320	连接
322	连接
324	连接
326	连接
328	连接
330	连接
332	侦听器插件
334	侦听管理器
336	连接
338	连接
340	网络
342	连接

400	方框图
402	消息队列
500	顺序图
502	代理服务器
504	侦听器插件
506	侦听管理器
600	顺序图
602	客户端系统
604	认证组件
606	代理服务器
608	服务
610	侦听器插件
612	侦听管理器
614	执法机构

[0070]

700	顺序图
702	管理员
704	侦听管理器
706	侦听器插件
708	执法机构

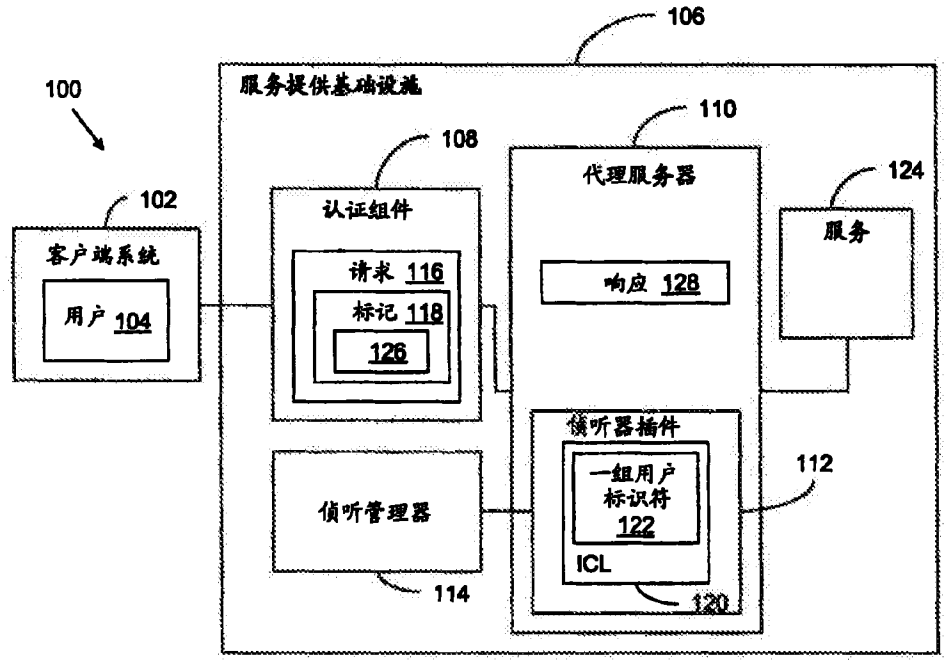


图 1

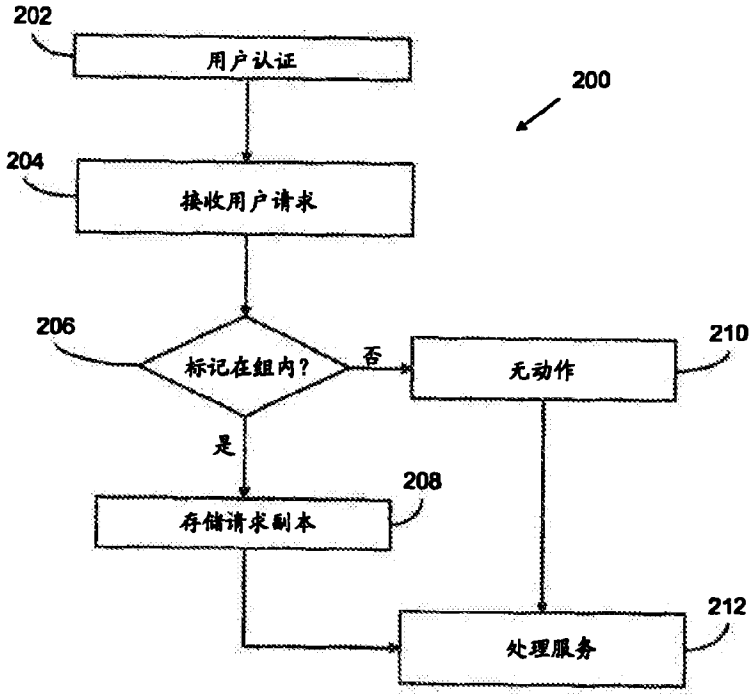


图 2

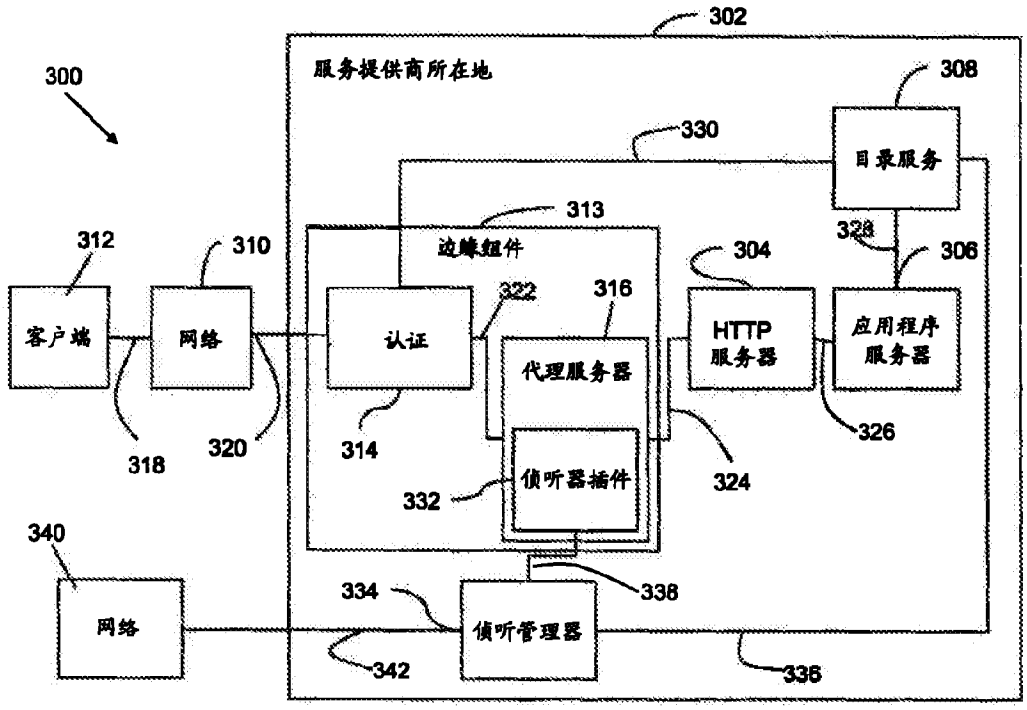


图 3

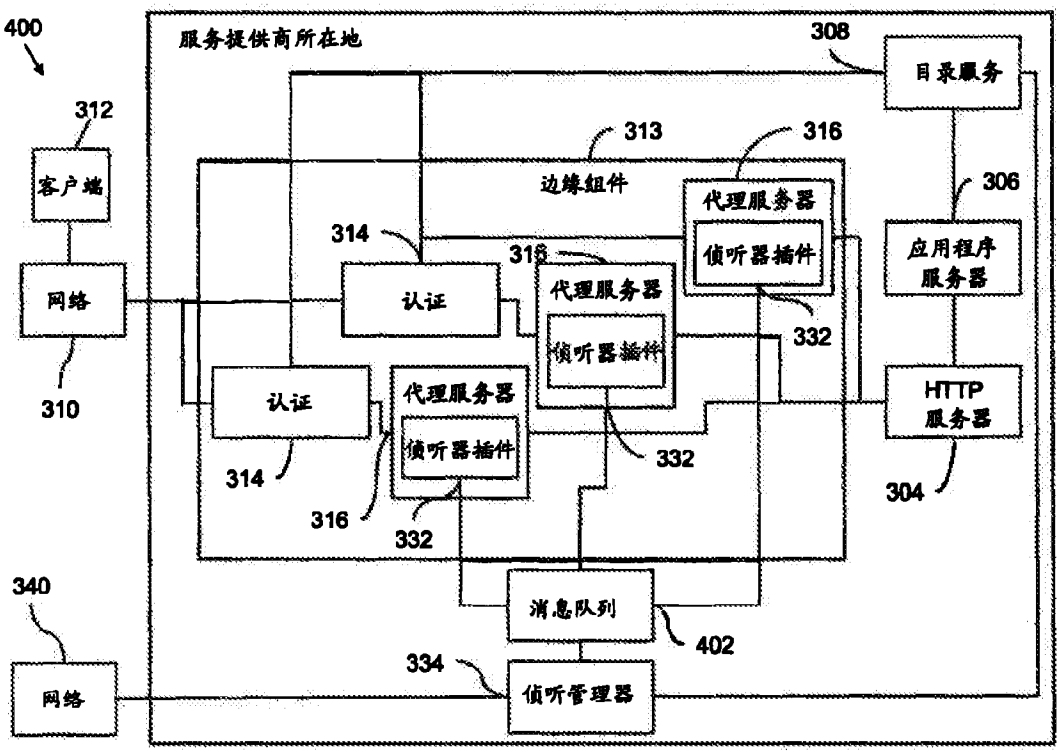


图 4

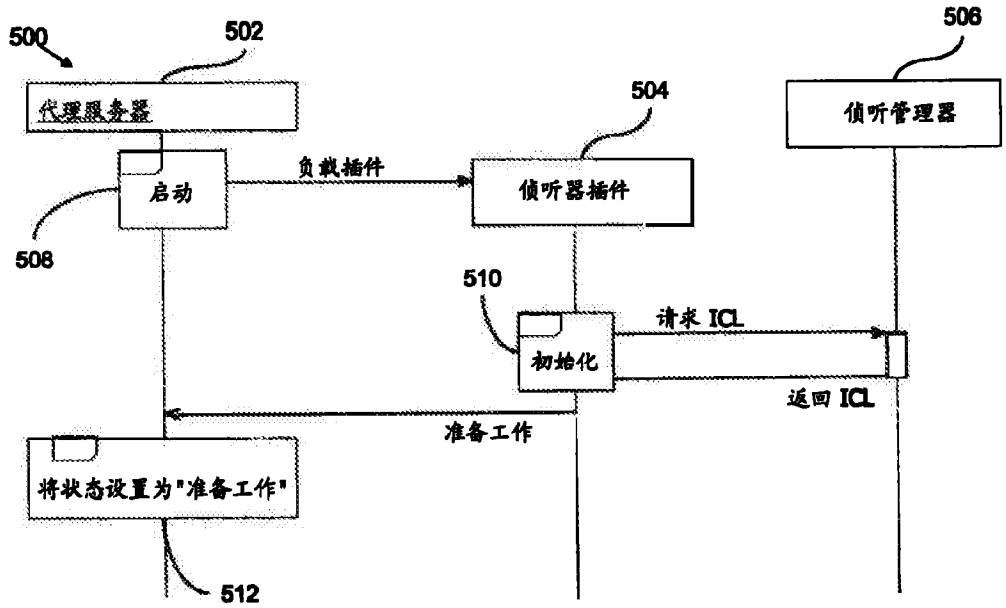


图 5

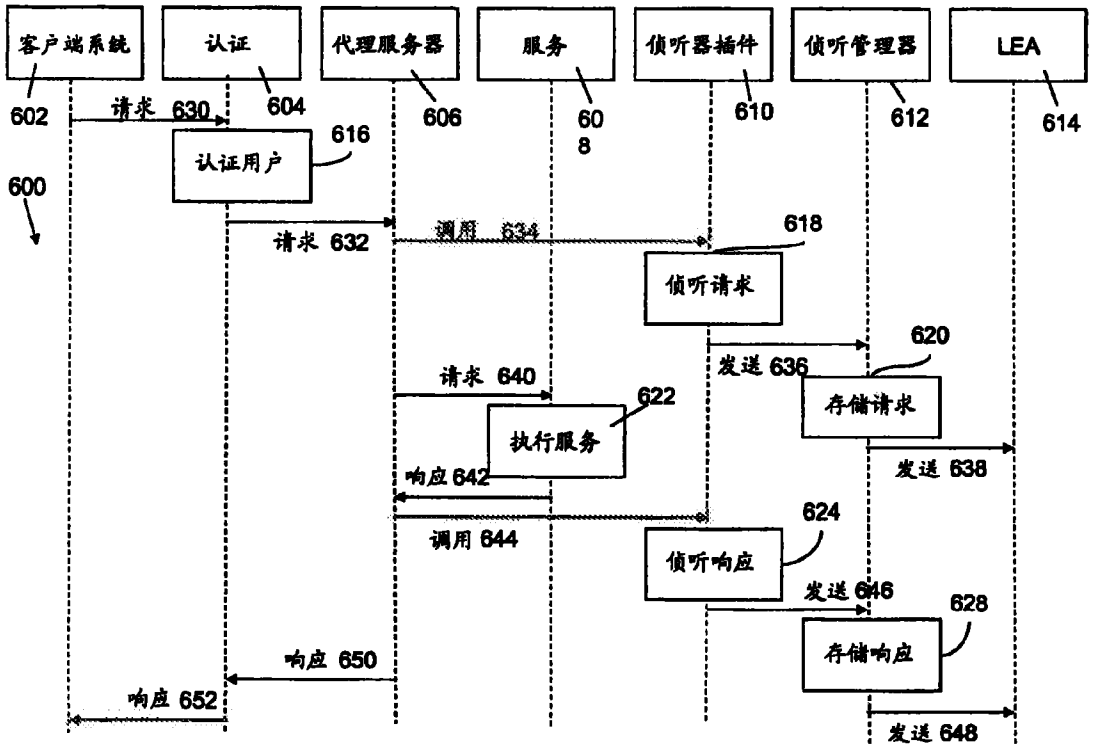


图 6

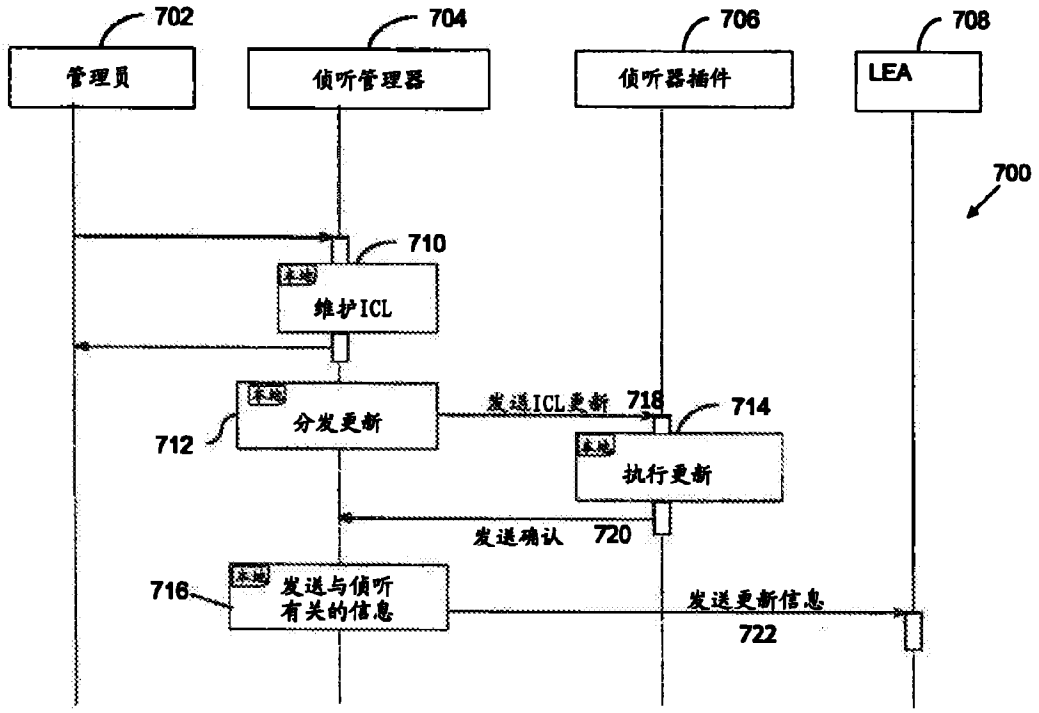


图 7

Espacenet

Bibliographic data: CN101772929 (B) — 2014-07-02

System and method for indicating emergency call back to user equipment

Inventor(s): PURNADI RENE W; ISLAM M KHALEDUL + (PURNADI RENE W, ; ISLAM M. KHALEDUL)

Applicant(s): RESEARCH IN MOTION LTD + (RESEARCH IN MOTION LIMITED)

Classification: **- international:*H04L12/66; H04M11/06; H04Q3/64***
- cooperative: H04M3/5116; H04Q3/64; H04L65/1016; H04M1/72538; H04Q2213/13152; H04Q2213/13176; H04Q2213/13204; H04Q2213/13248; H04Q2213/13348; H04Q2213/1337; H04Q2213/13389

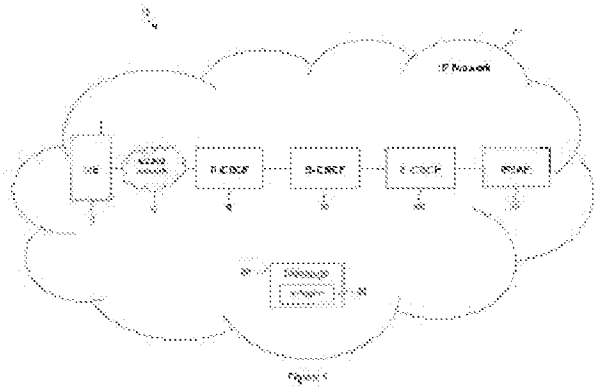
Application number: CN20078100171 20071204

Priority number(s): WO2007CA02176 20071204 ; US20070944258P 20070615

Also published as: CN101772929 (A) WO2008151406 (A1) WO2008151406 (A8) US2008310599 (A1) MX2009013633 (A) KR20120051078 (A) KR101162903 (B1) KR20100029124 (A) KR101162847 (B1) EP2165489 (A1) EP2165489 (A4) CA2690236 (A1) less

Abstract of CN101772929 (A)

A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.



(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101772929 B
(45)授权公告日 2014.07.02

(21)申请号 200780100171.X
(22)申请日 2007.12.04
(30)优先权数据
60/944,258 2007.06.15 US
(85)PCT国际申请进入国家阶段日
2010.02.05
(86)PCT国际申请的申请数据
PCT/CA2007/002176 2007.12.04
(87)PCT国际申请的公布数据
WO2008/151406 EN 2008.12.18
(73)专利权人 黑莓有限公司
地址 加拿大安大略省沃特卢市
(72)发明人 雷纳·W·普尔纳迪
M·哈立德·伊斯兰
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王玮
(51)Int.Cl.
H04L 12/66(2006.01)
H04Q 3/64(2006.01)
H04M 11/06(2006.01)
(56)对比文件
WO 2007016695 A2,2007.02.08,
US 2006072547 A1,2006.04.06,
审查员 林桂荣

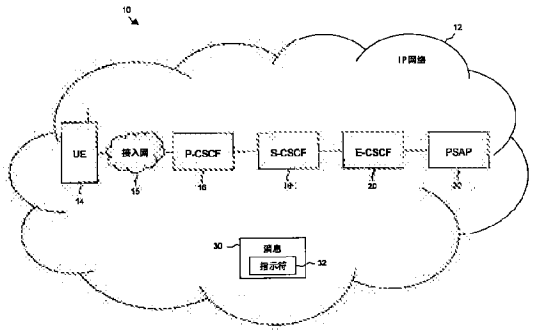
权利要求书1页 说明书8页 附图5页

(54)发明名称

向用户设备指示紧急回叫的系统和方法

(57)摘要

提供了一种用于向用户设备14和接入网15指示IMS(互联网协议多媒体子系统)紧急回叫的方法。该方法包括:将该紧急回叫来自PSAP(来自公共安全应答点)22的指示32包括在从PSAP至用户设备14和接入网15的消息30中。



CN 101772929 B

1. 一种向用户设备指示互联网协议多媒体子系统 IMS 紧急呼叫的设备，包括：

用于利用被包括在会话发起协议 SIP Invite 消息中的指示，将互联网协议多媒体子系统 IMS 呼叫识别为来自公共安全应答点 PSAP 的紧急呼叫的装置，

其中，所述指示是将 PSAP 标识为紧急呼叫来源的字符串，所述指示被包括在 SIP Invite 消息的来自首部或 P-Asserted-Identity 首部之一中。

2. 根据权利要求 1 所述的设备，其中，所述 SIP Invite 消息来自 PSAP。

3. 根据权利要求 1 所述的设备，还包括用于检查所有输入 SIP Invite 消息以发现所述指示的装置。

4. 根据权利要求 1 所述的设备，还包括用于当在用户设备接收到所述指示之后预定义时间长度内用户设备没有接收到响应于紧急呼叫的输入时触发自主动作的装置。

5. 根据权利要求 4 所述的设备，其中，所述自主动作是以下至少一项：

向 PSAP 发送自动化消息；

向 PSAP 发送用户设备的位置；以及

向除 PSAP 以外的紧急相关实体发送自动化消息。

6. 根据权利要求 1 所述的设备，其中，所述指示是每当用户设备发起 IMS 紧急呼叫时创建的。

7. 一种向用户设备指示互联网协议多媒体子系统 IMS 紧急呼叫的方法，包括：

利用被包括在会话发起协议 SIP Invite 消息中的指示，将互联网协议多媒体子系统 IMS 呼叫识别为来自公共安全应答点 PSAP 的紧急呼叫，

其中，所述指示是将 PSAP 标识为紧急呼叫来源的字符串，所述指示被包括在 SIP Invite 消息的来自首部或 P-Asserted-Identity 首部之一中。

8. 根据权利要求 7 所述的方法，其中，所述 SIP Invite 消息来自 PSAP。

9. 根据权利要求 7 所述的方法，还包括：当在用户设备接收到所述指示之后预定义时间长度内用户设备没有接收到响应于紧急呼叫的输入时，所述指示通过用户设备来触发自主动作。

10. 根据权利要求 9 所述的方法，其中，所述自主动作是以下至少一项：

向 PSAP 发送自动化消息；

向 PSAP 发送用户设备的位置；以及

向除 PSAP 以外的紧急相关实体发送自动化消息。

11. 根据权利要求 7 所述的方法，其中，当经由代理呼叫会话控制功能 P-CSCF 来将 SIP Invite 消息通信至用户设备时，所述 P-CSCF 通知接入网准备和以优先顺序排列针对紧急呼叫的资源。

12. 根据权利要求 7 所述的方法，其中，所述指示是每当用户设备发起 IMS 紧急呼叫时创建的。

向用户设备指示紧急回叫的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求由Purnadi等于2007年6月15日提交的、标题为“System and Method for Indicating IMS Emergency Call Back to UserEquipment”的美国临时专利申请的优先权，其全部内容并入此处以供参考。

背景技术

[0003] IP（互联网协议）多媒体子系统（IMS）是用于提供许多电话服务提供商开始实现的移动和固定多媒体服务的标准化架构。IMS架构可以包括使用标准协议进行通信的不同功能（即，网络元件）的集合。

[0004] 使用移动设备或任何用户设备（UE）的IMS网络用户可以进行紧急呼叫，例如911呼叫（在北美）或112呼叫（在欧洲大多数地区）。典型地，这种呼叫由公共安全应答点（PSAP）来处理，所述公共安全应答点可能协调对紧急事件的适当响应。在紧急呼叫终止之后，PSAP可以出于多种原因对用户进行回叫。例如，如果紧急呼叫出现异常终止，则PSAP可能回叫用户以确定用户是否希望传达任何附加信息。备选地，PSAP可能回叫用户以要求在初始呼叫中因疏忽而未请求的信息。在紧急呼叫终止之后从PSAP至紧急呼叫者的回叫的其他原因可以是本领域技术人员所熟悉的。

附图说明

[0005] 为了更完整地理解本公开，现在参照结合附图和详细的说明书而作出的以下简要描述，其中，类似的参考标记表示类似的部分。

[0006] 图1是根据本公开的实施例的包括用户设备和公共安全应答点在内的示意性IP网络的图。

[0007] 图2是示出了根据本公开的实施例的呼叫流程的顺序图。

[0008] 图3是包括可操作于本公开的各个实施例中的一些的用户设备在内的无线通信系统的图。

[0009] 图4是可操作于本公开的各个实施例中的一些的用户设备的框图。

[0010] 图5是可在可操作于本公开的各个实施例中的一些的用户设备上实现的软件环境的图。

[0011] 图6是适于本公开的各个实施例中的一些的示意性通用计算机系统。

具体实施方式

[0012] 起初应当理解，尽管以下提供了本公开的一个或多个实施例的示意性实施方式，但所公开的系统和/或方法是可以使用任何数目的技术来实现的，不论该技术是当前已知的还是现有的。本公开绝不应限于示意性实施方式、附图和以下示意的技术，包括此处示意和描述的示例设计和实施方式，但是在所附权利要求及其等同替换的全部范围内可以修改本公开。

[0013] 在实施例中，提供了一种向用户设备和接入网指示 IMS（互联网协议多媒体子系统）紧急回叫的方法。所述方法包括：将所述紧急回叫来自 PSAP（来自公共安全应答点）的指示包括在从 PSAP 至用户设备和接入网的消息中。

[0014] 在另一实施例中，提供了一种用户设备，包括被配置为将 IMS（互联网协议多媒体子系统）呼叫识别为来自 PSAP 的紧急回叫的处理器。

[0015] 在另一实施例中，提供了一种系统，包括一个或多个处理器和指令。所述指令在被所述一个或多个处理器处理器执行时，促使在从 PSAP 至用户设备 (UE) 的消息中提供紧急回叫指示符。

[0016] 当在从 UE 至 PSAP 的 IMS 紧急呼叫终止之后 PSAP 试图对 UE 进行 IMS 回叫时，如果 UE 没有识别出该回叫是来自 PSAP 的，则可能出现不期望的结果。例如，UE 可以将该回叫视为常规的呼叫并将其置为中断或呼叫等待，回叫可能被阻止，或 UE 可能无法对回叫适当地作出响应。本公开提供了通过将向 UE 的、回叫来自 PSAP 的指示包括在回叫中，来向 UE 指示来自 PSAP 的 IMS 紧急回叫。这允许 UE 在紧急回叫与常规呼叫之间进行区分。将向 UE 的呼叫标识为来自 PSAP 的回叫的指示或指示符可以以不同方式与该呼叫相关联，这些方式中的一些方式将在以下更详细地讨论。其他方式是本领域技术人员根据本公开将容易地想到的。在 US 专利 7,050,785 和 7,139,549 中提供了其他技术，这两个专利都是 Islam 等的，出于所有目的并入此处以供参考。

[0017] 图 1 示出了包括 IP（互联网协议）网络 12 的系统 10，系统 10 还可以包括 IMS 网络的一个或多个组件。示出了 UE 14，UE 14 可以包括连接至 IMS 网络的任何终端用户设备或系统（例如，移动电话、移动无线设备（包括数字、蜂窝或双模式设备）个人数字助理、膝上型 / 写字板 / 笔记本计算机、台式计算机等）。CSCF（呼叫会话控制功能）（未明确示出）是 IMS 网络中的公知元件，负责例如维护 SIP（会话发起协议）呼叫以及针对访问 IMS 网络内的服务的订户提供会话控制。

[0018] UE 14 经由接入网 15 来与 P-CSCF（代理 CSCF）16 进行通信。接入网 15 可能是任何公知的组件（例如，基站以及可以促使与后续网络组件进行无线连接的其他无线发送和接收设备）的集合。P-CSCF 16 是 SIP 代理，该 SIP 代理可以是针对 IMS 终端的第一接触点，并且如果所访问的网络还不是 IMS 兼容的，则 SIP 代理可以位于在全 IMS 网络中或归属网络中的所访的问网络中。P-CSCF 16 与 S-CSCF（服务 CSCF）18 进行通信。S-CSCF 18 是 SIP 服务器，该 SIP 服务器可以位于归属网络中，并可以执行会话控制、用户简档的下载和上载、以及其他功能。S-CSCF18 与 E-CSCF（紧急 CSCF）20 进行通信。E-CSCF 20 提供针对 PSAP（公共安全应答点）22 的会话控制功能，PSAP 22 可以是 911 系统或者另一紧急呼叫中心或系统。

[0019] 为了进行紧急呼叫或 911 呼叫，UE 14 可能经由 P-CSCF 16、S-CSCF 18 和 E-CSCF 20 来与 PSAP 22 进行通信。然而，仅当 UE 14 漫游时，才可能进行经由 P-CSCF 16 的通信。当 UE 14 处于其归属网络中时，可以不需要 P-CSCF 16，并且 UE 14 可能直接与 S-CSCF 18 进行通信。以下，被描述为经由 P-CSCF 16 进行的任何通信都应被理解为可能在不存在 P-CSCF 16 的情况下进行。

[0020] 当前 3GPP（第 3 代合作伙伴计划）和 3GPP2（第 3 代合作伙伴计划 2）规范 (3GPP 中的 TS 23.167 和 3GPP2 中的 X.P0049) 没有指定使 UE 14 确定输入呼叫是否实际上是来

自紧急系统（如 PSAP 22）的回叫的方法。根据一个实施例，PSAP 22 提供了 IMS 紧急回叫消息 30（如 SIPInvite），包括紧急回叫指示或指示符 32。UE 14 可以使用指示符 32 来将呼叫标识为来自 PSAP 22 的 IMS 紧急回叫，然后可以对该回叫适当地作出响应。例如，UE 14 可能使用指示符 32 来在与接入网 15 的承载建立期间设置合适的优先级，可能在必要时丢弃和阻止其他呼叫，或者可能采取其他动作以促进或增大成功完成紧急回叫的可能性。指示符 32 还可以允许 UE 14 提供向 UE 用户通知来电紧急回叫的事件（例如，可听的或视频显示的警告）。

[0021] 如果 UE 用户在过了特定时间之后尚未对回叫作出相应，则 UE 14 还可以使用指示符 32 来触发动作。无法以及时的方式应答紧急回叫可能是用户丧失了能力或需要紧急服务的指示。当在接收到指示符 32 之后预定义时间长度内没有进行对紧急回叫的响应时，UE 14 可能向 PSAP 22 发起指示用户不能作出应答的自动答复，可能发送 UE 14 的位置坐标，可能向另一紧急系统发送自动化消息，或者可能触发其他动作。例如，UE 14 可能在没有来自用户的物理输入的情况下完成呼叫，这在用户不能物理激活 UE 14 以接收呼叫时可能是有益的。P-CSCF 16 可以向接入网 15 提供紧急回叫指示符 32，并且接入网 15 可以使用紧急回叫指示符 32 来准备和以优先顺序排列紧急回叫的适当资源。

[0022] 可以基于当前规范以多种方式来传送紧急回叫指示符 32。然而，本公开不限于此，还可适用于多种不同系统和环境中。在一个实施例中，可以通过将 PSAP 公共指示符 (PSAP PUID) 包括于在终止来自 UE14 的紧急呼叫之后从 PSAP 22 发送至 UE 14 的 SIP 消息中来提供指示符 32。更具体地，可以将 PSAP PUID 包括在 SIP Invite 消息中作为指示符 32。在这种情况下，PSAP PUID 具有将 PSAP 22 标识为紧急相关实体的标准命名约定或格式（如 name@sos.domain、psap@domain 等）可以是有益的。即，单词或者字母、数字或其他字符的排列（如‘psap’、‘sos’或‘emergency’）可能用在 SIP Invite 中，以指示消息 30 是来自紧急系统（如 PSAP 22）的。

[0023] 可以在从 PSAP 22 发送至 UE 14 的 SIP Invite 消息中的各个位置提供 PSAP PUID。例如，PSAP PUID 可以置于典型地提供与 SIP 消息发送者身份有关的信息的“来自首部”中。SIP Invite “来自首部”中的标准化 PSAP PUID 格式可以使 SIP Invite 可容易地被 UE 14 识别为与来自 PSAP 22 的紧急回叫相关联的消息。即，UE 14 可能检验“来自首部”以找到指示 SIP Invite 来自 PSAP 22 的名称或字符串（如‘psap’、‘sos’或‘emergency’）。如果找到了这种字符串，则 UE 14 知道该消息来自 PSAP22 并相应地作出响应。UE 14 可能检验每个 SIP Invite 消息以发现该名称或字符串，或者可能仅在 UE 14 进行 911 呼叫或其他紧急呼叫之后的一段时间内进行检验。

[0024] 在另一实施例中，UE 紧急公共标识符 (ePUID) 可以用作指示符 32。作为背景，仅当 UE 14 执行 IMS 紧急注册时，UE 14 当前获得与标准 PUID 不同的 ePUID。然而，在当前指导原则下，仅当 UE 14 在处于其归属网络之外的同时进行紧急呼叫时，或者仅当 UE 14 不具有足够证书来执行 IMS 常规注册时，UE 14 才执行 IMS 紧急注册。因此，ePUID 可能不始终可用作指示符 32。

[0025] 本实施例提供了以下情况：每当 UE 14 进行紧急呼叫时 UE14 都执行紧急 IMS 注册，而不论 UE 14 时处于其归属网络中还是在漫游，也不论 UE 14 是否具有足够证书来进行常规注册。于是，甚至当 UE 14 从其归属网络内进行紧急呼叫时，UE 14 也可能具有 ePUID，

并且每当UE 14进行紧急呼叫时，UE 14都可以将该ePUID通过给PSAP 22。当PSAP 22向UE 14进行紧急回叫时，PSAP 22就可以使用ePUID作为消息30中的指示符32。更具体地，ePUID可以置于标识SIP消息接收者的SIP Invite“去往首部”中。当UE 14接收到包括自身ePUID的消息（例如在“去往首部”中具有UE ePUID的SIP Invite）时，UE 14可以将该消息识别为与来自PSAP 22的紧急回叫相关联并可以适当地作出响应。

[0026] 在其他实施例中，可以以多种其他方式将紧急回叫指示符32包括在从PSAP 22至UE 14的SIP Invite中。例如，可能添加显式的新紧急回叫首部，或者可能将隐式的紧急回叫指示符32置于现有首部（如P-Asserted-Identity首部）内。备选地，其他消息30可以包括或可以用作指示符32，或者可以采用本领域技术人员借助本公开容易想到的多种其他方式或技术。

[0027] 图2示出了先前使用其标准PUID发起了IMS紧急呼叫会话的UE14的示例性呼叫流程图。在该实施例中，当紧急呼叫终止时，PSAP 22试图使用SIP Invite消息来回叫UE 14。SIP Invite在“去往首部”中包括UE PUID，并在“来自首部”中包括标准化的或经识别的PSAP PUID（如name@sos.domain）。在“来自首部”中使用的标准化PSAP PUID格式由P-CSCF 16（或不存在P-CSCF 16时由S-CSCF 18）和UE 14识别为来自PSAP 22的紧急呼叫的指示。P-CSCF 16或S-CSCF 20触发接入网15，从而如上所述，UE 14和接入网15可以针对该呼叫设置最高优先级以确保成功的紧急回叫和/或可以执行其他动作。

[0028] 在事件202处，响应于异常紧急呼叫终止，或处于某种其他原因，PSAP 22向UE 14发起回叫。PSAP 22形成SIP Invite消息，该SIP Invite消息在“去往首部”中包括UE PUID并使用标准化的或经识别的PSAPPUID格式作为“来自首部”中的指示符。在该示例中，PSAP PUID使用name@sos.domain作为标准格式。从PSAP 22发起的SIP Invite中的‘sos’向UE 14指示这是紧急回叫。然而，置于SIP Invite消息中或其他消息中其他位置的其他参数也可以用作指示符。然后，将以这种方式形成的SIP Invite发送至E-CSCF 20。

[0029] 在事件204处，E-CSCF 20将SIP Invite转发至S-CSCF 18。在事件206处，S-CSCF 18将SIP Invite转发至P-CSCF 16。在事件208处，P-CSCF 16将SIP Invite转发至UE 14。P-CSCF 16可以使用紧急回叫指示符作为触发以通知接入网准备和以优先顺序排列紧急回叫的资源。在事件210处，UE 14检查输入SIP Invite中的“来自首部”，并将‘sos’识别为指示SIP Invite来自PSAP 22且SIP Invite与紧急回叫相关联的标准化格式。然后，UE 14可以使用该指示来将呼叫置为最高优先级，以确保成功的紧急回叫。UE 14也可以采取其他动作，包括：丢弃其他正在进行的呼叫、在无线承载建立过程中设置适当的优先级等等。

[0030] 在事件212处，UE 14形成SIP 200OK消息以对SIP Invite作出响应。UE 14将PSAP PUID置于“去往首部”中，并将其自身的UE PUID置于“来自首部”中。然后，将SIP 200OK发送至P-CSCF 16。注意，根据3GPP2规范，P-CSCF 16可能不允许通过在“去往首部”中具有PSAPPUID的SIP Invite来进行紧急呼叫初始化。然而，事件212处发送的消息不是SIP Invite初始化消息，而可以是SIP 200OK。因此，如事件214处所示，P-CSCF 16允许在“去往首部”中具有PSAP PUID的消息。应当注意，P-CSCF 16典型地需要知道并准备好接收SIP 200OK，或者P-CSCF 16可能拒绝SIP 200OK。在P-CSCF 16已从PSAP 22接收到SIPInvite之后，可以使P-CSCF 16知道UE 14可能发送200OK。

[0031] 在事件 216、218 和 220 处，P-CSCF 16 经由 S-CSCF 18 和 E-CSCF 20 来向 PSAP 22 路由 SIP 200OK。在事件 222 处，PSAP 22 形成 SIP ACK 消息以对 SIP 200OK 作出响应。PSAP 22 将 UE PUID 置于“去往首部”中，并将其自身的 PSAP PUID 置于“来自首部”中，并将 SIP ACK 发送至 E-CSCF 20。在事件 224、226 和 228 处，经由 S-CSCF 18 和 P-CSCF 16 来向 UE 14 路由 SIP ACK。在这一点上，如事件 230 处所示，完成紧急回叫的建立。应当理解，图 2 仅示出了本公开的一个实施例的一个呼叫流程，并且本公开不仅限于所示出的呼叫流程。对于此处公开的多个其他实施例，可能发生其他其他呼叫流程。

[0032] 图 3 示出了包括 UE 14 的实施例在内的无线通信系统。UE 14 可操作用于实现本公开的方面，但本公开不应限于这些实施方式。尽管被示为移动电话，但 UE 14 可以采取多种形式，包括无线手机、寻呼机、个人数字助理 (PDA)、便携式计算机、写字板计算机或膝上型计算机。许多合适的设备将这些功能当中的一些或全部相结合。在本公开的一些实施例中，UE 14 不是如便携式、膝上型或写字板计算机之类的通用计算设备，而是如移动电话、无线手持机、寻呼机、PDA 或车辆中安装的电信设备之类的专用通信设备。在另一实施例中，UE 14 可以是便携式、膝上型或其他计算设备。UE 14 可以支持专门的活动，例如游戏、库存控制、作业控制和 / 或任务管理功能等。

[0033] UE 14 包括显示器 402。UE 14 还包括触敏表面、键盘或由用户输入的总体称为 404 的其他输入键。键盘可以是全字母数字键盘或简化字母数字键盘 (如 QWERTY、Dvorak、AZERTY 和顺序类型) 或与电话键区相关联的带有字母表字母的传统数字键区。输入键可以包括滚轮、退出或换码键、轨迹球以及其他导航或功能键，其可以被向内按下以提供更多的输入功能。UE 14 可以呈现供用户选择的选项、供用户驱动的控件和 / 或供用户导向的光标或其他指示符。

[0034] UE 14 还可以接受来自用户的数据条目，该数据条目指示用于拨打的号码或用于对 UE 14 的操作进行配置的不同参数值。UE 14 还可以响应于用户命令来执行一个或多个软件或固件应用程序。这些应用程序可以将 UE 14 配置为响应于用户交互来执行不同定制功能。此外，可以用无线电来编程和 / 或配置 UE 14，例如从无线基站、无线接入点或对等端 UE 14 来配置 UE 14。

[0035] 在可由 UE 14 执行的各种应用程序当中有网页浏览器，其使显示器 402 能够示出网页。该网页是可以经由与无线网络接入节点、蜂窝塔、对等端 UE 14 或者任何其他无线通信网络或系统 400 进行无线通信来获得的。网络 400 耦合至有线网络 408(如互联网)。经由无线链路和有线网络，UE 14 可以访问不同服务器 (如服务器 410) 上的信息。服务器 410 可以提供可在显示器 402 上示出的内容。备选地，UE 14 可以以中继类型或跳类型的连接，通过充当中间媒介的对等端 UE 14，来接入网络 400。

[0036] 图 4 示出了 UE 14 的框图。尽管示出了 UE 14 的多种已知组件，但在实施例中，可以在 UE 14 中包括所列出的组件和 / 或未列出的附加组件的子集。UE 14 包括数字信号处理器 (DSP)502 和存储器 504。如图所示，UE 14 还可以包括天线和前端单元 506、射频 (RF) 收发器 508、模拟基带处理单元 510、麦克风 512、听筒扬声器 514、耳机端口 516、输入 / 输出接口 518、可拆卸式存储卡 520、通用串行总线 (USB) 端口 522、短距离无线通信子系统 524、警报器 526、键区 528、液晶显示器 (LCD)，该液晶显示器 (LCD) 可以包括触敏表面 530、LCD 控制器 532、电荷耦合器件 (CCD) 摄像机 534、摄像机控制器 536 和全球定位系统 (GPS) 传感

器 538。在实施例中，UE 14 可以包括另一种显示器，其不提供触敏屏幕。在实施例中，DSP 502 可以直接与存储器 504 进行通信而不经过输入 / 输出接口 518。

[0037] DSP 502 或某其他形式的控制器或中央处理单元操作用于根据在存储器 504 中存储的或在 DPS 502 本身内包含的存储器中存储的嵌入式软件或固件，来控制 UE 14 的各种组件。除了嵌入式软件或固件之外，DPS 502 还可以执行其他应用程序，该其他应用程序存储在存储器 504 中，或者是可经由如便携式数据存储介质（如可拆卸式存储卡 520）之类的信息载体介质、或经由有线或无线网络通信而获取到的。应用软件可以包括将 DSP 502 配置为提供所期望的功能的、已编译的机器可读指令集，或者应用软件可以是要由解释器或编译器来处理以间接配置 DSP 502 的高级软件指令。

[0038] 可以提供天线和前端单元 506 以在无线信号和电信号之间进行转换，使得 UE 14 能够发送和接收来自蜂窝网络或某些其他可用无线通信网络或来自对等端 UE 14 的信息。在实施例中，天线和前端单元 506 可以包括多个天线以支持波束成形和 / 或多输入多输出 (MIMO) 操作。本领域技术人员已知，MIMO 操作可以提供空间多样性，其可以用于克服困难的信道条件和 / 或增加信道吞吐量。天线和前端单元 506 可以包括天线调谐和 / 或阻抗匹配组件、RF 功率放大器和 / 或低噪声放大器。

[0039] RF 收发器 508 提供了频移，将接收到的 RF 信号转换到基带并将基带发送信号转换到 RF。在一些描述中，无线电收发器或 RF 收发器可以被理解为包括其他信号处理功能，如调制 / 解调、编码 / 解码、交织 / 去交织、扩频 / 解扩、快速傅立叶逆变换 (IFFT) / 快速傅立叶变换 (FFT)、循环前缀附加 / 移除以及其他信号处理功能。出于清楚的目的，此处的描述将该信号处理的描述与 RF 和 / 或无线电级 (radio stage) 分开，并在构思上将信号处理分配给模拟基带处理单元 510 和 / 或 DSP 502 或其他中央处理单元。在一些实施例中，RF 收发器 508、天线和前端 506 的部分以及模拟基带处理单元 510 可以被组合在一个或多个处理单元和 / 或特定用途集成电路 (ASIC) 中。

[0040] 模拟基带处理单元 510 可以提供对输入和输出的各种模拟处理，例如对来自麦克风 512 和耳机 516 的输入的模拟处理以及对向听筒 514 和耳机 516 的输出的模拟处理。为此，模拟基带处理单元 510 可以具有用于连接至内置麦克风 512 和听筒扬声器 514 的端口，使得 UE 14 能够用作蜂窝电话。模拟基带处理单元 510 还可以包括用于连接至耳机或其他免提麦克风和扬声器配置的端口。模拟基带处理单元 510 可以沿一个信号方向提供数模转换并沿相反的信号方向提供模数转换。在一些实施例中，模拟基带处理单元 510 的至少一些功能可以由数字处理组件来提供，例如由 DSP 502 或其他中央处理单元来提供。

[0041] DSP 502 可以执行调制 / 解调、编码 / 解码、交织 / 去交织、扩频 / 解扩、快速傅立叶逆变换 (IFFT) / 快速傅立叶变换 (FFT)、循环前缀附加 / 移除以及其他与无线通信相关联的信号处理功能。在实施例中，例如在码分多址 (CDMA) 技术应用中，针对发射器功能，DSP 502 可以执行调制、编码、交织和扩频，而针对接收器功能，DSP 502 可以执行解扩、去交织、解码和解调。在另一实施例中，例如在正交频分多址 (OFDMA) 技术应用中，针对发射器功能，DSP 502 可以执行调制、编码、交织、快速傅立叶逆变换和循环前缀附加，而针对接收器功能，DSP 502 可以执行循环前缀移除、快速傅立叶变换、去交织、解码和解调。在其他无线技术应用中，DSP 502 可以执行其他信号处理功能和信号处理功能的组合。

[0042] DSP 502 可以经由模拟基带处理单元 510 与无线网络进行通信。在一些实施例中，

该通信可以提供互联网连接性，使得用户能够访问互联网上的内容并能够发送和接收电子邮件或文本消息。输入 / 输出接口 518 与 DSP 502 以及各种存储器和接口互相连接。存储器 504 和可拆卸式存储卡 520 可以提供软件和数据以配置 DSP 502 的操作。在接口当中可以有 USB 接口 522 和短距离无线通信子系统 524。USB 接口 522 可以用于为 UE 14 充电，还可以使 UE 14 能够充当外围设备，以与个人计算机或其他计算机系统交换信息。短距离无线通信子系统 524 可以包括红外端口、蓝牙接口、遵循 IEEE 802.11 的无线接口、或可以使 UE 14 能够与其他附近移动设备和 / 或无线基站进行无线通信的任意其他短距离无线通信子系统。

[0043] 输入 / 输出接口 518 还可以将 DSP 502 连接至警报器 526，警报器 526 在被触发时使 UE 14 例如通过振铃、播放旋律或震动来向用户提供通知。警报器 526 可以充当一种机制，用于通过无声震动或针对特定呼叫者播放预先指定的具体旋律来向用户告警诸如如来电呼叫、新文本消息和约会提醒等不同事件中的任何事件。

[0044] 键区 528 经由接口 518 耦合至 DSP 502，以为用户提供一种进行选择、输入信息以及向 UE 14 提供输入的机制。键区 528 可以是全字母数字键盘或简化字母数字键盘（如 QWERTY、Dvorak、AZERTY 和顺序类型）或者与电话键区相关联的带有字母表字母的传统数字键区。输入键可以包括滚轮、退出或换码键、轨迹球和其他导航或功能键，其可以被向内按下以提供更多的输入功能。另一种输入机制可以是 LCD530，其可以包括触摸屏能力，也可以向用户显示文本和 / 或图形。LCD 控制器 532 将 DSP 502 耦合至 LCD 530。

[0045] 如果配备有 CCD 摄像机 534，则 CCD 摄像机 534 使 UE 14 能够拍摄数字图像。DSP 502 经由摄像机控制器 536 与 CCD 摄像机 534 进行通信。在另一实施例中，可以采用根据与电荷耦合器件摄像机不同的技术而操作的摄像机。GPS 传感器 538 耦合至 DSP 502，以对全球定位系统信号进行解码，从而使 UE 14 能够确定其位置。也可以包括多种其他外围设备以提供附加的功能，例如，无线电和电视接收。

[0046] 图 5 示出了可由 DSP 502 实现的软件环境 602。DSP 502 执行操作系统驱动器 604，操作系统驱动器 604 提供其余软件操作的平台。操作系统驱动器 604 向无线设备硬件的驱动器提供了可访问应用软件的标准化接口。操作系统驱动器 604 包括应用程序管理服务（“AMS”）606，该服务在运行于 UE 14 上的应用程序之间传送控制。图 5 还示出了网页浏览器应用程序 608、媒体播放器应用程序 610 和 Java 小应用程序 612。网页浏览器应用程序 608 将 UE 14 配置为充当网页浏览器，允许用户向表格中输入信息和选择链接以检索和观看网页。媒体播放器应用程序 610 将 UE 14 配置为检索和播放音频或视听媒体。Java 小应用程序 612 将 UE 14 配置为提供游戏、实用程序和其他功能。组件 614 可以提供与紧急呼叫相关的功能。

[0047] UE 14、P-CSCF 16、S-CSCF 18、E-CSCF 20 和 PSAP 22 以及此处描述的其他组件可以完全或部分地在通用计算机上实现或者可以包括该通用计算机，该通用计算机具有足够处理能力、存储资源和网络吞吐能力以处理置于该通用计算机上的必要工作量。图 6 示出了可适于实现此处描述的一个或多个实施例的典型通用计算机系统 700。计算机系统 700 包括处理器 720（可称为中央处理单元或 CPU），处理器 720 与包括辅助存储器 750、只读存储器 (ROM)740、随机存取存储器 (RAM)730、输入 / 输出 (I/O) 设备 710 和网络连接性设备 760 在内的存储设备进行通信。该处理器可以被实现为一个或多个 CPU 芯片。

[0048] 辅助存储器 750 典型地包括一个或多个盘驱动器或磁带驱动器，辅助存储器 750 用于数据的非易失性存储，并在 RAM 730 不足够大以容纳所有工作数据的情况下用作溢出数据存储设备。辅助存储器 750 可以用于存储当被选择以执行时被加载到 RAM 730 中的程序。ROM740 用于存储在程序执行期间读取的指令以及可能的数据。ROM 740 是非易失性存储设备，其典型地具有与辅助存储器的较大存储容量相比较小的存储容量。RAM 730 用于存储易失性数据以及可能存储指令。对 ROM 740 和 RAM 730 的访问典型地比对辅助存储器 750 的访问要快。

[0049] I/O 设备 710 可以包括打印机、视频监视器、液晶显示器 (LCD)、触屏显示器、键盘、键区、开关、拨号盘、鼠标、轨迹球、语音识别器、卡读取器、纸带读取器或其他公知输入设备。

[0050] 网络连接设备 760 可以采用以下形式：调制解调器、调制解调器组、以太网卡、通用串行总线 (USB) 接口卡、串行接口、令牌环卡、光纤分布式数据接口 (FDDI) 卡、无线局域网 (WLAN) 卡、无线电收发器卡（如，码分多址 (CDMA) 和 / 或全球移动通信系统 (GSM) 无线电收发器卡）以及其他公知网络设备。这些网络连接 760 设备可以使处理器 720 能够与互联网或者一个或多个内联网进行通信。利用这种网络连接，可以想到，处理器 720 在执行上述方法步骤的过程中可能从网络接收信息或可能向网络输出信息。常被示作要使用处理器 720 执行的一系列指令的这种信息是可以例如以在载波中体现的计算机数据信号的形式从网络接收和输出至网络的。

[0051] 可包括例如要使用处理器 720 执行的数据或指令在内的这种信息是可以例如以计算机数据基带信号或体现在载波中的信号的形式从网络接收和输出至网络的。由网络连接 760 设备产生的基带信号或体现在载波中的信号可以在电导体表面中或电导体表面上、在同轴电缆中、在波导中、在光学介质（例如光纤）中或者在空气或自由空间中进行传播。在基带信号或嵌入载波中的信号中所包含的信息可以是根据不同事件来排序的，如这对于处理或产生该信息或者发送或接收该信息而言可能是需要的）。基带信号或嵌入载波中的信号或者当前使用或今后开发的其他类型的信号（这里称为传输介质）可以是根据本领域技术人员若干方法来产生的。

[0052] 处理器 720 执行其从硬盘、软盘、光盘（基于这些各种盘的系统都可以被视为辅助存储器 750）、ROM 740、RAM 730 或网络连接设备 760 访问的指令、代码、计算机程序、脚本。尽管仅示出了一个处理器 720，但可以存在多个处理器。如被讨论为由处理器实现的指令或处理可以由一个或多个处理器同时、串行或以其他方式处理。

[0053] 尽管在本公开中已提供了多个实施例，但应当注意，在不脱离本公开的精神或范围的情况下，可以以许多其他具体形式来体现所公开的系统和方法。当前示例应被视为示意性的而非限制性的，并且并不意在限制此处给出的细节。例如，可以在另一系统中组合或结合各种元件或组件，或者可以省略或不实现特定特征。

[0054] 此外，在不脱离本公开的范围的情况下，在各个实施例中描述和示出为分离或单独的技术、系统、子系统和方法可以与其他系统、模块、技术或方法组合或结合。被示出或讨论为彼此耦合或直接耦合或进行通信的其他项目可以通过某种接口、设备或中间组件来（不论是电、机械还是以其他方式）间接耦合或进行通信。在不脱离此处公开的精神和范围的情况下，本领域技术人员可确定改变、替换和变更的其他示例。

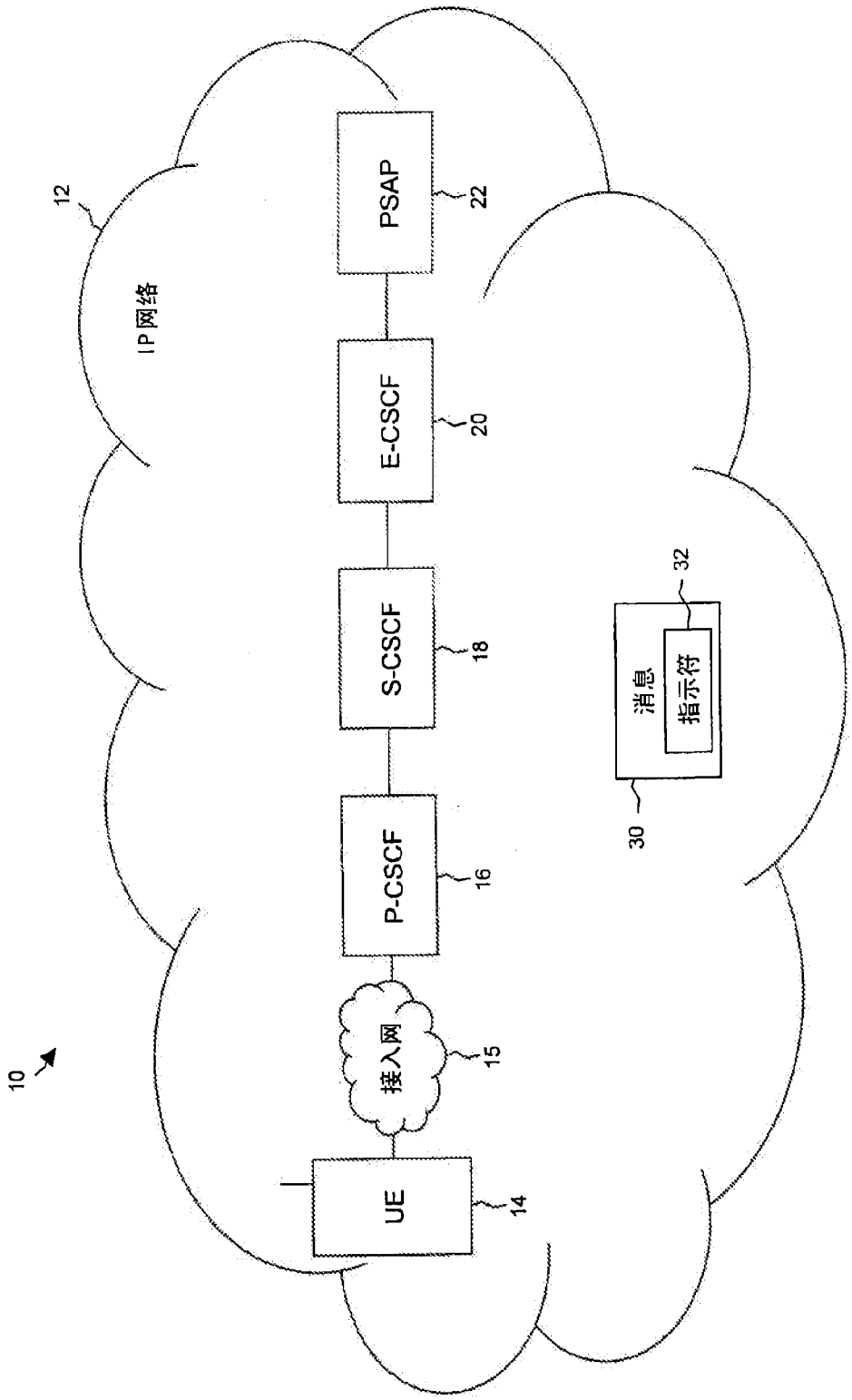


图 1

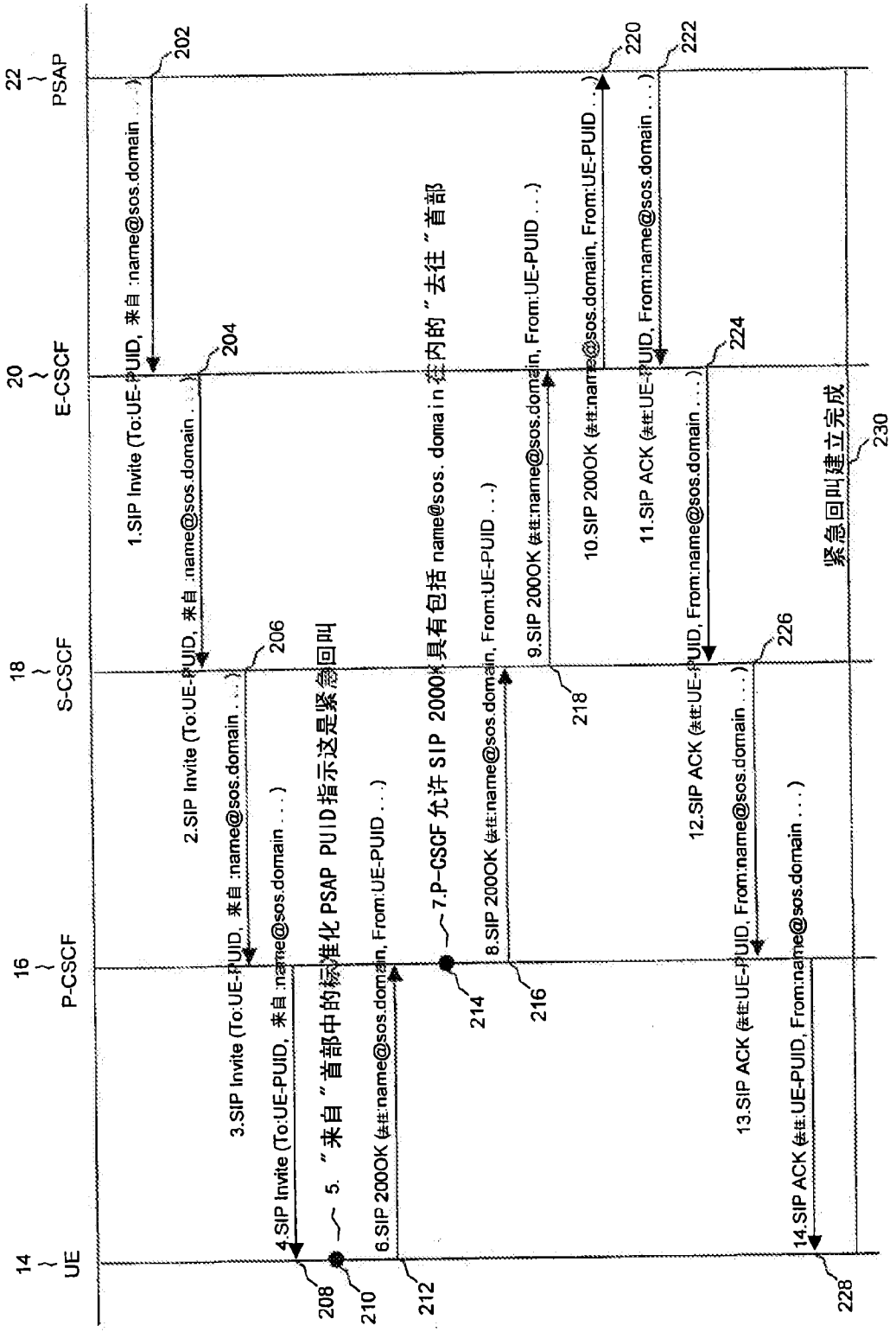


图 2

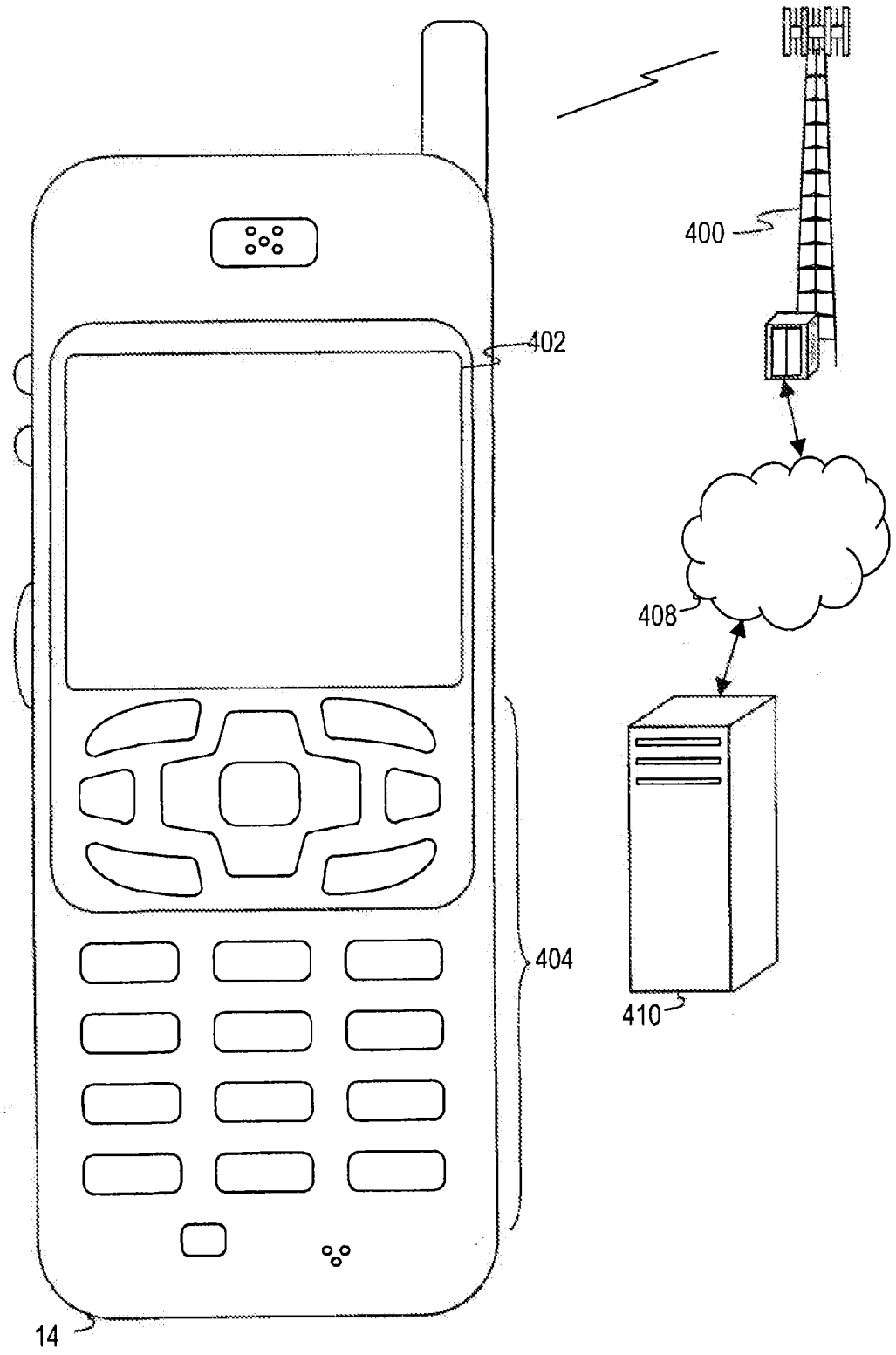


图 3

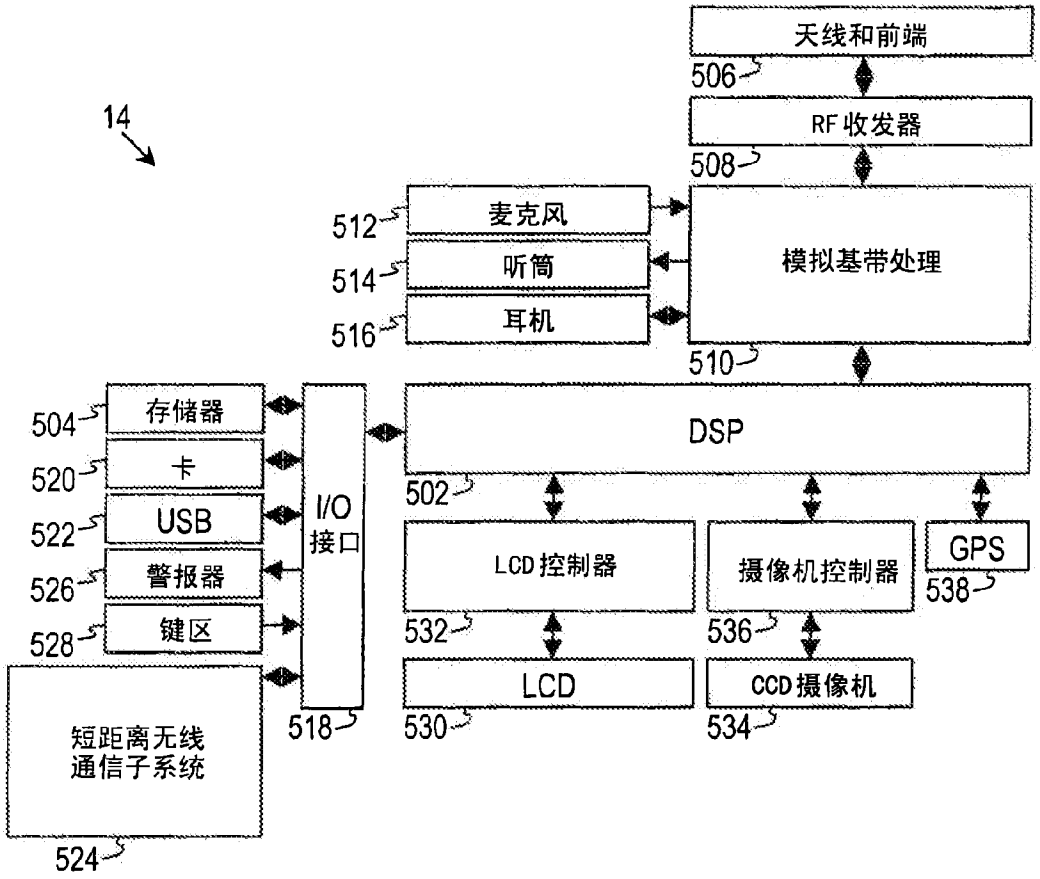


图 4

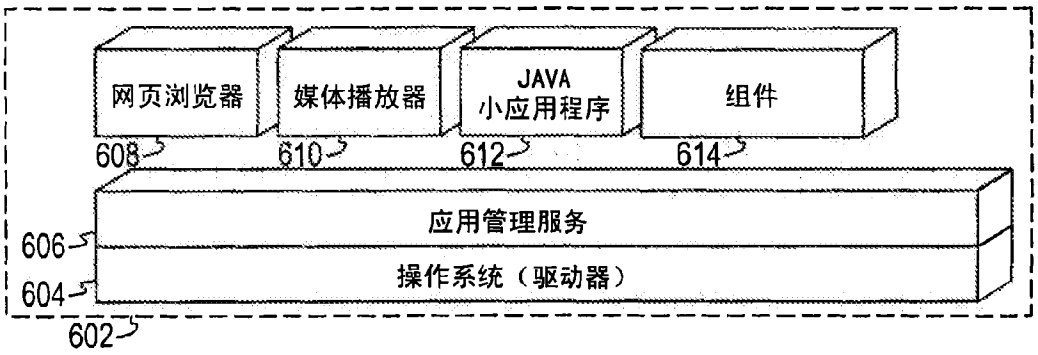


图 5

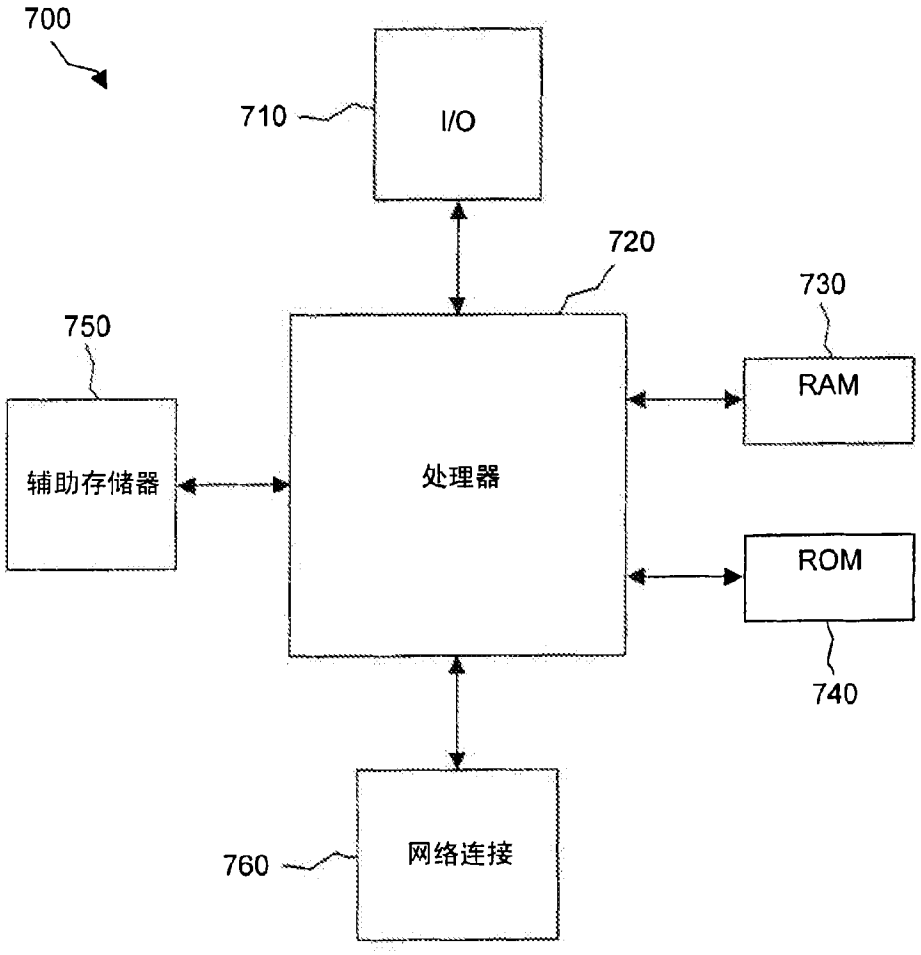


图 6

Espacenet

Bibliographic data: DE60201827 (T2) — 2005-11-10

Lawful interception for VoIP calls in IP based networks

Inventor(s): SHEN YUZHONG [DE]; GORGES THOMAS [DE] + (SHEN, YUZHONG, ; GORGES, THOMAS)

Applicant(s): ALCATEL SA [FR] + (ALCATEL, PARIS)

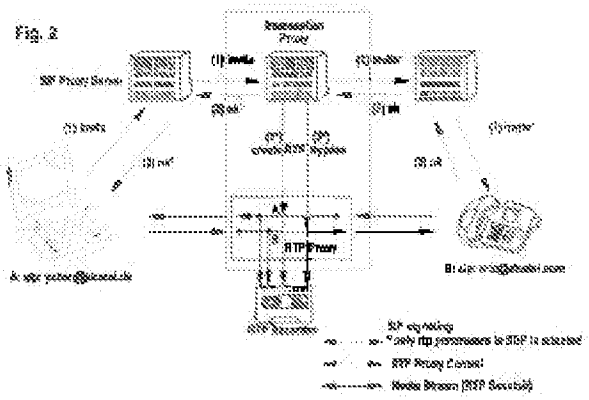
Classification: - international: ***H04L29/06; H04M3/22;*** *H04M3/42; H04M7/00;* (IPC1-7): H04L29/06; H04M7/00
- cooperative: **H04L29/06**; **H04L63/30**; **H04L65/1006**; **H04L65/1079**; **H04L65/608**; **H04M3/2281**; **H04W12/02**; H04L29/06027; H04M3/42221; H04M7/006

Application number: DE2002601827T 20020808

Priority number (s): EP20020360235 20020808

Also published as: EP1389862 (A1) EP1389862 (B1) US2004202295 (A1) ES2229073 (T3) AT281734 (T)

Abstract not available for DE60201827 (T2)
Abstract of corresponding document: EP1389862 (A1)



The lawful interception device to monitor media streams of two IP parties includes a SIP (Session Initiation Protocol) proxy server or a MGC (Media Gateway Controller) to detect information in the signalling information being transmitted between the two IP (Internet Protocol) parties and to generate instructions out of the detected signalling information for instructing a RTP (Real-time Transport Protocol) proxy server to create channels to bypass a media stream to be intercepted via an intermediate storage medium. Due to adaptation of connection parameters in the SDP part of the SIP messages sent to the IP parties the interception is transparent to the IP parties.

(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 602 01 827 T2** 2005.11.10

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 389 862 B1**
(21) Deutsches Aktenzeichen: **602 01 827.7**
(96) Europäisches Aktenzeichen: **02 360 235.2**
(96) Europäischer Anmeldetag: **08.08.2002**
(97) Erstveröffentlichung durch das EPA: **18.02.2004**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **03.11.2004**
(47) Veröffentlichungstag im Patentblatt: **10.11.2005**

(51) Int Cl.[7]: **H04L 29/06**
H04M 7/00

(73) Patentinhaber:
Alcatel, Paris, FR

(74) Vertreter:
Patentanwälte U. Knecht und Kollegen, 70435 Stuttgart

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, SK, TR

(72) Erfinder:
Shen, Yuzhong, 70499 Stuttgart, DE; Gorges, Thomas, 71638 Ludwigsburg, DE

(54) Bezeichnung: **Legales Abfangen für VOIP Anrufe in einem IP-Fernmeldenetz**

Beschreibung

TECHNISCHES GEBIET DER ERFINDUNG

[0001] Die Erfindung betrifft allgemein das Gebiet der Telekommunikationssysteme und insbesondere eine legale Abfangeinrichtung für Medienströme, insbesondere für VoIP-Gespräche in IP-basierten Netzen.

ALLGEMEINER STAND DER TECHNIK

[0002] Legales Abfangen wird derzeit in Vermittlungsstellen der Klasse 4/Klasse 5 von öffentlichen Fernsprechwählnetzen (PSTN)/öffentlichen Mobilkommunikationsnetzen (PLMN) eingesetzt. In 3G/UMTS-Netzen oder Netzen der nächsten Generation kann eine Verbindung von Ende zu Ende auf IP basieren. Kein Verkehr durchläuft Vermittlungsstellen der Klasse 5/Klasse 4. Dies bedeutet, dass derzeitige legale Abfanglösungen dort nicht eingesetzt werden können. Eine Lösung wäre, eine Auswertung von IP-Paketen in einem damit verbundenen Netzknoten vorzunehmen, doch es ist schwierig zu erkennen, welchen Weg ein Anruf (Medienstrom) durch das Netz nehmen wird.

[0003] Aus Thernelius F: „SIP, NAT, and Firewalls", Master's Thesis, Kungst Tekniska Hoegskolan, Department of Teleinformatics – Ericsson, Mai 2000 (2000-05), ist ein SIP-Zeichengabeverfahren für einen Medienstrom bekannt. Bei diesem Verfahren wird eine SIP-Einladungsnachricht eines ersten IP-Teilnehmers empfangen, mindestens ein Verbindungsparameter im SDP der empfangenen SIP-Einladungsnachricht angepasst, die angepasste SIP-Einladungsnachricht zu einem zweiten IP-Teilnehmer übertragen, vom zweiten IP-Teilnehmer eine SIP-Antwortnachricht empfangen, mindestens ein Verbindungsparameter im SDP der empfangenen SIP-Antwortnachricht angepasst und die angepasste SIP-Antwortnachricht zum ersten IP-Teilnehmer übertragen.

[0004] Aus WO 02 15627 A ist ein Verfahren für eine Modusauswahl-Prozedur bekannt. Ein Netzelement ist so ausgelegt, dass es eine Prozedur zur Auswahl desselben Modus für eine bidirektionale Kommunikation zwischen den Netzelementen durchführt. Die Modusauswahl gewährleistet, dass in Aufwärts- und Abwärtsrichtung ein und derselbe Modus verwendet wird und ermöglicht somit z. B. IP-Telefonie in UMTS unter Verwendung des SIP-Protokolls.

[0005] Aus EP-A-1 111 892 ist ein Verfahren zur Überwachung von IP-Netzen bekannt. Ein einer Endbenutzereinrichtung zugeordneter Authentifikationsserver stellt fest, ob die Endbenutzereinrichtung überwacht wird. Ist dies der Fall, informiert der Authentifikationsserver einen Proxy-Server, der Anrufsignalisierungsinformationen kopiert, daraus Medienstrom-Kennungs- und Dekodierinformationen entnimmt und diese an einen Kanten-Router weiterleitet, der den Medienstrom des Endbenutzers kopiert.

[0006] Aus WO 01 89145 A ist ein Verfahren zum Abhören von Gesprächen mit einem Mobilfunkgerät in einem IP-basierten Netz bekannt. Wenn das Mobilfunkgerät eine Zugangsanforderungsnachricht an den Gatekeeper sendet, fragt der Gatekeeper bei der Abhörstation an, ob das Mobilfunkgerät abgehört werden soll. Die Abhörstation antwortet dem Gatekeeper, dass das Mobilfunkgerät abgehört werden soll, und gibt eine IP-Adresse an, an welche die abhörten Pakete gesendet werden sollen. Dann sendet der Gatekeeper an den dem Mobilfunkendgerät zugeordneten Zugangsrouter eine Abhöranforderungsnachricht. Die Anforderung identifiziert das abzuhörende Mobilfunkgerät, weist den Zugangsrouter an, das Mobilfunkgerät abzuhören, und liefert eine eindeutige Rufkennung und die IP-Adresse, an welche die abgehörten Pakete zu senden sind. Erkennt der Zugangsrouter ein dem Mobilfunkgerät zugeordnetes Paket, dann überträgt er alle dem Mobilfunkgerät zugeordneten Pakete zur Abhörstation.

ZUSAMMENFASSUNG DER ERFINDUNG

[0007] Es ist Aufgabe der Erfindung, eine legale Abfangeinrichtung für VoIP-Gespräche in IP-basierten Netzen anzugeben.

[0008] Die erfindungsgemäße legale Abfangeinrichtung erfasst Informationen in den zwischen zwei IP-Teilnehmern übertragenen Zeichengabenachrichten und erzeugt aus den erfassten Zeichengabeinformationen Anweisungen an einen RTP(Real-time Transport Protocol)-Proxy-Server, Kanäle zur Umleitung eines abzufangenden VoIP-Anrufs über ein Zwischenspeichermedium vorzusehen. Anstelle von Sprache kann jeder andere Medienstrom abgefangen werden, wie z. B. Daten, Internetzugang, E-Mail, Videodaten, Echtzeitbilder usw.

[0009] In einem SIP(Session Initiation Protocol)-Abfang-Proxy-Server, in dem das Abfangen gesteuert werden soll, werden Anwendungen zur Auswahl von abzufangenden Anrufen ausgeführt. Soll ein Gespräch abgehört werden, benötigt der SIP-Proxy-Server zunächst die Einladungsnachricht vom A-Teilnehmer. Im SDP(Session Description Protocol)-Teil der Einladungsnachricht sind Abhörinformationen enthalten.

[0010] Über eine RTP-Proxy-Steuerschnittstelle weist der SIP-Proxy-Server dann einen RTP-Proxy-Server an, einen Umleitungskanal (bypass channel) zum Abhören eines Medienstroms zuzuteilen (A-Kanal: Senden an A-Teilnemer). Die RTP-Informationen dieses Umleitungskanals (Abhörteil: ip und port) sind im SDP-Teil der SIP-Einladungsnachricht enthalten und werden zum Ziel weitergeleitet.

[0011] Wenn der SIP-Proxy-Server eine Antwort des B-Teilnehmers erhalten hat, weist er den RTP-Proxy über die RTP-Proxy-Steuerschnittstelle an, einen weiteren Umleitungskanal zum Abhören des Medienstroms zuzuteilen (B-Kanal: Senden an B-Teilnehmer). Die RTP-Informationen dieses zweiten Umleitungskanals (Abhörteil: ip und port) sind im SDP-Teil der SIP-ok-Nachricht enthalten und werden zum Ursprung (A-Teilnehmer) gesandt.

[0012] Nach Einrichtung der Sitzung leiten beide Teilnehmer in Abhängigkeit von Verbindungsparametern in den empfangenen SIP-Nachrichten RTP-Verbindungen zum RTP-Proxy-Server ein. Doch diese sind für A und B transparent. A und B wissen nicht, dass sie mit einem RTP-Proxy verbunden sind.

[0013] Der RTP-Proxy kann mit der Aufzeichnung beider Medienkanäle (A und B) beginnen. Am Ende des Gesprächs wird vom RTP-Proxy z. B. eine Mediendatei mit zwei Tonspuren erstellt.

[0014] Vorteile:
- zentraler Netzknoten zum Abfangen von Medienströmen
- niedrige Einrichtungskosten
- transparent für Endbenutzer
- der RTP-Proxy kann in der oben beschriebnen Weise auch in einem Media-Gateway-Control(MEGACO, H.248)-basierten Netz oder einem H.323-Netz eingesetzt werden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0015] Zum besseren Verständnis der vorliegenden Erfindung wird auf die beigefügten Zeichnungen Bezug genommen. Es zeigen:

[0016] Fig. 1 ein vereinfachtes Blockdiagramm eines Teils eines als Beispiel dienenden Telekommunikationsnetzes nach der Lehre des Standes der Technik; und

[0017] Fig. 2 ein vereinfachtes Blockdiagramm eines Teils eines als Beispiel dienenden Telekommunikationsnetzes nach der Lehre der vorliegenden Erfindung.

AUSFÜHRLICHE BESCHREIBUNG DER ERFINDUNG

[0018] Fig. 1 zeigt einen Teil eines als Beispiel dienenden Telekommunikationsnetzes nach der Lehre des Standes der Technik.

[0019] Zwei IP-Teilnehmer, z. B. yshen@alcatel.de und eric@alcatel.com, sind über zwei Netze miteinander verbunden: ein SIP-Zeichengabenetz und ein Übertragungsnetz. Über das SIP-Zeichengabenetz wird die Zeichengabe durchgeführt, z. B. wird eine Verbindung zwischen den beiden IP-Teilnehmern aufgebaut. Über das Übertragungsnetz werden die zu übermittelnden Informationen, z. B. Sprache, Daten usw., in Form von Medienströmen übertragen (RTP-Sitzung).

[0020] Im SIP-basierten Netz ist jeder SIP-Proxy-Server für Zeichengabe und Sitzungsüberwachung zuständig. Der Medienstrom läuft von einem IP-Endpunkt zu einem anderen IP-Endpunkt. Ein zentraler Medienweg wie in einem PSTN-Netz ist nicht erforderlich. Ein legales Abfangen eines Medienstroms könnte nur in der Vermittlungsschicht erfolgen.

[0021] Das Aufzeichnen von Medienströmen durch Analyse des Netzverkehrs für legale Abfangzwecke ist sehr aufwendig, da sich der Weg der Pakete durch das IP-Netz ändern kann.

[0022] Deshalb könnte die Aufzeichnung nur sehr nahe bei den Endpunkten erfolgen. Außerdem müssen die aufgezeichneten Pakete wieder zusammengefügt werden. Eine Wiedergabe in Echtzeit ist schwierig.

[0023] Im Folgenden sind Definitionen und Hintergrundinformationen für SIP, Proxy-Server, RTP, SDP usw. aufgeführt.

SIP

[0024] Das Session Initiation Protocol (SIP) ist ein Anwendungsschicht-Steuerungs(Zeichengabe)-Protokoll zum Aufbau, Modifizieren und Beenden von Sitzungen mit einem oder mehr Teilnehmern. Zu diesen Sitzungen gehören Internet-Multimedia-Konferenzen, Internet-Fernsprechverbindungen und Multimedia-Verteilung. Sitzungsteilnehmer können über Multicasting oder ein Geflecht von Unicast-Beziehungen oder eine Kombination davon miteinander kommunizieren.

[0025] SIP-Einladungen für die Einrichtung von Sitzungen enthalten Sitzungsbeschreibungen, die es Teilnehmern ermöglichen, einen Satz kompatibler Medientypen zu vereinbaren. SIP unterstützt die Benutzermobilität, indem es Anforderungen zum jeweiligen Standort des Benutzers umleitet. Benutzer können ihren jeweiligen Standort registrieren lassen. SIP ist an kein bestimmtes Konferenz-Steuerungsprotokoll gebunden. SIP ist unabhängig vom Transportprotokoll einer niedrigeren Schicht und kann mit zusätzlichen Fähigkeiten erweitert werden.

[0026] Das Session Initiation Protokoll (SIP) ist ein Anwendungsschicht-Steuerungsprotokoll, das Multimedia-Sitzungen oder -Verbindungen aufbauen, modifizieren und beenden kann. Zu diesen Multimedia-Sitzungen gehören Multimedia-Konferenzen, Fernlernen (distance learning), Internet-Telefonie und ähnliche Anwendungen. SIP kann sowohl Personen als auch „Roboter", wie z. B. einen Medienspeicherdienst, einladen. SIP kann Teilnehmer sowohl zu Unicast- als auch zu Multicast-Sitzungen einladen; der Initiator muss nicht unbedingt ein Teilnehmer der Sitzung sein, zu der er einlädt. Medien und Teilnehmer können einer bestehenden Sitzung hinzugefügt werden.

[0027] SIP kann benutzt werden, um Sitzungen zu initiieren und um Teilnehmer zu Sitzungen einzuladen, die mit anderen Mitteln angekündigt und eingerichtet wurden. Sitzungen können unter Verwendung von Multicast-Protokollen, wie z. B. elektronische Post, Newsgroups, Web-Seiten oder Verzeichnisse (LDAP), angekündigt werden.

[0028] SIP unterstützt transparent Namensabbildungs- und Umleitungsdienste und ermöglicht die Implementierung von ISDN- und IN-Telefonie-Teilnemerdiensten. Diese Leistungsmerkmale ermöglichen auch eine personenbezogene Mobilität. In der Sprache der Dienste des intelligenten Netzes ist personenbezogene Mobilität definiert als „die Fähigkeit von Endbenutzern, an jedem Endgerät an jedem Standort Anrufe abzusetzen und zu empfangen und auf abonnierte Telekommunikationsdienste zuzugreifen, und die Fähigkeit des Netzes, Endbenutzer bei Veränderung ihres Standortes zu identifizieren. Personenbezogene Mobilität basiert auf der Verwendung einer eindeutigen persönlichen Identität (d. h., einer persönlichen Nummer)". Die personenbezogene Mobilität ergänzt die gerätebezogne Mobilität, d. h., die Fähigkeit, die Kommunikation aufrechtzuerhalten, wenn ein „Single-End"-System von einem Unternetz in ein anderes wandert.

[0029] SIP unterstützt fünf Aspekte des Aufbaus und Beendens von Multimedia-Kommunikationsverbindungen:
Benutzerstandort: Bestimmung des für die Kommunikation zu verwendenden Endsystems;
Benutzerfähigkeiten: Bestimmung der zu verwendenden Medien und Medienparameter;
Benutzerverfügbarkeit: Bestimmung der Bereitschaft des gerufenen Teilnehmers, sich an einer Kommunikation zu beteiligen;
Verbindungsaufbau; „Rufen", Bestimmung von Verbindungsparametern sowohl beim gerufenen als auch beim rufenden Teilnehmer;
Verbindungsabwicklung: einschließlich Umlegen und Auslösen von Verbindungen.

[0030] Unter Verwendung einer Mehrpunkt-Steuerungseinheit (Multipoint Control Unit – MCU) oder einer voll vermaschten Verbindung anstelle von Multicasting kann SIP auch Sammelrufe initiieren. Internet-Telefonie-Gateways, die Teilnehmer des öffentlichen Fernsprechwählnetzes (Public Switched Telephone Network – PSTN) miteinander verbinden, können SIP zum Verbindungsaufbau verwenden.

[0031] SIP ist als Teil der IETF-Multimedia-Daten- und Steuerungsarchitektur vorgesehen, die derzeit Proto-

kolle wie z. B. das Real-time Transport Protocol (RTP) für den Transport von Echtzeitdaten und für die Bereitstellung von QoS-Feedback enthält.

[0032] Eine Anforderung und eine Antwort bilden zusammen eine Transaktion. SIP verwendet z. B. Einladungs- und Quittungsnachrichten, um Verbindungen aufzubauen. Weitere verwendete Nachrichten sind z. B. ok, bye, options, register, cancel. SIP-Teilnehmer werden über einen SIP-ULR identifiziert, z. B. sip:clientname@hostaddress. Jeder Client kann Anforderungen an einen Proxy-Server oder direkt an eine IP-Adresse senden.

[0033] Der Aufbau einer Verbindung erfolgt in drei Schritten: Senden einer Einladungsnachricht (Anforderungsnachricht) von einem ersten IP-Teilnehmer zu einem zweiten IP-Teilnehmer, Senden einer ok(Antwort)-Nachricht vom zweiten IP-Teilnehmer zum ersten IP-Teilnehmer, Senden einer Quittungs(Antwort)-Nachricht vom ersten IP-Teilnehmer zum zweiten IP-Teilnehmer. Die Einladungsnachricht enthält so viele Informationen, dass der zweite IP-Teilnehmer beurteilen kann, ob eine Verbindung gewünscht wird oder nicht. Die Quittungsnachricht ist eine Bestätigung, die dazu dient, die Sicherheit der Verbindung zu erhöhen. SIP ist somit unabhängig von TCP oder UDP.

[0034] Das erfindungsgemäße SIP ist das derzeit genormte SIP sowie Modifikationen davon und Äquivalente dafür.

RTP

[0035] Die Audio/Video Transport Working Group der IETF wurde gebildet, um ein Protokoll für die Echtzeitübertragung von Audio- und Videoinformationen über UDP und IP-Multicast zu spezifizieren. Dies ist das Real-time Transport Protocol, RTP, mit dem dazugehörigen Profil für Audio/Video-Konferenzen und Nutzlastformatdokumente. Zu den derzeit diskutierten Nutzlastformaten gehören eine Anzahl von medienspezifischen Formaten (MPEG-4, DTMF, PureVoice) und auf viele Formate anwendbare FEC-Verfahren (Paritäts-FEC, Reed-Solomon-Codierung). RTP wird als Ersatz für eine übliche leitungsvermittelte Verbindung zwischen zwei Knoten verwendet.

[0036] Das Real-time Transport Protocol (RTP) ist ein Nutzlastformat, das z. B. für nach dem Adaptive-Multi-Rate(AMR)- oder Adaptive-Multi-Rate-Wideband(RMR-WB)-Verfahren codierte Sprachsignale verwendet werden soll. RTP stellt Ende-zu-Ende-Transportfunktionen bereit, die für Anwendungen geeignet sind, welche Echtzeitdaten, wie z. B. Audio-, Video- oder Simulationsdaten, über Multicast- oder Unicast-Netzdienste übertragen. RTP regelt nicht die Ressourcen-Reservierung und gewährleistet nicht die Betriebsgüte für Echtzeitdienste. Der Datentransport wird z. B. durch das RTCP (Real-time Transport Control Protocol) verbessert, um eine Überwachung der Datenübermittlung auf eine für große Multicast-Netze skalierbare Weise zu ermöglichen und eine Mindest-Steuerungs- und Identifizierungsfunktionalität zu gewährleisten. RTP und RTCP sind so ausgelegt, dass sie von den darunter liegenden Transport- und Vermittlungsschichten unabhängig sind. Das Protokoll unterstützt die Verwendung von Umsetzern und Mischern auf RTP-Ebene. Die Daten werden durch RTP in Paketform, zum Beispiel als Audio-Abtastwerte oder komprimierte Videodaten, transportiert. Ein Datenpaket enthält z. B. den festen RTP-Header (Kopfteil), eine möglicherweise leere List von beisteuernden Quellen und die Nutzdaten.

[0037] Das erfindungsgemäße RTP ist das derzeit diskutierte RTP sowie Modifikationen davon und Äquivalente dafür. RTP kann ein Protokoll sowohl für Audio- als auch Videosignale oder nur für Audiosignale oder Videosignale oder für Audio-, Video- und Datensignale oder für Audiosignale und Daten usw. sein. Eine Modifikation von RTP ist z. B. RTP/I, ein Echtzeitprotokoll auf Anwendungsebene für verteilte interaktive Medien. Typische Beispiele für verteilte interaktive Medien sind gemeinsam genutzte Whiteboards, vernetzte Computerspiele und verteilte virtuelle Umgebungen. RTP/I definiert eine genormte Rahmung für die Übertragung von Daten und stellt Mechanismen bereit, die für diese Medienklasse generell benötigt werden. Dadurch ermöglicht RTP/I die Entwicklung einer wiederverwendbaren Funktionalität und von generischen Diensten, die für mannigfaltige verteilte interaktive Medien verwendet werden können. Beispiele für diese Art von Funktionalität sind die Fähigkeit, Sitzungen aufzuzeichnen, verspätete Teilnehmer zu unterstützen und Sicherheitsdienste bereitzustellen. RTP/I ist ein Protokoll, das sich an die Rahmung auf Anwendungsebene (application level framing) und die integrierte Schichtverarbeitung (integrated layer processing) anlehnt. Es ist so ausgelegt, dass es von den darunter liegenden Vermittlungs- und Transportschichten unabhängig ist. Somit ist RTP/I ein modifiziertes RTP-Protokoll, das viele Aspekte von RTP verwendet, jedoch vollkommen an die speziellen Bedürfnisse von verteilten interaktiven Medien angepasst ist.

Proxy, Proxy-Server

[0038] Ein intermediäres Programm, das sowohl als Server als auch als Client zur Abgabe von Anforderungen für andere Clienten dient. Anforderungen werden intern oder durch Weitergabe, gegebenenfalls nach Umsetzung, an andere Server abgearbeitet. Ein Proxy wertet eine Anforderungsnachricht aus und schreibt sie nötigenfalls neu, bevor er sie weiterleitet.

Server

[0039] Ein Server ist ein Anwendungsprogramm, das Anforderungen zur Abarbeitung annimmt und Antworten auf diese Anforderungen zurücksendet. Servers sind entweder Proxy-, Umleitungs- oder User-Agent-Server oder Registratoren.

User Agent Client(UAC), Calling User Agent

[0040] Ein User Agent Client ist eine Client-Anwendung, welche die SIP-Anforderung initiiert.

SDP

[0041] Das Session Description Protocol (SDP) ist für die Beschreibung von Multimedia-Sitzungen zwecks Sitzungsankündigung, Einladung zu Sitzungen und anderer Formen der Multmedia-Sitzungs-Initiierung vorgesehen.

[0042] Der Zweck des SDP ist, Informationen über Medienströme in Multimedia-Sitzungen zu übermitteln, um es den Empfängern einer Sitzungsbeschreibung zu ermöglichen, an der Sitzung teilzunehmen. SDP ist in erster Linie zur Verwendung in einem Verbundnetzwerk vorgesehen, wenngleich es ausreichend allgemein ist, um Konferenzen in anderen Netzumgebungen beschreiben zu können.

[0043] Eine Multimedia-Sitzung ist für diese Zwecke definiert als eine Menge von Medienströmen, die für eine gewisse Zeitdauer existieren. Medienströme können „viele-zu-vielen" sein. Die Zeiten, während derer die Sitzung aktiv ist, müssen nicht kontinuierlich sein.

[0044] Bisher unterschieden sich multicastbasierte Sitzungen im Internet von vielen anderen Konferenzformen dadurch, dass jeder, der den Verkehr empfängt, sich der Sitzung anschließen kann (es sei denn, der Sitzungsverkehr ist verschlüsselt). In einer solchen Umgebung dient SDP zwei Hauptzwecken. Es ist ein Mittel, um die Existenz einer Sitzung mitzuteilen, und ein Mittel zur Übermittlung von genügend Informationen, um eine Teilnahme an der Sitzung zu ermöglichen. In einer Unicast-Umgebung ist wahrscheinlich nur der letztere Zweck relevant.

[0045] SDP enthält also:
- Sitzungsname und -zweck
- Zeit(en), in der (denen) die Sitzung aktiv ist
- die die Sitzung umfassenden Medien
- Informationen zum Empfang dieser Medien (Adressen, Ports, Formate und so weiter)

[0046] Da die zur Teilnahme an einer Sitzung erforderlichen Ressourcen begrenzt sein können, können einige weitere Informationen wünschenswert sein:
- Informationen über die von der Konferenz zu verwendende Bandbreite
- Informationen für die Kontaktierung der für die Sitzung zuständigen Person

[0047] Im Allgemeinen muss SDP genügend Informationen vermitteln, um es zu ermöglichen, sich einer Sitzung anzuschließen (gegebenenfalls mit Ausnahme von Verschlüsselungscodes) und die Ressourcen bekannt zu geben, die von Nichtteilnehmern zu verwenden sind, bei denen möglicherweise ein Bedürfnis besteht, informiert zu werden.

[0048] SDP enthält:
- den Medientyp (Video, Audio usw.)
- das Transportprotokoll (RTP/UDP/IP, H.320 usw.)
- das Medienformat (H.261 Video, MPEG Video usw.)

[0049] Für eine IP-Muilticast-Sitzung wird auch Folgendes übermittelt:
- Multicast-Adresse für Medien
- Transport-Port für Medien

[0050] Diese Adresse und dieser Port sind die Zieladresse und der Zielport des Multicast-Stroms, ob gesendet, empfangen oder beides.

[0051] Für eine IP-Unicast-Sitzung wird Folgendes übermittelt:
- entfernte Adresse für Medien
- Transport-Port für Kontaktadresse

[0052] Die Semantik dieser Adresse und dieses Ports ist abhängig von den Medien und dem definierten Transportprotokoll. Standardmäßig sind dies die entfernte Adresse und der entfernte Port, an den Daten gesendet werden, und die entfernte Adresse und der lokale Port, an dem Daten empfangen werden sollen. Für einige Medien kann jedoch definiert sein, dass diese Semantik zur Einrichtung eines Steuerkanals für den eigentlichen Medienfluss verwendet wird.

[0053] Das erfindungsgemäße SDP ist das derzeit genormte SDP sowie Modifikationen davon und Äquivalente dafür.

[0054] Fig. 2 zeigt einen Teil eines als Beispiel dienenden Telekommunikationsnetzes nach der Lehre der vorliegenden Erfindung.

[0055] Wie in Fig. 1 sind zwei IP-Teilnehmer, z. B. yshen@alcatel.de und eric@alcatel.com, über zwei Netze miteinander verbunden: ein SIP-Zeichengabenetz und ein Übertragungsnetz. Über das SIP-Zeichengabenetz wird die Zeichengabe durchgeführt, z. B. wird eine Verbindung zwischen den beiden IP-Teilnehmern aufgebaut. Über das Übertragungsnetz werden die zu übermittelnden Informationen, z. B. Sprache, Daten usw., in Form von Medienströmen übertragen (RTP-Sitzung).

[0056] Im Unterschied zu Fig. 1 ist in Fig. 2 eine legale Abfangeinrichtung vorgesehen. Die legale Abfangeinrichtung ist z. B. ein Prozessor mit spezieller Software. Der Prozessor ist z. B. ein digitaler Signalprozessor, ein Steuergerät, ein Mikroprozessor oder dergleichen. Statt eines Prozessors können zwei oder mehr Prozessoren verwendet werden. Zwei oder mehr Prozessoren können sich an verschiedenen Orten befinden. Ein Prozessor könnte zur Durchführung von SIP-Proxy-Server-Operationen und ein anderer zur Durchführung von RTP-Proxy-Server-Operationen benutzt werden. Im Allgemeinen können ein, zwei oder mehr Hardwareeinheiten zur Ausführung von einem, zwei oder mehr Softwareprogrammen verwendet werden. Jedes Softwareprogramm kann zusätzlich teilweise auf unterschiedlichen Hardwareeinheiten ausgeführt werden.

[0057] Die legale Abfangeinrichtung enthält einen SIP(Session Initiation Protocol)-Proxy-Server oder einen MGC (Media Gateway Controller) zur Erfassung von Informationen in der zwischen zwei IP(Internet Protocol)-Teilnehmern übertragenen Zeichengabenachricht und zur Erzeugung von Anweisungen aus der erfassten Zeichengabeinformation an einen RTP(Real-time Transport Protocol)-Proxy-Server, Kanäle für die Umleitung eines abzufangenden Medienstroms über ein Zwischenspeichermedium einzurichten. Medienströme sind z. B. VoIP, Daten, Internetzugang, E-Mail, Video, Echtzeitbilder, Musik, Videoclips, Videospiele usw. Das Speichermedium kann eine Compact Disk, ein Magnetspeichermedium, ein Lesezugriffsspeicher oder dergleichen sein.

[0058] Das Verfahren zur SIP-Zeichengabe für einen Medienstrom umfasst folgende Schritte:
Empfangen einer SIP-Einladungsnachricht eines ersten IP-Teilnehmers;
Anpassen mindestens einen Verbindungsparameters im SDP (Session Description Protocol) der empfangenen SIP-Einladungsnachricht;
Übertragen der angepassten SIP-Einladungsnachricht zu einem zweiten IP-Teilnehmer;
Empfangen einer SIP-Antwortnachricht des zweiten IP-Teilnehmers;
Anpassen mindestens eines Verbindungsparameters im SDP (Session Description Protocol) der empfangenen SIP-Antwortnachricht;
Übertragen der angepassten SIP-Antwortnachricht zum ersten IP-Teilnehmer.

[0059] Mindestens ein RTP-Parameter enthält Angaben über einen Umleitungskanal, eine Adresse oder einen Port. Die an beide IP-Teilnehmer gesandten RTP-Parameter unterscheiden sich voneinander.

[0060] Nach Empfang der SIP-Einladungsnachricht des ersten IP-Teilnehmers sendet der SIP-Abfang-Pro-

xy-Server eine Aufforderung an den RTP-Abfang-Proxy-Server, mindestens zwei Kanäle für eine bidirektionale Kommunikation zuzuteilen. Die für die Kommunikation zwischen SIP-Abfang-Proxy-Server und RTP-Abfang-Proxy-Server verwendete Schnittstelle ist eine XML-basierte API. Die Anzahl der zuzuteilenden Kanäle kann abhängig von der Menge der zu übertragenden Daten, der angeforderten Bandbreite, der angeforderten Dienstgüte, der Art der zu übertragenden Informationen, wie z. B. Sprache, Sprache und Daten, Sprache und Video, usw. variieren. Mindestens einer der zugeteilten Kanäle dient zur Übertragung von Informationen zwischen dem RTP-Abfang-Proxy-Server und dem Endgerät des ersten IP-Teilnehmers. Das Endgerät kann ein Telefon, ein Laptop, ein Personal Computer, ein Screenphone, ein Mobiltelefon usw. sein. Mindestens ein anderer der zugeteilten Kanäle dient zur Übertragung von Informationen zwischen dem RTP-Abfang-Proxy-Server und dem Endgerät des zweiten IP-Teilnehmers.

[0061] Angenommen, Kanal A im RTP-Abfang-Proxy-Server ist für die Übertragung von Informationen zwischen dem zweiten IP-Endgerät und dem Endgerät des ersten IP-Teilnehmers, und Kanal B für die Übertragung von Informationen zwischen dem Endgerät des ersten IP-Teilnehmers und dem zweiten IP-Endgerät zugeteilt. Dann sendet der RTP-Abfang-Proxy-Server Informationen über die Zuteilung der Kanäle A und B and den SIP-Abfang-Proxy-Server. Der SIP-Abfang-Proxy-Server fügt eine Information über Kanal A in die an den zweiten IP-Teilnehmer zu sendende Einladungsnachricht ein. Die Information über Kanal A wird vorteilhafterweise in die Verbindungsparameter-Informationen eingefügt, die im SDP der SIP-Einladungsnachricht enthalten sind.

[0062] Nach Empfang der SIP-Antwortnachricht des zweiten IP-Teilnehmers, die einer ok-Nachricht entspricht, welche besagt, dass eine Verbindung zum ersten IP-Teilnehmer gewünscht wird, ersetzt der SIP-Abfang-Proxy-Server den im SDP-Teil der ok-Nachricht enthaltenen Verbindungsparameter durch die Information über Kanal B. Die modifizierte, die Information über Kanal B einschließende ok-Nachricht wird zum ersten IP-Teilnehmer übertragen.

[0063] Somit sendet der erste IP-Teilnehmer Daten an Kanal B und empfängt Daten über Kanal A des RTP-Abfang-Proxy-Servers. Der zweite IP-Teilnehmer sendet Daten an Kanal A und empfängt Daten über Kanal B des RTP-Abfang-Proxy-Servers. Innerhalb der legalen Abfangeinrichtung ist das Zwischenspeichermedium sowohl mit Kanal A als auch mit Kanal B verbunden. Somit durchläuft der Informationsfluss zwischen den beiden IP-Teilnehmern das Zwischenspeichermedium, wodurch Abfangen ermöglicht wird. Der erste Teilnehmer weiß nicht, auf welchem Kanal der zweite Teilnehmer sendet, und der zweite Teilnehmer weiß nicht, auf welchem Kanal der erste Teilnehmer sendet. Damit ist das Abfangen für beide IP-Teilnehmer transparent.

[0064] Ein Computerprogramm zur Durchführung mindestens eines Teils der Schritte des erfindungsgemäßen Verfahrens kann als Erweiterungssoftware dienen, die z. B. an Dienstanbieter verkauft wird, welche dann einen oder mehr herkömmliche Proxy-Server zu einem oder mehr Servern mit der Funktionalität eines SIP-Abfang-Proxy-Servers erweitern. Das Computerprogramm enthält mindestens folgende Schritte:
Anpassen mindestens eines Verbindungsparameters im SDP (Session Description Protocol) der empfangenen SIP-Einladungsnachricht;
Anpassen mindestens eines Verbindungsparameters im SDP (Session Description Protocol) der empfangenen SIP-Antwortnachricht.

[0065] Das Computerprogramm kann auch so gestaltet sein, dass es alle Schritte des oben beschriebenen Verfahrens ausführt.

[0066] Innerhalb eines IP-Netzes können ein, zwei oder mehr SIP-Proxy-Server, ein, zwei oder mehr SIP-Abfang-Proxy-Server, ein, zwei oder mehr RTP-Proxy-Server und ein, zwei oder mehr RTP-Abfang-Proxy-Server verwendet werden.

[0067] Das IP-Netz kann ein Leitungsnetz, ein Funknetz oder eine Kombination dieser beiden Netzarten sein.

Liste der Abkürzungen

3G	Third Generation (dritte Generation)
API	Application Programming Interface (Anwendungsprogramm-Schnittstelle)
AMR	Adaptive Multi-Rate
AMR-WB	AMR-Wideband
DTMF	Dual-Tone Multi-Frequency (Mehrfrequenzwahlverfahren)
FEC	Forward Error Correction (Vorwärtsfehlerkorrektur)
H248	ITU Standard
H261	ITU Standard
H320	ITU Standard
H323	ITU Standard
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network (diensteintegrierendes digitales Fernmeldenetz)
LDAP	Lightweight Directory Access Protocol
MEGACO	Media Gateway Controller (Medien-Gateway-Steuerung)
MPEG	Motion Picture Expert Group
MGC	Media Gateway Controller (Medien-Gateway-Steuerung)
NGN	Next Generation Network (Netz der nächsten Generation)
PSTN	Public Switched Telephone Network (öffentliches Fernsprechwählnetz)
QoS	Quality of Service (Dienstgüte)
RTCP	Real-time Transport Control Protocol (Echtzeit-Sendesteuerungsprotokoll)
RTP	Real-time Transport Protocol (Echtzeit-Transportprotokoll)
SDP	Session Description Protocol (Sitzungsbeschreibungsprotokoll)
SIP	Session Initiation Protocol (Sitzungsinitiierungsprotokoll)
TCP	Transmission Control Protocol (Übertragungssteuerungsprotokoll)
UAC	User Agent Client
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP (Sprache über IP)
XML	eXtensible Markup Language (erweiterbare Auszeichnungssprache)

Patentansprüche

1. Legale Abfangeinrichtung mit einem Session-Initiation-Protocol-Proxy-Server oder einer Medien-Gateway-Steuerung, der bzw. die geeignet ist, Informationen in der zwischen zwei Internet-Protokoll-Teilnehmern übertragenen Zeichengabenachricht zu erfassen, und **dadurch gekennzeichnet** ist, dass er bzw. sie geeignet ist, aus der erfassten Zeichengabeinformation Anweisungen für einen Echtzeit-Transportprotokoll-Proxy-Server zu erzeugen, Kanäle für die Umleitung eines abzufangenden Medienstroms über ein Zwischenspeichermedium einzurichten.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

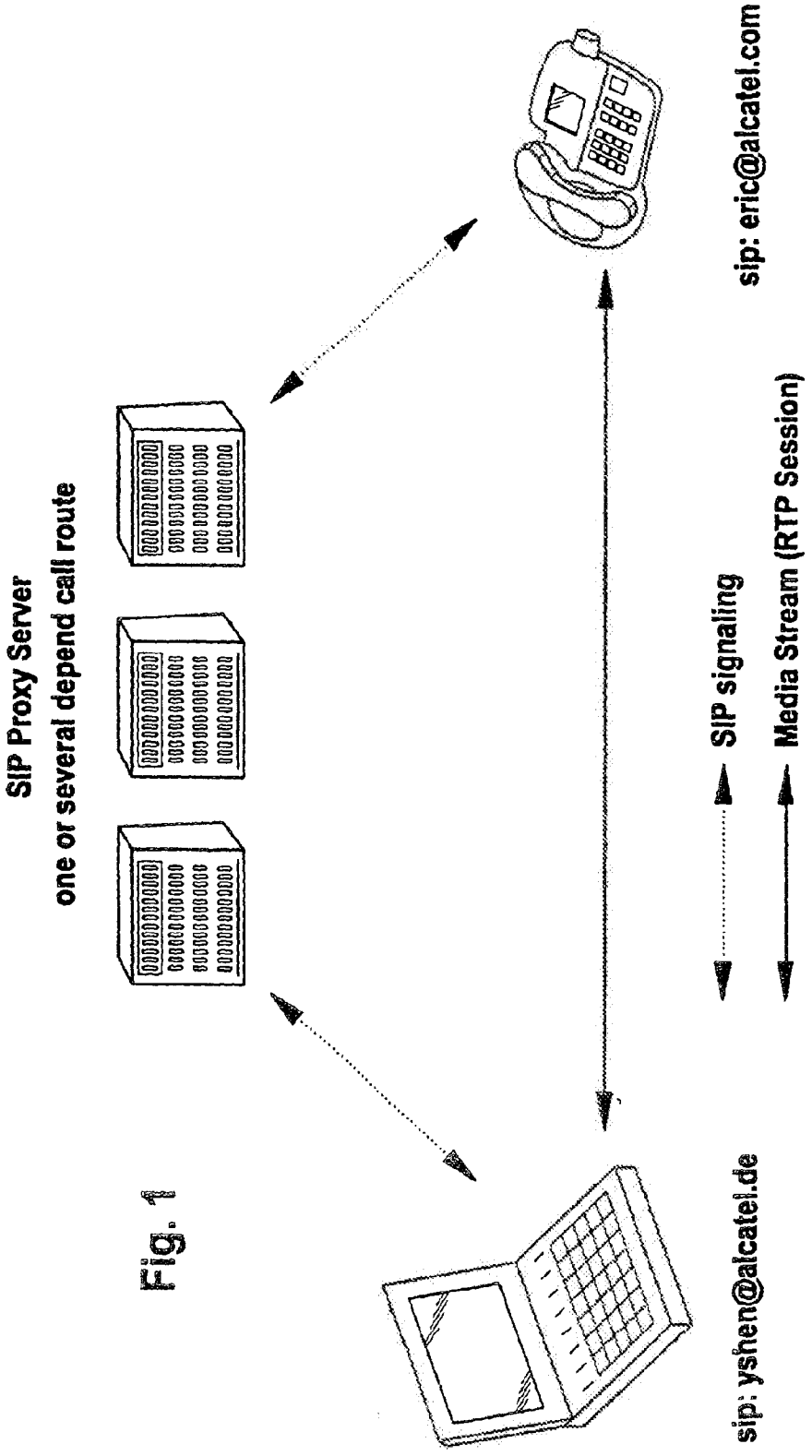


Fig. 1

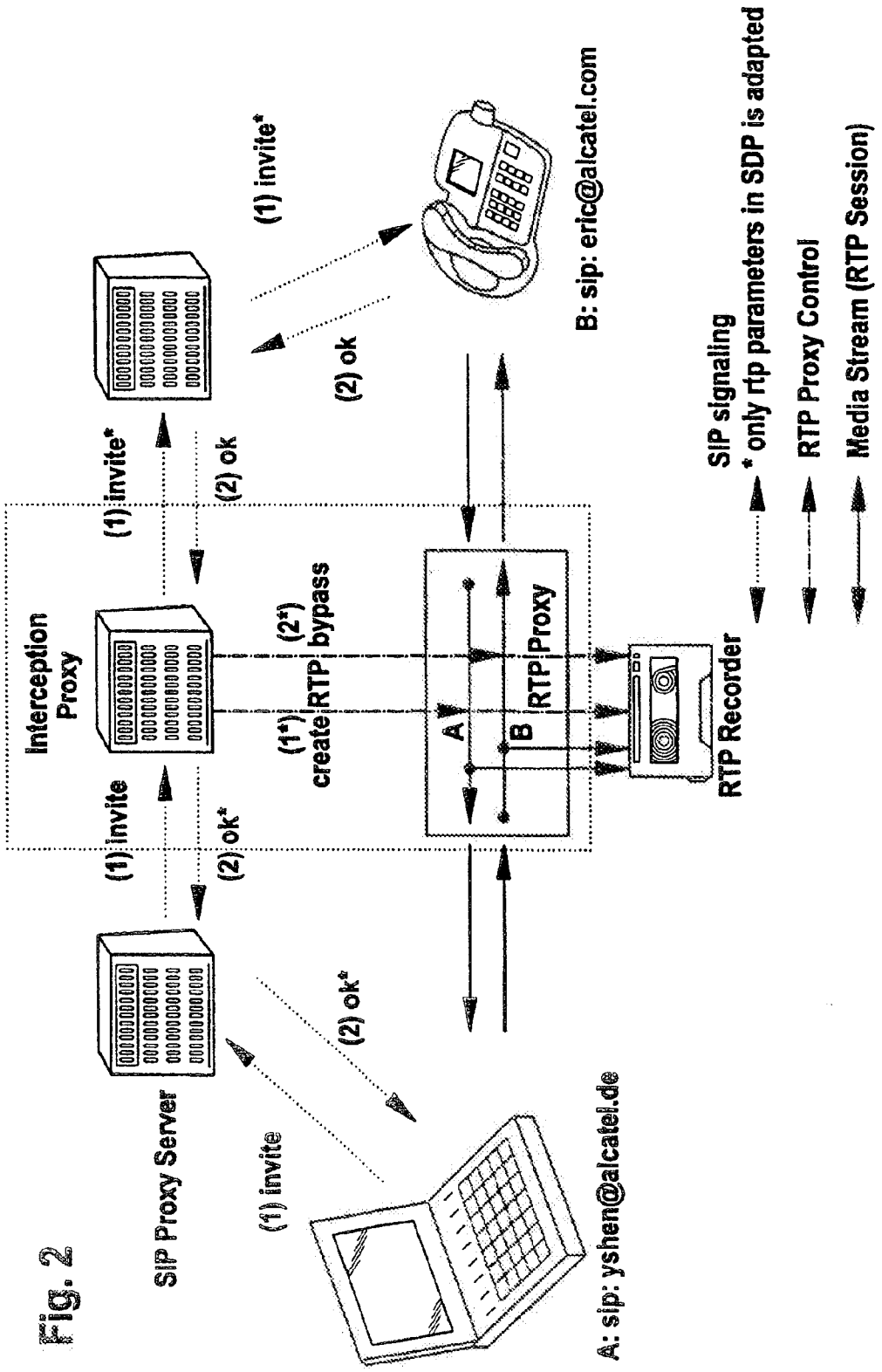


Fig. 2

Espacenet

Bibliographic data: DE112005003306 (T5) — 2008-01-24

DISTRIBUTED VOICE NETWORK

Inventor(s): LEBIZAY GERALD [US] + (LEBIZAY, GERALD)

Applicant(s): INTEL CORP [US] + (INTEL CORPORATION)

Classification: **- international:*H04L29/06***
- cooperative: G06Q20/102; H04L29/06027; H04L65/103; H04L65/104; H04L65/1043; H04L65/607

Application number: DE20051103306T 20051229

Priority number(s): US20040027915 20041230 ; WO2005US47679 20051229

Also published as: WO2006072099 (A1) US2012250624 (A1) US8605714 (B2) US2010008345 (A1) US8204044 (B2) US2006146797 (A1) US7593390 (B2) TWI307592 (B) GB2437666 (A) GB2437666 (B) CN102833232 (A) CN101095329 (A) CN101095329 (B) less

Abstract not available for DE112005003306 (T5)
Abstract of corresponding document: WO2006072099 (A1)

A method and apparatus (114, 116) that receives an IP packet and encapsulates the packet with an IP header. Further, time-domain multiplexed voice data is received and converted into VoIP packets. Still further, Signaling System (7) (SS7) compliant signals are decoded. The decoded (SS7) signals are received and encapsulated prior to transmission to a telephony device (102).

(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 003 306 T5** 2008.01.24

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/072099**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 003 306.6**
(86) PCT-Aktenzeichen: **PCT/US2005/047679**
(86) PCT-Anmeldetag: **29.12.2005**
(87) PCT-Veröffentlichungstag: **06.07.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **24.01.2008**

(51) Int Cl.[8]: ***H04L 29/06*** (2006.01)

(30) Unionspriorität:
11/027,915 **30.12.2004** **US**

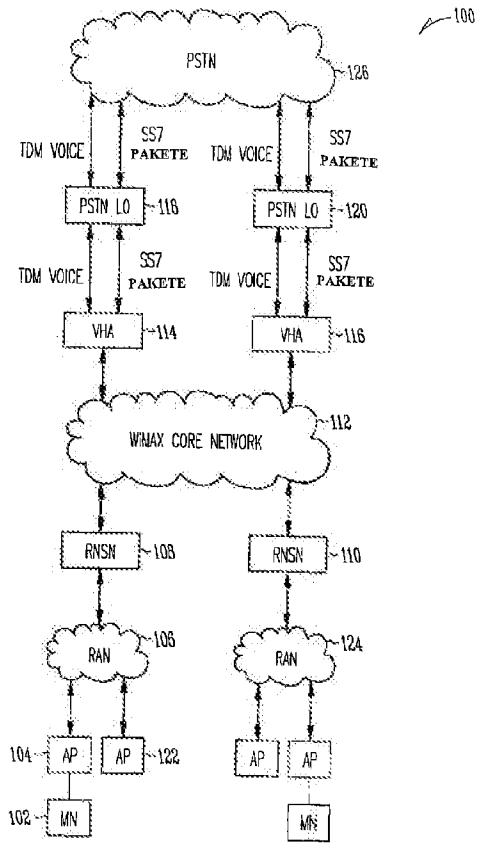
(71) Anmelder:
Intel Corporation, Santa Clara, Calif., US

(74) Vertreter:
BOEHMERT & BOEHMERT, 28209 Bremen

(72) Erfinder:
Lebizay, Gerald, Madision, N.J., US

(54) Bezeichnung: **Verteiltes Sprachnetzwerk**

(57) Hauptanspruch: Gerät mit:
– Einkapselungsschaltungen, um ein IP-Paket zu empfangen und das Paket mit einem IP-Header zu versehen;
– VoIP (Voice-over-IP) Schaltungen, um Zeit-Domain-multiplexte Sprachdaten zu empfangen und diese Daten in VoIP-Pakete umzuwandeln;
– Signalschaltungen, um Signalsystem 7 (SS7) kompatible Signale zu decodieren; und
– Steuerschaltungen, um
decodierte SS7-Signale aus den Signalschaltungenn zu empfangen und die decodierten SS7-Signale an die verkapselten Schaltungen zur Übertragung an eine Telefonieeinrichtung zu senden,
VoIP-Pakete auf der VoIP-Schaltung zu empfangen und die VoIP-Pakete an die Verkapselungsschaltungen zur Übertragung an die Telefoneinrichtung weiterzuleiten.



Beschreibung

Technisches Gebiet

[0001] Ausführungsbeispiele der Erfindung betreffen die Sprache-über-IP (VoIP)-Technologie, die in einem mobilen drahtlosen Breitbandnetzwerk implementiert ist.

Hintergrund

[0002] Die VoIP (Voice-over-IP)-Technologie erlaubt es teilnehmenden Parteien, mündlich über ein Paket-geschaltetes IP Netzwerk zu kommunizieren. Die VoIP-Technologie hat in ihrer Popularität gewonnen und abhängig von bestimmten Faktoren kann sie eine Tonqualität gewährleisten, die der von PSTN (Public Switched Telephone Network) den öffentlichen geschalteten Telefonnetzwerken vergleichbar ist.

[0003] Weiter hat auch die Popularität von drahtlosen Mobilnetzwerken zugenommen. Drahtlose mobile Netzwerke erlauben einem Gerät, sich in ein Netzwerk einzukoppeln, ohne eine physikalische leitende Leitung zu benötigen, um Daten zwischen dem Gerät und dem Netzwerk zu übertragen. Weiter können solche Netzwerke Mobilität ermöglichen, indem sie es einem Gerät erlauben, die Zugriffspunkte zu wechseln, in einer Art und Weise, die den Netzwerkelementen oder Knoten außerhalb des drahtlosen mobilen Netzwerkes transparent ist.

[0004] Obwohl die VoIP-Technologie und die drahtlosen mobilen Netzwerke steigende Popularität genießen, gibt es keine mobilen Nutzergeräte für die vorliegenden VoIP-Dienste über das Internet. Ein Faktor, der das Voranschreiten solcher mobilen Geräte verhindert, betrifft das Ermitteln eines einfachen Schemas, durch das einem mobilen Gerät ermöglicht werden kann, sich über eine bedeutende geographische Fläche fremd einzuschalten (und daher potentiell zwischen diesen Domänen zu wandern) während es eine einzelne IP-Adresse zu behalten scheint. Das UDP (User Datagram Protocol) indiziert Verbindungen unter der Benutzung eines Quadrupletts, das die IP-Adressen und Portnummern von beiden Verbindungsendpunkten umfasst. Das Ändern einer dieser vier Nummern verursacht, dass die Verbindung unterbrochen und verloren geht. Daher ist es wichtig, dass das Gerät die gleiche IP-Adresse behält, während es geographisch sich woanders einschaltet. Die Schwierigkeit im Adressieren dieses Themas steigt, wenn die geographische Fläche wächstm, durch die es dem Gerät erlaubt wird, zu wandern.

[0005] Aus dem Vorangegangen ist es klar, dass eine Notwendigkeit existiert für ein Schema, durch das drahtlose IP-Telefongeräten erlaubt werden kann, sich in einer geographisch bedeutsamen Fläche fremd einzuschalten, wie z.B. der Fläche einer großen Stadt. Es ist wünschenswert, dass sich ein solches Schema einfach als ein Overlay zu einem existierenden drahtloses Netzwerk implementieren lässt. Es ist weiter wünschenswert, dass ein solches Schema leicht mit dem PSTN verbunden werden kann.

Kurze Beschreibung der Zeichnungen

[0006] Fig. 1 zeigt eine Netzwerkumgebung, in der ein Ausführungsbeispiel eines Sprach-Heimagenten (VHA, engl.: voice home agent) genutzt wird.

[0007] Fig. 2 zeigt einen Protokollstapel, der einen VHA nach einem Ausführungsbeispiel der Erfindung ausmacht.

[0008] Fig. 3 zeigt ein Tunnelschema, das durch eine mobile IP-Schicht des Protokollstapels genutzt wird, die in der Fig. 2 dargestellt ist.

[0009] Fig. 4 zeigt ein Verfahren des Beginnens eines VoIP-Anrufs nach einem Ausführungsbeispiel der Erfindung.

[0010] Fig. 5 zeigt ein Verfahren zum Durchführen eines VoIP-Anrufs nach einem Ausführungsbeispiel der Erfindung.

[0011] Fig. 6 zeigt eine Hardwareumgebung, in der ein VHA nach einem Ausführungsbeispiel der Erfindung verkörpert sein kann.

Ausführliche Beschreibung

[0012] Fig. 1 zeigt eine Netzwerkumgebung **100**, in der einem oder mehreren Mobilknoten **102** erlaubt werden kann, über ein geographisch bedeutsames Gebiet sich fremdeinzuloggen, wie z.B. in einem Großstadtgebiet. Die Mobilknoten **102** kommunizieren über digitale Transmission (typischerweise im 2-bis-6 GHz lizensierten Frequenzbereich und mit typischen Kanalbandbreiten zwischen 1,5 bis 20 MHz) mit einem Zugriffspunkt **104**. Ein Zugriffspunkt (auch als Basisstation bezeichnet), wie z.B. der, der durch das Bezugszeichen **104** bezeichnet ist, empfangt Übertragungen aus dem Mobilknoten und kommuniziert die Übertragungen an Netzwerkelemente innerhalb eines zugehörigen regionalen Zugriffnetzwerkes **106**. Nach einem Ausführungsbeispiel ist das regionale Zugriffsnetzwerk **106** ein verdrahtetes Netzwerk (z.B. eine physikalische Leitung verbindet die verschiedenen Elemente, die ein solches regionales Zugriffsnetzwerk ausmachen), das ein tatsächliches Paket basiertes Zugriffsnetzwerk wie z.B. ein Ethernet-Netzwerk, ein IP/MPLS-Netzwerk oder ein ATM-Netzwerk. Die Übertragung zwischen dem Zugriffspunkt **104** und dem Mobilknoten **102** ist mit den Standardsignalen des Institut der elektrischen und

elektronischen Ingenieure (IEEE) 802.16 Standardsignalen, IEEE Standard 802.12-2001, veröffentlicht 2001 und späteren Versionen (hierin als IEEE 802.16 Standard oder IEEE 802.16e-Standard) kompatibel. Ein regionales Netzwerk **106** das Zugriffspunkte (wie z.B. **104**) miteinander verbindet und mit den IEEE 802.16e-Standards übereinstimmt, wird als WiMAX-Netzwerk bezeichnet.

[0013] An der Peripherie eines WiMAX-Regionalnetzwerks **106**, ist ein Radio-Netzwerk Serviceknoten **108**. Der Radio-Netzwerk Serviceknoten **108** schafft ein Routen und eine Steuerung zwischen anderen WiMAX-Regionalnetzwerken wie z.B. dem WiMAX-Netzwerk, das durch Bezugszeichen **124** identifiziert ist. Jedes Regionalzugriffsnetzwerk **106** und **124** umfasst einen Radio-Netzwerk Serviceknoten (**108**, **110**), der in das regionale Zugriffsnetzwerk **106** oder **124** an ein WiMAX-Kernnetzwerk **112** koppelt, das alle die regionalen Zugriffsnetzwerke **106** und **124** miteinander verbindet. Obwohl das WiMAX-Kernnetzwerk **112** in Fig. 1 als die zwei WiMAX-Netzwerke **106** und **124** miteinander verbindend dargestellt ist, kann das WiMAX-Kernnetzwerk **112** im Prinzip jede Anzahl von regionalen Zugriffsnetzwerken miteinander verbinden.

[0014] Das WiMAX-Kernnetzwerk **112** kann ein herkömmliches IP-Netzwrk sein, das aus IP-Netzwerkelementen besteht, die allgemein verfügbar sind, wie z.B. optischen Netzwerkelementen, die hohe Datentransferraten erlauben. Als ein solches kann das WiMAX-Kernnetzwerk **112** direkt mit dem Internet (nicht in Fig. 1 dargestellt) verbinden.

[0015] An der Peripherie des WiMAX-Kernnetzwerkes **112** sind einer oder mehr VHA(s) **114** und **116** vorhanden. Dort existiert ein VHA **114** oder **116**, der zu jedem WiMAX-Regionalzugriffsnetzwerk **106** und **124** gehört. Die Struktur der und die Verfahren, die durch ein VHA **114** oder **116** benutzt werden, werden im Detail im Folgenden beschrieben. In Kürze kann ein VHA als ein Netzwerkelement beschrieben werden, das die VoIP-Intergration zwischen einem WiMAX-Kernnetzwerk (wie z.B. einem Kernnetzwerk **112**) und dem öffentlichen geschalteten Telefonnetzwerk (PSTN) **126** erlaubt. Zusätzlich schafft ein VHA eine Funktionalität, die es einem Mobilknoten (wie z.B. den Mobilknoten **102**) erlaubt, sich von einem WiMAX-Regionalzugriffsnetzwerk (wie z.B. Netzwerk **106**) in ein anderes (wie z.B. **124**) einzuschalten.

[0016] Obwohl Fig. 1 einen einzelnen VHA **114** oder **116** mit jedem Regionalnetzzugriffsnetzwek **124** verbunden zeigt, können mehr als nur als ein VHA mit einem vorgegebenen Regionalzugriffsnetzwerk verbunden sein. Obwohl Bezugszeichen **114** und **116** hierin als zu einem einzelnen VHA gehörig dargestellt werden, kann jedes Bezugszeichen **116** und **116** als bezugnehmend auf eine Gruppe vom VHA verstanden werden, die ihre jeweiligen WiMAX-Regionalzugriffsnetzwerke **106** und **124** bedienen.

[0017] Jeder VHA **114** und **116** bietet eine Schnittstelle an das WiMAX-Kernnetzwerk **112** in einem Geschäftslokal **118** oder **120** des PSTN **126**. Das PSTN **126** nutzt ein außerhalb der Bandbreite Signalschema (out-of-band-signalling), das als Signalsystem 7 (SS7) von der Internationalen Telekommunikations Union (ITU) der Telecommunication Standardization Sector (ITU-T) bezeichnet wird. Ein außerhalb der Bandbreite Signalschema nutzt einen anderen physikalischen Part für die Anrufsteuerung als den, der dazu benutzt wird, den Inhalt des Anrufes selbst (z.B. die Sprachdaten) zu übertragen. Daher wird, wie in Fig. 1 dargestellt, ein VHA zwei separate Schnittstellen bedienen. Eine Schnittstelle für Sprachdaten, die als multiplexte digitale Sprachdaten in der Zeitdomain übertragen werden und eine Schnittstelle für SS7 Steuersignale, die als SS7 Pakete übertragen werden.

[0018] Ein Mobilknoten, wie z.B. der, der durch Bezugszeichen **102** bezeichnet ist, kann als Telefonhandgerät (in gleicher Weise wie ein Mobiltelefon) verkörpert sein, kann ein PDA (personal digital assistant) sein oder kann als eine andere mobile Recheneinheit verkörpert sein. Nach einem Anschalten macht der Mobilknoten eine anfängliche Übertragung an den nahezu möglichen Zugriffspunkt. Zum Zeitpunkt der Übertragung weist der Mobilknoten einen Managementkanal zu der den Mobilknoten an den Accesspoint fixiert. Der Accesspoint und der Mobilknoten können miteinander über eine Distanz kommunizieren, die zwischen ein bis fünf Meilen (1,8 km–18 km) beträgt. In Anbetracht der Größe eines solchen Gebietes können andere Mobilknoten hierin beherbergt sein. Daher kann ein Zukunftspunkt mit Hunderten von Mobilknoten kommunizieren. Die Benutzung von Managementkanälen erlaubt, einen Accessknoten einen Accesspunkt von einem anderen zu unterscheiden.

[0019] Jeder Accesspoint in einem WiMAX-Regionalzugriffsnetzwerk besitzt eine IP-Adresse, die ihn identifiziert. Jedoch funktioniert diese IP-Adresse nur innerhalb des regionalen Accessnetzwerks (das auch als Domain bezeichnet wird), in dem der Accesspoint sich befindet. Daher kann ein Accesspoint direkt Daten zu einem anderen Accesspoint innerhalb des regionalen Accessnetzwerks, in dem er sich befindet, senden. Um Daten an einen Accespoint in einer anderen Domain zu schicken, muss der Radionetzwerkknoten, der die betreffende Domain bedient, in der der Accesspoint sich befindet, als ein Mittler genutzt werden.

[0020] Wie oben beschrieben, wird eine Anfangstransmission während des Startens des Mobilnetzknotens gemacht werden müssen, um einen Ma-

nagementkanal und Authentifizierung des Benutzers an die Basisstation zu schicken. Daraufhin macht der Mobilknoten eine Anfangskommunikation mit dem VHA, der die Domain versorgt, in der der Mobilknoten sich befindet. Diese Kommunikation markiert den Anfang des Registrierungsprozesses durch den der Mobilknoten den VHA informiert, in welcher Domain sich der Mobilknoten befindet. Als Antwort weist der VHA dem Mobilknoten eine IP-Adresse zu, die als mobile IP (MIP)-Adresse bekannt ist. Der VHA (voice home agent) speichert auch eine Care-Of-(c/o) Adresse für den Mobilknoten. Die MIP-Adresse des Mobilknotens ändert sich nicht, sogar wenn der Mobilknoten in eine geographische Region wandert, in der er mit einem anderen Accesspoint kommuniziert oder mit einem WiMAX-Regionalzugriffsnetzwerk ganz anderer Art. Die CO-Adresse andererseits identifiziert die Domain, mit der der Mobilknoten kommuniziert und ändert sich daher, wenn der Mobilknoten von einem Regionalaccessnetzwerk zu einem anderen seine Einwahl ändert.

[0021] Ein VHA kann einem Mobilknoten mehr als eine IP-Adresse zuweisen. Zum Beispiel kann der Mobilknoten eine IP-Adresse besitzen, die dafür vorgesehen ist, die Sprachdaten zu übertragen und eine andere IP-Adresse, die zum Tragen von Signaldaten vorgesehen ist. Zum Zwecke der Einfachheit geht die Offenbarung von der Annahme aus, dass jeder Mobilknoten eine einzelne IP-Adresse besitzt, die ihm während der Registrierung zugewiesen wurde.

[0022] Zum Zeitpunkt der Registrierung aktualisiert der VHA eine Datenbasis, die er unterhält. Die Datenbasis kann Information betreffend die Merkmale, die von dem Mobilknoten unterstützt werden (call waiting, voicemail, etc.) umfassen. Die Datenbasis wird aktualisiert, um eine Telefonnummer zuzufügen, durch den der Mobilknoten identifiziert ist, weiter die MIP-Adresse, die dem Mobilknoten zugewiesen ist und die Domain, in der der Mobilknoten angeordnet ist (z.B., die c/o-Adresse des Mobilknotens).

[0023] Ein WiMAX-Regionalzugriffsnetzwerk **106** oder **124** nutzt eine Technik, die als Tunneling bekannt ist. Durch die Vorteile dieser Technik ist eine Bewegung eines Mobilknotens innerhalb eines geographischen Gebietes, das von einer vorgegebenen Wi-MAX-Domain **106** oder **124** bedient wird, transparent gegenüber Netzwerkelementen oder Knoten außerhalb der Domain. Dadurch kann z.B. ein Netzwerkknoten außerhalb einer WiMAX-Domain **106** nicht mitteilen, ob der Mobilknoten **102** mit dem Accesspoint **104** oder dem Accesspoint **122** kommuniziert. Ein Netzwerkelement außerhalb der Domain **106** muss nur wissen, dass der Mobilknoten **102** innerhalb der Domain **106** angeordnet ist, um mit dem Mobilknoten **102** zu kommunizieren. Daher wird, wenn immer ein Mobilknoten (z.B., der Mobilknoten **102**) sich von einer Domain zu einer anderen bewegt, der Mobilknoten erneut mit dem VHA anmelden, bei dem er vorher registriert war. Als Antwort aktualisiert der VHA seine Datenbasis, um eine c/o-Adresse (z.B., eine Netzwerkadresse der Domain, mit der der Mobilknoten kommuniziert) zu dem Mobilknoten zu speichern.

[0024] Die vorangehende Diskussion ist auf eine Netzwerkumgebung fokussiert, in der ein VHA **114** oder **116** betrieben wird. Die folgende Diskussion gibt kurz die Protokollschichten wieder, die einen VHA **114** oder **116** ausmachen.

[0025] Fig. 2 zeigt einen Protokollstapel **200**, der durch den VHA **114** oder **116** ausgeführt wird. Wie aus Fig. 2 ersichtlich ist, umfasst der Protokollstapel **200** eine Mobil-IP (MIP) Schicht **202**, die Funktionalität nach einem industrieakzeptieren MIP Standard wie z.B. dem Standard, der im „IP Mobility Support", C. Perkins, ed., IETF RFC 2002, Oktober 1996 beschrieben ist. Die Funktionalität, die von der MIP-Schicht **202** geschaffen wird, wird auch den oberen Schichten **204** bis **210** des Stapels **200** möglich gemacht.

[0026] Der MIP-Layer schafft die Tunnelingfunktionalität, die oben beschrieben ist. Die Fig. 3 zeigt den MIP-Layer **202** während er ein Pakt **300** empfangt, das einen IP-Header **302** aufweist. Der IP-Header **302** umfasst die MIP-Adresse, die an den bestimmten Mobilknoten in seiner 32-Bit Ziel IP-Adressfeld und ist daher als $\text{IP-Header}_{\text{MIP}}$ bezeichnet. Als Antwort auf das Empfangen eines solchen Paketes **300** fügt der MIP-Layer **202** das Paket **300** an einen zweiten IP-Header **304** hinzu. Der zweite IP-Header nutzt die c/o-Adresse des besonderen Mobilknotens, der durch die MIP-Adresse identifiziert ist und daher $\text{IP-Header}_{\text{CareOf}}$. Dadurch beobachtet das WiMAX-Kernnetzwerk **112** den zweiten IP-Header **304** und leitet das Paket **300** an den zweiten IP-Header **304**, was bedeutet, dass das Paket **300** an die entsprechende Domain **106** oder **124** geleitet ist. Vor dem Empfang durch das Mobilnetzwerk wird der zweite IP-Header **304** abgetrennt.

[0027] Der Effekt der Tunnelingtechnik, die in Bezug auf Fig. 3 beschrieben wird, ist, dass jeder Mobilknoten IP-Pakete empfangt, die die MIP-Adresse umfassen, die ihnen während des Registrierungsprozesses zugewiesen wurden. Dementsprechend kann jeder Mobilknoten fremd zugreifen, – sogar Fremdzugriff zwischen Domainen – während die IP-Adresse, die ihm zugewiesen ist, während des Registrierungsprozesses beibehalten wird.

[0028] Viele Schichten des Tunnelns können in der Netzwerkumgebung **100** genutzt werden, die in Fig. 1 dargestellt ist. Zum Beispiel kann jedes WiMAX-regionale Zugriffsnetzwerk **106** und **124** Tunneling nutzen, so dass Elemente, die außerhalb der Do-

main liegen nur IP-Adresspakete an die richtige Domain benötigen, damit jedes Paket den gewünschten Mobilknoten erreicht.

[0029] Bezugnehmend auf Fig. 2 kann erkannt werden, dass der Protokollstapel **200** auf einen VoIP-Layer **204** umfasst, der Sprache über IP-Funktionalität schafft und einem industrieakzeptierten VoIP-Standard entspricht, wie z.B. dem RTP (Realtime Transport Protocol), das durch IETF RFC 1889 und/oder RTSP (Realtime Straming Protocol), das durch IETF RFC 2326 definiert ist. Kurz gesagt, empfangt der VoIP-Layer **204** VoIP-Pakete und überträgt diese Pakete in die Zeitdomain in multiplexte Digitalsprachdaten für ein PSTN (Public Switched Telephone Network – ein öffentliches geschaltetes Telefonnetzwerk) **118** und **120** und umgekehrt. Wie im folgenden beschrieben, wird in dem Kontext einer Diskussion zwischen einem Nutzer eines Mobilknotens und einem Nutzer eines PSTN der VoIP-Layer **204** die Zeitdomain Multiplex Digitaldaten in VoIP-Pakete konvertieren. Die VoIP-Pakete, die die MIP-Adresse umfassen, werden an einen bestimmten Mobilknoten gesandt. Die VoIP-Pakete werden an den MIP-Layer **202** weitergegeben, der die VoIP-Pakete an einen IP-Header anhängt, der die c/o-Adresse des bestimmten Mobilknotens umfasst.

[0030] Der Protokollstack **200** umfasst auch ein Sitzungsbeginnprotokoll **206**, das SIP-Funktionalität schafft, die mit einem industrieakzeptierten Standard übereinstimmt wie z.B. die IETF RFC 3261. In Kürze gesagt, schafft der SIP-Layer **206** eine Anwendungs-Layer-Steuerungsfunktionalität zum Schaffen, Modifizieren und Beenden von Kommunikationssitzungen mit einem oder mehreren Teilnehmern. Zum Beispiel kann der SIP-Layer **206** die Funktionalität umfassen, einem Mobilknoten zu signalisieren, dass eine andere Partei mit ihm zu kommunizieren wünscht.

[0031] Der Protokollstack **200** umfasst einen Layer **210**, der mit dem PSTN über eine Schnittstelle in Verbindung tritt. Der Layer **210** umfasst einen MGW (Media Gateway), der Zeit-Domain multiplexte Sprachdaten in IP-Pakete multiplext. Er umfasst auch eine SS7-Schnittstelle, die SS7-Signale empfängt, die Signale decodiert und die extrahierte Information an den VHA-Steuerungsebene **208** weitergibt. Die VHA-Steuerungsebene **208** koordiniert die Arbeit der verschiedenen Layer. Sie vermittelt Kommunikation zwischen dem Hauptgateway und dem VoIP-Layer **204** und vermittelt auch Kommunikation zwischen der SS7-Schnittstelle und dem SIP-Layer **206**. Zum Beispiel kann die VHA-Steuerungsebene **208** ein Signal von der SS7-Schnittstelle **210** empfangen, das anzeigt, das eine Verbindung zu einer bestimmten Telefonnummer gewünscht ist. Als Antwort kann die Steuerungsebene **208** die SIP-Ebene **206** wecken, um eine SIP-Einladungsmitteilung an den Mobilknoten entsprechend der Telefonnummer zu senden. Auf gleicher Weise kann die Steuerungsebene **208** Sprachdaten in einem bestimmten Zeitfenster empfangen und die Daten an die VoIP-Schicht zur Umwandlung in VoIP-Pakete weiterleiten und für Kommunikation mit bestimmten Mobilknoten (auf diese Weise wird ein Sprachpfad beibehalten).

[0032] Die vorangehende Diskussion zeigt kurz die Protokollschichten **202** bis **210**, die ein VHA **114** oder **116** ausmachen. Eine Diskussion in Bezug auf den Betrieb des VHA **114** oder **116** im Bezug auf Anruf-Start und Anruf-Ausführung folgt nun. Diese Diskussion beschreibt den Betrieb des VHA als Ganzes (entgegengesetzt zu einer Layerzu-Layer-Basis) und schafft eine integrierte Ansicht hohen Niveaus des Betriebs des VHA.

[0033] Fig. 4 zeigt den Betrieb des VHA **114** oder **116** beim Initiieren eines Telefonanrufes zu einem Mobilknoten. Dieses Verfahren kann durch einen Nutzer der PSTN oder durch einen Nutzer eines Mobilknotens gestartet werden, der durch den VHA **114** oder **116** bedient wird. Wenn das Verfahren von einem Nutzer des PSTN begonnen wird, dann empfangt der VHA **114** oder **116** ein SS7-Signal, das anzeigt, dass ein Telefonanruf mit einem Mobilknoten, der durch eine bestimmte Telefonnummer identifiziert ist, gewünscht wird, wie dies in Arbeitsschritt **400** dargestellt ist. Die Telefonnummer wird von dem SS7-Signal extrahiert (Arbeitsschritt **400**). Das SS7-Signal wird in eine Einladungsmitteilung konvertiert (Schritt **400**), die eine SIP-Mitteilung ist, die anzeigt, dass eine Kommunikationsverarbeitung gewünscht ist. Daher wird nach Beendigung des Schrittes **400** der VHA **114** oder **116** eine Einladungsmitteilung an eine bestimmte Telefonnummer konstruiert haben.

[0034] Andererseits kann der Prozess durch einen Mobilknoten initiiert worden sein, der durch den VHA **114** oder **116** bedient wird. Wenn ein Mobilknoten den Telefonanruf beginnt, sendet der Mobilknoten eine SIP-Einladungsmitteilung, die an eine ausgewählte Telefonnummer adressiert ist an den VHA **114** oder **116**. Diese SIP-Einladungsmitteilung wird von dem VHA empfangen, wie in Schritt **402** dargestellt.

[0035] Ob die SIP-Einladungsmitteilung empfangen wird (wie dies der Fall ist, wenn ein Mobilknoten den Telefonanruf beginnt), oder ob sie von dem VHA erzeugt wird (wie dies der Fall ist, wenn ein Nutzer des PSTN den Telefonanruf beginnt, der Betriebsablauf schreitet zu Arbeitsschritt **404** vor. In Arbeitsschritt **404** fragt der VHA eine Datenbasis die MIP-Adresse zu identifizieren und die c/o-Adresse, die mit der Telefonnummer zugehörig ist, die in der Einladungsmitteilung eingebettet ist.

[0036] Wenn die Telefonnummer, die in Arbeitsschritt **404** identifiziert wurde, mit der Domain, die von

dem VHA **114** oder **116** bedient wurde, korrespondiert, sendet das VHA **114** oder **116** die SIP-Einladungsmitteilung an den Mobilknoten unter Benutzung der Tunnelingtechnik, die in Bezug auf Fig. 3 beschrieben wurde (Arbeitsschritt **406**).

[0037] Wenn die Telefonnummer, die in Arbeitsschritt **404** identifiziert wurde mit einer Domain korrespondiert, die nicht von dem VHA **114** oder **116** bedient wurde, dann sendet der VHA **114** oder **116** die SIP-Einladungsmitteilung an den VHA **114** oder **116**, der die Domain korrespondierend an dem eingeladenen Mobilgerät bedient (Arbeitsschritt **408**).

[0038] Wenn die Telefonnummer anzeigt, dass die Telefonnummer zu einer Telefoniereinrichtung gehört, die durch das PSTN bedient wird, wird die Einladungsmitteilung an ein SS7-Signal konvertiert, um den Telefonanruf auf das PSTN zurückzuführen (Arbeitsschritt **410**).

[0039] Nachdem die Einladungsmitteilung gesendet wurde (mittels einer SIP-Einladungsmitteilung oder mittels eines SS7-Signals) wartet der VHA **114** oder **116** eine Antwort ab auf die Einladungsmitteilung wie im Arbeitsschritt **412** dargestellt. Wenn der Nutzer der eingeladenen Telefonieeinrichtung wünscht den Telefonanruf zu beantworten, kann eine Antwort, die einen solchen Wunsch anzeigt, von der VHA **114** oder **116** empfangen werden (Arbeitsschritt **412**). Wenn die Antwort von einem Mobilknoten stammt, kann die Antwort dem VHA **114** oder **116** in der Form einer SIP-Bestätigungs(Ack)-Mitteilung erreichen. Andererseits kann, wenn die Antwort von einer PSTN-Telefonieeinrichtung stammt, die Antwort an den VHA **114** oder **116** in Form eines SS7-Signals kommen, das in eine SIP-ack-Mitteilung konvertiert werden kann.

[0040] Nachdem die Antwort empfangen wurde, wird sie an den Initiator weitergeleitet (Arbeitsschritt **414**). Wenn der Initiator des Telefonanrufs einen Mobilknoten ist, umfasst die Weiterleitungsoperation das Senden der Antwort an den Mobilknoten (unter Benutzung einer MIP-Layer **202**, um die Tunnelingtechnik zu nutzen, mit Bezug auf Fig. 3. Andererseits, wenn der Initiator des Telefonanrufs eine Telefonieeinrichtung auf dem PSTN ist, dann wird die Antwort in ein SS7-Signal konvertiert und ist an das PSTN durch die SS7-Schnittstelle **210** gerichtet.

[0041] Schließlich ist, unter der Annahme, dass die Antwort, die in Schritt **412** empfangen wurde, anzeigt, dass der Nutzer des eingeladenen Mobilknotens eine Kommunikationsdurchführung zu beginnen wünscht (z.B. wünscht, den Anruf zu beantworten) ein Sprachweg zu der einladenden und der eingeladenen Einrichtung etabliert (Arbeitsschritt **416**). Etablieren des Sprachweges kann bedeuten, dass ein zugehöriger bestimmter Zeitfenster in der Zeitdomain multiplexte Sprachdaten von dem PSTN lokalen Büro **118** oder **120** mit einer besonderen MIP-Adresse (und umgekehrt) zusammenführt. Zusätzlich kann es das Zusammenführen einer MIP-Adresse eines Mobilknotens mit einer c/o-Adresse oder einer Adresse eines VHA **114** oder **116** bedeuten, der einen bestimmten Mobilknoten bedient.

[0042] Nachdem eine VoIP-Sitzung etabliert wurde (wie in Fig. 4 dargestellt), können die Parteien miteinander sprechen. Während die Parteien sprechen, empfangt der VHA **114** oder **116** entweder VoIP-Pakete oder Zeit-Domain multiplexte Sprachdaten von dem PSTN wie in Arbeitsschritt **500** der Fig. 5 dargestellt. Wenn der VHA Zeit-Domain multiplexte Sprachdaten vom PSTN empfängt, werden solche Daten in VoIP-Pakete konvertiert, wie oben beschrieben.

[0043] Als Nächstes werden wie in Arbeitsschritt **502** dargestellt, das VoIP-Paket oder die Sprachdaten entlang des Sprachweges, der in Betriebsschritt **416** der Fig. 4 etabliert wurde, gesendet. Für den Fall des Sendens von VoIP-Paketen an einen Mobilknoten kann dies bedeuten, dass VoIP-Pakete an einen VHA **114** oder **116** gesendet werden, der den Mobilknoten bedient oder es kann nur bedeuten, dass direkt die empfangenen VoIP-Pakete an einen Mobilknoten gesendet werden unter Benutzung der Tunnelingtechnik, die mit Bezug auf Fig. 3 beschrieben wurde. Für den Fall des Sendens von Sprachdaten kann eine Telefonieeinrichtung auf dem PSTN kann der Arbeitsschritt **502** das Konvertieren von VoIP-Daten in Time-Domain multiplexte digitale Sprachdaten umfassen und das Einsetzen solcher Sprachdaten in ein geeignetes Zeitfenster, so dass die PSTN-Schalteinrichtung die Daten an die entsprechende Position routet.

[0044] Die vorangehende Diskussion betrifft den Betrieb des VHA während des Beginns und der Durchführung eines Telefonanrufs. Die folgende Beschreibung stellt vom Ansichtspunkt des Systemniveaus den Beginn und die Durchführung eines Telefonanrufs in Zusammenhang mit einer Netzwerkumgebung **100** dar, die in Fig. 1 dargestellt ist.

[0045] In dem Kontext eines Telefonanrufs zwischen einer PSTN-Telefonieeinrichtung (Initiator des Anrufs) und einem Mobilknoten (Angerufener) wird der Arbeitsablauf wie folgt voranschreiten. Zu Beginn wird der VHA **114** oder **116** ein SS7-Signal empfangen, das eine Kommunikationssitzung mit einem Mobilgerät gewünscht ist, das mit einer vorgegebenen Telefonnummer korrespondiert. Der VHA extrahiert die Telefonnummer und kreiert eine SIP-Einladungsmitteilung, die an eine MIP-Adresse des eingeladenen Mobilknotens gerichtet ist (wenn der eingeladene Mobilknoten nicht zugänglich ist, kann der Anruf umgeleitet werden an einen Voice Mail Service).

[0046] Durch die Tunneling Fähigkeit des VHA und die verschiedene WiMAX-Domain, kann die SIP-Einladungsmitteilung den eingeladenen Mobilknoten erreichen, wobei sie zu der MIP-Adresse des Mobilknotens gerichtet ist. Innerhalb der SIP-Einladungsmitteilung wird die Anrufer-ID Information eingebettet. Daher kann eine Mitteilung, die die einladende Telefonieeinrichtung identifiziert am eingeladenen Mobilknoten angezeigt werden. Inzwischen sendet der VHA **114** oder **116** ein SS7-Signal, das von einem Anrufton bei dem einladenden Telefongerät resultiert.

[0047] Wenn der Nutzer des Mobilknotens den Anruf annimmt, wird eine SIP-Bestätigungsmitteilung an den VHA **114** oder **116** gesandt. Der VHA **114** oder **116** übersetzt die SIP-Bestätigungsmitteilung in ein SS7-Signal und stellt einen Sprachweg her. Zu diesem Zeitpunkt beginnen die Nutzer der PSTN-Telefonieeinrichtung und des Mobilknotens zu sprechen.

[0048] Im Kontext eines Telefonanrufes zwischen zwei mobilen Knoten (in unterschiedlichen Domainen) kann der Arbeitsablauf wie folgt sein. Zunächst empfangt der VHA eine SIP-Einladungsmitteilung von dem einladenden Mobilknoten. Die SIP-Einladungsmitteilung wird an eine Telefonnummer adressiert, die mit dem gewünschten Mobilknoten korrespondiert. Als Antwort wird der VHA die SIP-Einladungsmitteilung an den VHA senden, der die Domain bedient, in der der eingeladene Knoten angeordnet ist. Der letztere VHA sendet die Antwort an die SIP-Adresse des einladenden Mobilknotens.

[0049] Durch die Fähigkeit des Tunnelings des VHA und die verschiedenen WiMAX-Domainen, kann die SIP-Einladungsmitteilung den eingeladenen Mobilknoten erreichen, wobei sie an die MIP-Adresse des Mobilknotens adressiert ist. Innerhalb der SIP-Einladungsmitteilung wird Anrufer-ID Information eingebettet. Daher kann eine Mitteilung, die die einladende Telefonieeinrichtung identifiziert, an dem eingeladenen Mobilknoten angezeigt werden. Weiter kann die IP-Adresse des einladenden Mobilknotens in der SIP-Einladungsmitteilung enthalten sein.

[0050] Wenn der Nutzer des eingeladenen Mobilknotens den Anruf annimmt, wird ein SIP-Bestätigungssignal an den VHA **114** oder **116** in der Domain gesendet, in der der eingeladene Mobilknoten vorhanden ist. Als Antwort wird der VHA **114** oder **116** das SIP-Einladungssignal an den VHA **114** und **116** weiterleiten, der die Domain bedient, in der das einladende Mobilknoten angeordnet ist. Der letztere VHA **114** oder **116** leitet die SIP-Bestätigungsmitteilung an die MIP-Adresse des einladenden Mobilknotens. Die SIP-Bestätigungsmitteilung umfasst die IP-Adresse des eingeladenen Knotens.

[0051] Die Sprachkommunikation kann nun in einer von zwei Weisen erfolgen. Als erstes können die Mobilknoten miteinander ohne die Zwischenschaltung von VHAs kommunizieren. Dies ist möglich, da durch die Fähigkeiten des SIP-Einladungs- und Bestätigungsmitteilung jeder Mobilknoten von der IP-Adressse des anderen gewahr ist. Jedoch kann die Verbindung zwischen den zwei Mobilknoten verloren gehen, sollte einer der Mobilknoten in eine andere Domain sich fremd einloggen.

[0052] Als zweites kann der Sprachpfad sich zwischen beiden VHAs erstrecken. Dieses Schema erlaubt es jeder der Mobilknoten sich von einer Domain zur nächsten fremd einzuloggen.

[0053] Die Fig. 6 zeigt eine Hardwareumgebung, in der der VHA **114** oder **116** verkörpert sein kann. Die Umgebung umfasst vier Blätter **600**, **602**, **604** und **606**. Jedes Blatt umfasst seine eigene Rechnerumgebung, inkl. eines Prozessors, eines Speichers und eines Input/Output-Moduls (einer Steuerung Hub und eines I/O-Bus zum Beispiel) die Zugriff auf eine Netzwerkschnittstelle oder einen Speicher geben. Jedes Blatt **600**, **606** kann über ein lokales Netzwerk wie zum Beispiel ein Ethernet Hub kommunizieren. Die Blätter oder Karten **600–606** können als dünne Platten innerhalb eines Regals befestigt werden.

[0054] Jedes Blatt kann dazu vorgesehen werden, verschiedene Facetten der im vorangegangenen beschriebenen Steuerungsebenenfunktionen oder Datenebenenfunktionen ausführen. Zum Beispiel kann das Blatt **602** die Funktionen, die mit dem MIP-Layer **202** in Bezug stehen, ausführen. Dieses Blatt **602** umfasst die Routingfunktionalität, die benötigt wird, wenn ein VoIP-Paket empfangen wird und an einen anderen VHA gereutet werden muss oder an einen Mobilknoten wie oben beschrieben. Das Blatt **602** umfasst ein Netzwerkinterface das es erlaubt, dass die Software/Firmware, die darauf ausgeführt wird, mit dem WiMAX **112** kommuniziert.

[0055] Blatt **604** kann die VoIP-Funktionalität ausführen, die oben in Bezug auf den VoIP-Layer **204**, der in der Fig. 2 diskutiert wurde, beschrieben wurde. Blatt **604** umfasst ein Zeit-Domain-Multiplexing-Schnittstelle, um es der Software/Firmware, die dazu ausgeführt wird, zu erlauben, mit dem Timedomain-Multiplex Digital Sprachsignal von dem PSTN zu interagieren.

[0056] Das Blatt **606** kann die SS7-Signale decodieren und den extrahierten Inhalt an die SS7-Anwendungsschicht Funktionalität senden, die auf dem Blatt **600** ruht. Das Blatt **606** umfasst eine SS7-Schnittstelle, um es der Software/Firmware zu erlauben, darauf ausgeführt zu werden, um mit den SS7-Paketen aus dem PSTN lokalen Betrieb zu interagieren.

[0057] Blatt **600** kann die VHA-Steuerungsebenen-

funktion, die oben beschrieben wurde, ausführen. Zum Beispiel kann das Blatt einen Speichertreiber umfassen (um die Datenbasis, die notwendig ist, eine solche Funktionalität beizubehalten) durchzuführen. Das Blatt **600** kann die SIP-Funktionalität und die Anwendungsschichtfunktionalität des SS7-Subsystems ebenso ausführen. In einem Ausführungsbeispiel führt das Blatt **600** eine Abrechnungsroutine aus. Die Abrechnungsroutine kann auf einer Nutzer-zu-Nutzer- oder einer Konto-zu-Konto- Basis die Zeitdauer eines vorgegebenen Nutzers bestimmen, die er mit dem Netzwerk verbunden ist, die Menge an Verkehr, die von dem Nutzer konsumiert wurde, den Typ des Dienstes, der genutzt wurde (Ortsanruf, Ferngespräch, etc.) oder die Bandbreite, die von dem Nutzer konsumiert wurde. Die verfolgte Information kann in einer Datenbasis gespeichert werden und periodische Abrechnungen können daraus erzeugt werden.

[0058] Ausführungen der Erfindung können implementiert werden in einem oder in einer Kombination der folgenden Hardware, Firmware und Software. Ausführungen der Erfindung können auch als Befehle reglementiert werden, die auf einem maschinenlesbaren Medium gespeichert sind (z.B., einem Computer). Zum Beispiel kann das maschinenlesbare Medium ein Nur-Lese-Speicher (ROM) ein RAM (Random-Access Memory) eine magnetische Speicherplatte, ein optische Speichermedium, ein Flashspeicher, elektrische optische akustische oder andere Formen von sich fortpflanzenden Signalen (z.B., Trägerwellen, Infrarotsignale, Digitalsignale, etc.) und andere sein.

[0059] Die Zusammenfassung ist geschaffen, um mit Abschnitt 37 CFR Sektion 1.72(b) übereinzustimmen die erfordert, dass eine Zusammenfassung es dem Leser erlaubt, die Natur und den Zweck der technischen Offenbarung zu erfassen. Es wird darum gebeten, dass verstanden wird, dass diese nicht dazu genutzt wird, den Schutzbereich oder die Offenbarung der Ansprüche zu interpretieren.

[0060] In der vorangehenden detaillierten Beschreibung sind verschiedene Merkmale an einigen Punkten zusammen zu einem einzelnen Ausführungsbeispiel zum Zwecke der Zusammenfassung der Offenbarung gruppiert. Dieses Verfahren der Offenbarung soll nicht dahingehend interpretiert werden, dass es Sinn und Zweck war, die beanspruchten Ausführungsbeispiele mehr Merkmale aufweisen zu lassen als explizit in jedem Anspruch dargelegt sind. Stattdessen soll in den folgenden Ansprüchen das Erfinderische des Anmeldegegenstandes in weniger als allen Merkmalen eines einzelnen Ausführungsbeispiels liegen. Die nachfolgenden Ansprüche werden daher in die Offenbarung mit aufgenommen, wobei jeder Anspruch als eigenständig zu behandeln ist als einzelnes vorzugsweise Ausführungsbeispiel.

ZUSAMMENFASSUNG

[0061] Verfahren und Vorrichtung (**114**, **116**), die ein IP-Paket empfängt und das Paket mit einem IP-Header verkapselt. Weiter sind Zeit-Domain-multiplexte Sprachdaten empfangen worden und in VoIP-Pakete konvertiert worden. Weiter wiederum werden SS7 (signaling system 7) kompatible Signale decodiert. Die decodierten SS7 Signale werden empfangen und vor der Übertragung an eine Telefonieeinrichtung (**102**) verkapselt.

Patentansprüche

1. Gerät mit:
– Einkapselungsschaltungen, um ein IP-Paket zu empfangen und das Paket mit einem IP-Header zu versehen;
– VoIP (Voice-over-IP) Schaltungen, um Zeit-Domain-multiplexte Sprachdaten zu empfangen und diese Daten in VoIP-Pakete umzuwandeln;
– Signalschaltungen, um Signalsystem 7 (SS7) kompatible Signale zu decodieren; und
– Steuerschaltungen, um
decodierte SS7-Signale aus den Signalschaltungenn zu empfangen und die decodierten SS7-Signale an die verkapselten Schaltungen zur Übertragung an eine Telefonieeinrichtung zu senden,
VoIP-Pakete auf der VoIP-Schaltung zu empfangen und die VoIP-Pakete an die Verkapselungsschaltungen zur Übertragung an die Telefoneinrichtung weiterzuleiten.

2. Gerät nach Anspruch 1, wobei der Verkapselungsschaltkreis, die VoIP-Schaltungen, die Signal-Schaltungen und die Steuer-Schaltungen als Mikroprozessoren in Datenkommunikation mit einer Speichereinrichtung verkörpert sind.

3. Gerät nach Anspruch 1, wobei die Verkapselungsschaltungen als eine erste Schaltkarte verkörpert sind, die VoIP-Schaltungen in einer zweiten Schaltkarte verkörpert sind, die Signal-Schaltungen als dritte Schaltkarte verkörpert sind, und die Steuer-Schaltungen als vierte Schaltkarte verkörpert sind; und die ersten, zweiten, dritten und vierten Schaltkarten in Datenkommunikation miteinander stehen.

4. Gerät nach Anspruch 3, wobei die ersten, zweiten, dritten und vierten Schaltkarten über ein LAN (local area network) miteinander kommunizieren.

5. Gerät nach Anspruch 3, wobei die vierte Schaltkarte weiter dazu konfiguriert ist, eine Datenbank in Bezug auf Telefonnummern, mobile IP (MIP) Adressen und c/o-Adressen von mobilen Telefoneinrichtungen zu unterhalten.

6. Gerät nach Anspruch 3, wobei die erste

Schaltkarte ein Interface an ein IP-Netzwerk umfasst.

7. Gerät nach Anspruch 3, wobei die zweite Schaltkarte ein Interface an ein Netzwerk, das Zeit-Domain-multiplexte Sprachdaten trägt, umfasst.

8. Gerät nach Anspruch 3, wobei die dritte Schaltkarte ein Interface an ein SS7-Netzwerk umfasst.

9. Verfahren zum Durchführen einer VoIP-Telefonsitzung umfassend:
– Empfangen einer Anforderung von einer ersten Telefonieeinrichtung um eine zweite Telefonieeinrichtung, die durch eine besondere Telefonnummer identifiziert ist, dazu einzuladen, in einer VoIP-Telefonsitzung teilzunehmen,
– In-Bezug-Setzen der Telefonnummer zu einer IP-Adresse, die zu der Telefonnummer zugehörig ist,
– Senden einer Einladung an die IP-Adresse,
– Empfangen einer Antwort auf die Einladung, und
– Modifizieren und Weiterleiten einer Antwort an die erste Telefonieeinrichtung, so dass die modifizierte Antwort ein erstes IP Header inklusive einer ersten IP-Adresse der ersten Telefonieeinrichtung umfasst und eine zweite IP Header inklusive einer zweiten IP-Adresse der ersten Telefonieeinrichtung, wobei die IP-Adresse einen Punkt der Verbindung der ersten Telefonieeinrichtung zum einem Netzwerk anzeigt und wobei die zweite IP-Adresse als Ergebnis der Registrierung der ersten Telefonieeinrichtung mit einem VHA (voice home agent) erzeugt ist.

10. Verfahren nach Anspruch 9, wobei das In-Bezug-setzen der Telefonnummer zu einer IP-Adresse den Zugriff auf eine Datenbasis umfasst, um eine IP-Adresse eines VHA zu bestimmen, der der zweiten Telefonieeinrichtung dient.

11. Verfahren nach Anspruch 9, wobei die Einladung mit einem SIP (Session Initiation Protocol) kompatibel ist.

12. Verfahren nach Anspruch 9, weiter umfassend:
– Empfangen eines IP-Paketes, das Daten enthält, die einen Sprachton repräsentieren, und
– Weiterleiten eines IP-Paketes an das erste Gerät unter Benutzung eines dritten IP-Headers inklusive einer dritten IP-Adresse und eines vierten IP-Headers sowie einer vierten IP-Adresse,
wobei die dritte IP-Adresse einen Verbindungspunkt einer ersten Telefonieeinrichtung mit einem Netzwerk zeigt, und wobei die vierte IP-Adresse als ein Ergebnis der Registrierung der ersten Telefonieeinrichtung bei einem VHA ist.

13. Verfahren nach Anspruch 9, weiter umfassend:
– Empfangen eines IP-Paketes, das Sprache repräsentierende Daten umfasst, und
– Senden eines IP-Paketes an einen VHA, der der zweiten Einrichtung dient.

14. Verfahren nach Anspruch 9, weiter umfassend:
– Feststellen, dass die erste Telefonieeinrichtung ihren Verbindungscode mit dem Netzwerk geändert hat,
– erneutes Definieren der ersten IP-Adresse, um den geänderten Verbindungspunkt zu identifizieren.

15. Verfahren nach Anspruch 9, wobei die erste IP-Adresse ein Radionetzwerkdienst-Knoten identifiziert, der an ein 802.16e-kompatibles Netzwerk gekoppelt ist, das einen Zugriffspunkt umfaßt, an den die erste Telefonieeinrichtung kommuniziert.

16. Maschinenlesbares Medium, das Befehle vermittelt, die, wenn auf sie zugegriffen wird, eine Maschine dazu veranlassen, folgende Arbeitsschritte durchzuführen:
– Empfangen einer Anforderung von einer ersten Telefonieeinrichtung um eine zweite Telefonieeinrichtung, die durch eine bestimmte Telefonnummer identifiziert ist, dazu einzuladen, in einer VoIP-Telefoniesitzung teilzunehmen,
– In-Bezug-Setzen der Telefonnummer zu einer IP-Adresse, die mit der Telefonnummer zugehörig ist,
– Senden einer Einladung an die IP-Adresse,
– Empfangen einer Antwort auf die Einladung, und
– Modifizieren und Weiterleiten der Antwort an die erste Telefonieeinrichtung, so dass die modifizierte Antwort einen ersten IP-Header umfaßt, inklusive einer ersten IP-Adresse einer ersten Telefonieeinrichtung, und einen zweite IP-Header, inklusive einer zweiten IP-Adresse der ersten Telefonieeinrichtung, wobei die erste IP-Adresse einen Verbindungspunkt der ersten Telefonieeinrichtung mit dem Netzwerk anzeigt, und wobei die zweite IP-Adresse als Ergebnis der Registrierung der ersten Telefonieeinrichtung mit einem VHA erzeugt ist.

17. Medium nach Anspruch 16, wobei die Telefonnummer als IP-Adresse umfassend den Zugriff auf eine Datenbasis ist, um eine IP-Adresse einer VHA festzustellen, die als zweite Einrichtung dient.

18. Medium nach Anspruch 16, wobei die Einladung mit einem SIP (Session Initiation Protocol) kompatibel ist.

19. Medium nach Anspruch 16, wobei die Arbeitsschritte weiter umfassen:
– Empfangen eines IP-Paketes, das Sprache repräsentierende Daten umfasst, und
– Weiterleiten eines IP-Paketes an die erste Einrichtung unter Benutzung eines dritten IP-Headers inklusive einer dritten IP-Adresse und eines vierten IP-Heders inklusive einer vierten IP-Adresse, und

wobei die dritte IP-Adresse einen Verbindungspunkt der ersten Telefonieeinrichtung an ein Netzwerk anzeigt, und wobei die vierte IP-Adresse als Ergebnis der Registrierung der ersten Telefonieeinrichtung mit einem VHA erzeugt ist.

20. Medium nach Anspruch 16, wobei der Betrieb weiter umfasst:
– Empfangen eines IP-Paketes, das Sprache repräsentierende Daten umfasst, und
– Senden des IP-Paketes zu einem VHA (Voice Home Agent), der der zweiten Einrichtung dient.

21. Medium nach Anspruch 16, wobei die Arbeitsschritte weiter umfassen:
– Feststellen, dass die erste Telefonieeinrichtung ihren Verbindungspunkt mit dem Netzwerk verändert hat, und
– Umändern der ersten IP-Adresse, um den veränderten Verbindungspunkt zu identifizieren.

22. Medium nach Anspruch 16, wobei die erste IP-Adresse ein Radionetzwerkdienst-Knoten identifiziert, der mit einem 802.16e-kompatiblen Netzwerk gekoppelt ist, das einen Zugriffspunkt umfaßt, mit dem die erste Telefonieeinrichtung kommuniziert.

23. System umfassend:
– Einkapselungsschaltungen um ein IP-Paket zu empfangen und das Paket mit einem IP-Header zu versehen;
– VoIP (Voice-over-IP) Schaltungen, um Zeit-Domain-multiplexte Sprachdaten zu empfangen und diese Daten in VoIP-Pakete zu konvertieren;
– Abrechnungsschaltungen, die dazu eingerichtet sind, die Dauer und den Typ der Nutzung des Systems zu messen und solche Messungen mit einem Nutzerkonto in Bezug zu setzen;
– Signalschaltungen, um System 7 (SS7) kompatible Signal zu decodieren und
– Steuer-Schaltungen, um
decodierte SS7 Signale aus den Signalschaltungen zu empfangen und die decodierten SS7 Signale an die Verkapselungsschaltungen zu übertragen und an eine Telefonieeinrichtung weiterzuleiten; und
VoIP-Pakete aus den VoIP-Schaltungen zu empfangen und die VoIP-Pakete an die Verkapselungsschaltungen zu übertragen und an die Telefonieeinrichtung weiterzuleiten.

24. System nach Anspruch 23, wobei die Einkapselungsschaltungen, die VoIP-Schaltungen, die Signalschaltungen, die Abrechnungsschaltungen und die Steuerschaltungen als Mikroprozessoren in Datenkommunikation mit einer Speichereinrichtung verkörpert sind.

25. System nach Anspruch 23, wobei die Verkapselungsschaltungen auf eine erste Schaltkarte, die VoIP-Schaltungen als eine zweite Schaltkarte, die Signalschaltungen als eine dritte Schaltkarte und die Kontrollschaltungen und die Abrechnungsschaltungen als eine vierte Schaltkarte verkörpert sind, und die erste, zweite, dritte und vierte Schaltkarte in Datenkommunikation miteinander stehen.

26. System nach Anspruch 25, wobei die erste, zweite, dritte und vierte Schaltkarte miteinander über ein LAN (local area network) kommunizieren.

27. System nach Anspruch 25, wobei die vierte Schaltkarte weiter konfiguriert ist um eine Datenbasis zu unterhalten, die in Bezug auf Telefonnumern mobile IP (MIP) Adressen und c/o-Adressen von mobilen Telefoniegeräten.

28. System nach Anspruch 25, wobei die erste Schaltkarte eine Schnittstelle an ein IP-Netzwerk umfasst.

29. System nach Anspruch 25, wobei die zweite Schaltkarte eine Schnittstelle an ein Netzwerk umfasst, das Zeit-Domain-multiplexte Sprachdaten trägt.

30. System nach Anspruch 25, wobei die dritte Schaltkarte ein Interface an ein SS7-Netzwerk bietet.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

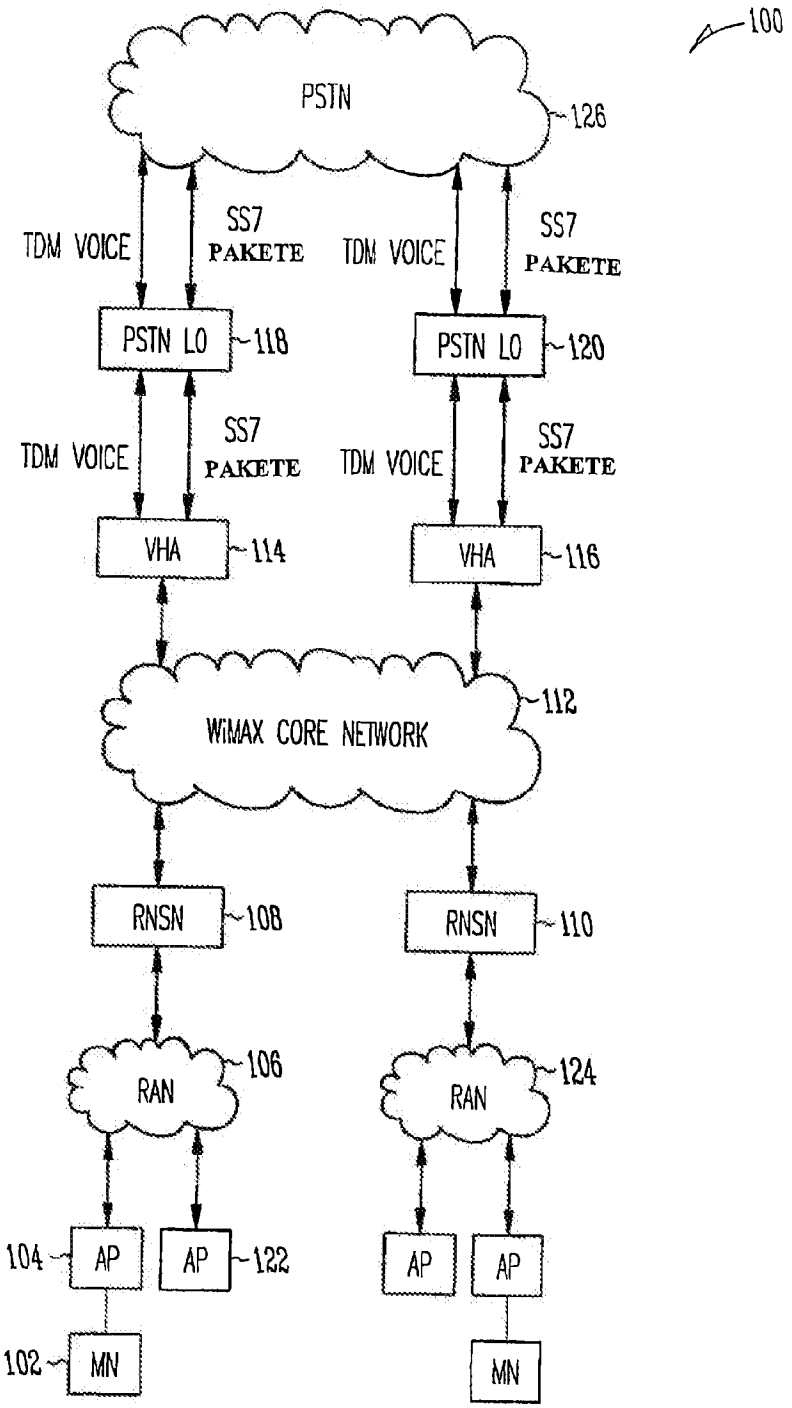


Fig. 1

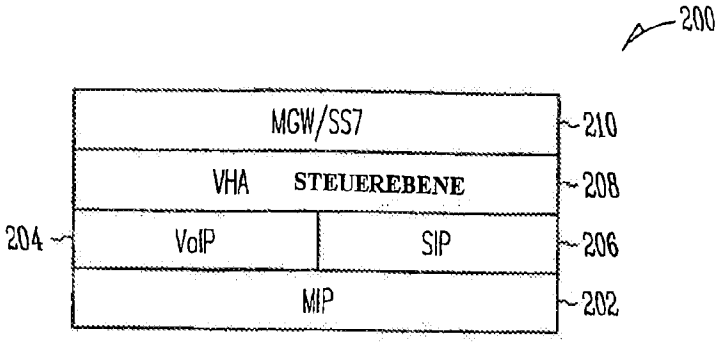


Fig.2

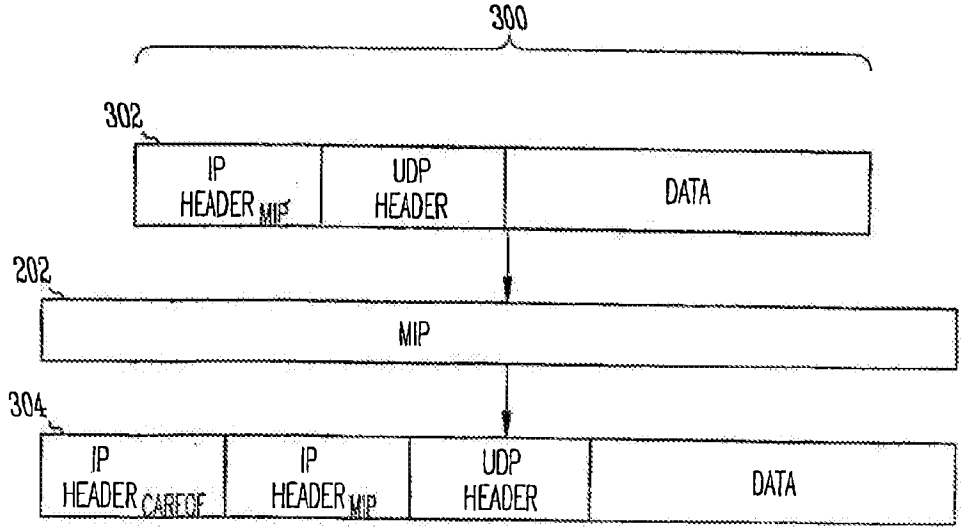


Fig.3

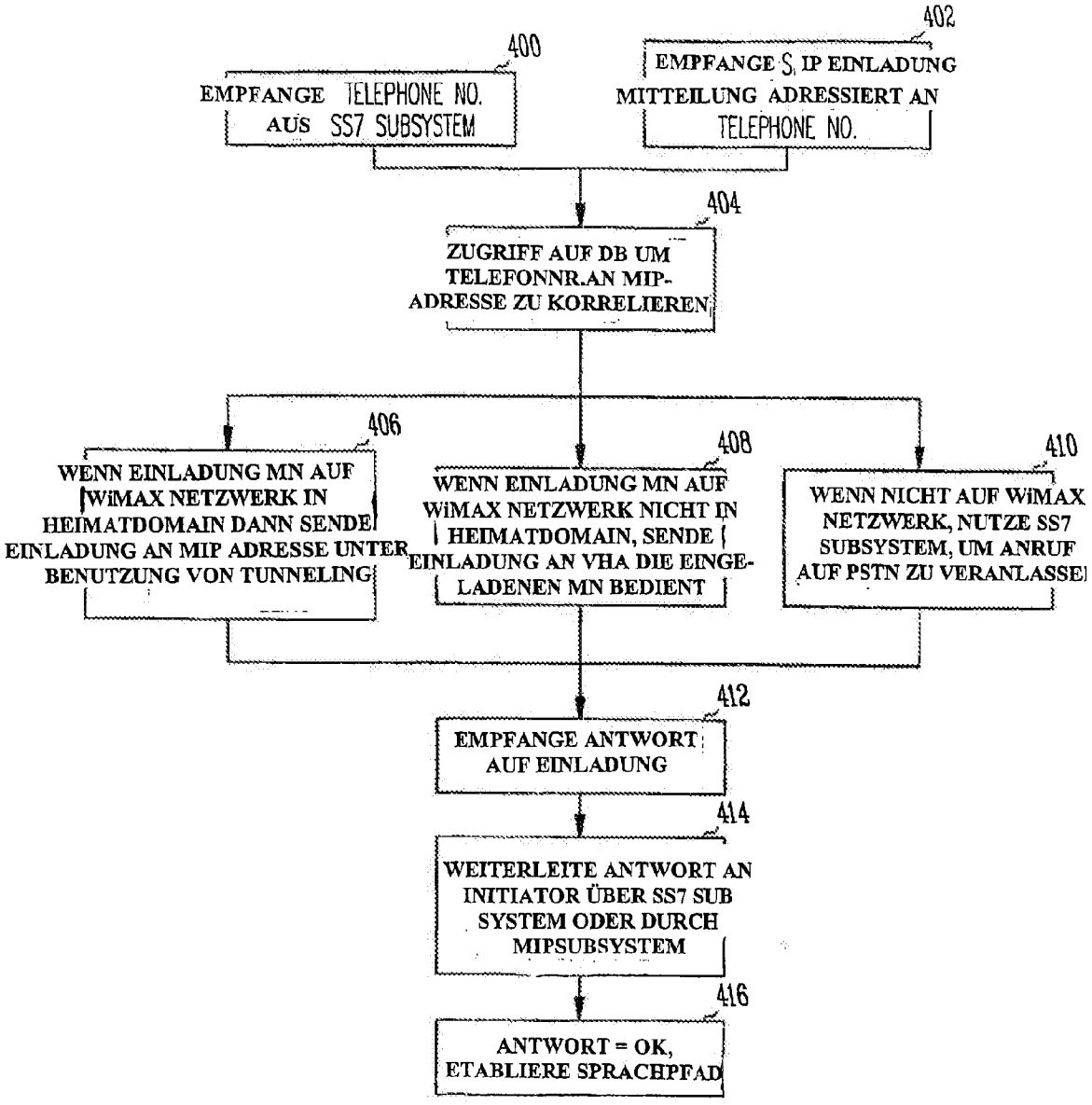


Fig. 4

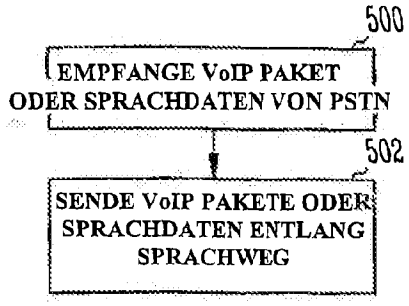


Fig. 5

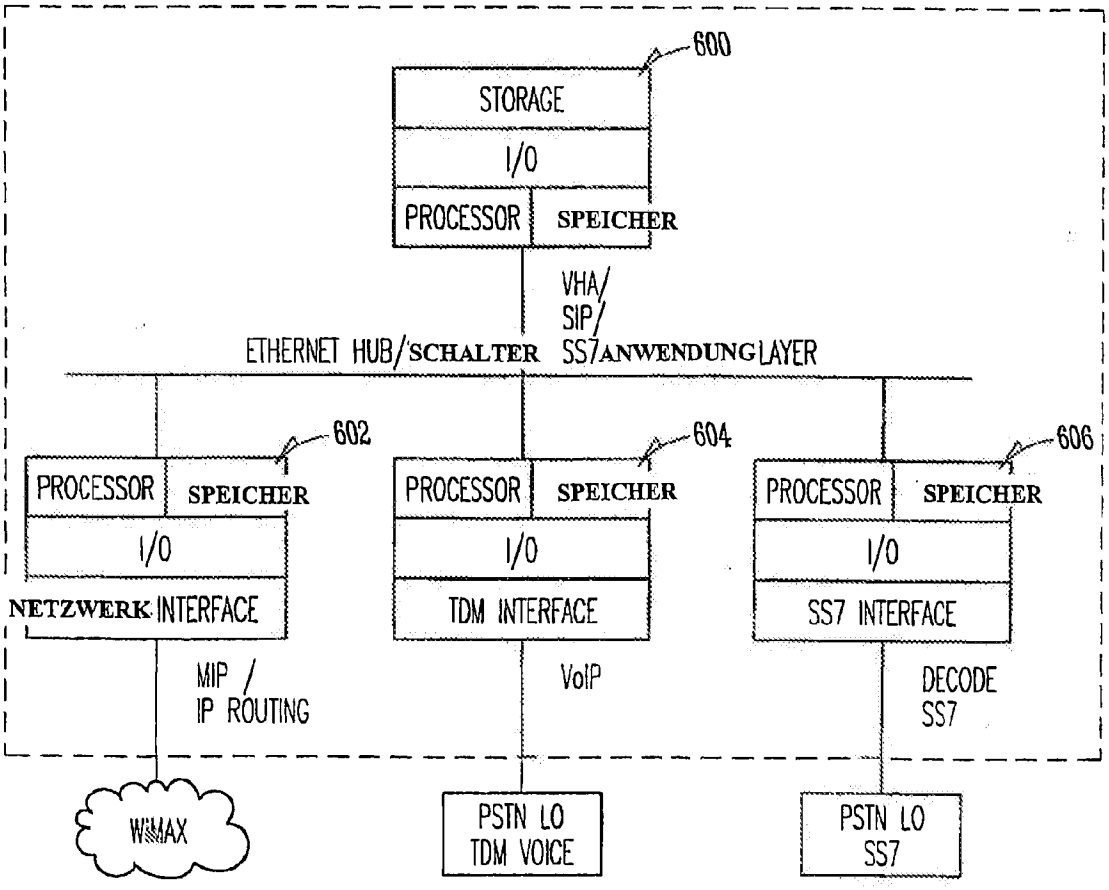


Fig. 6

Espacenet

Bibliographic data: DE60133316 (T2) — 2008-07-10

SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS

Inventor(s): PYKE CRAIK R [CA]; HERN WILLIAM [GB]; THOMPSON ROGER L [US]; CARON SERGE S [CA]; MOUNJI HALIMA H [CA]; EWOTI CHARLES B [DE]; GOERENS MICHAEL [DE]; STRENG PETE J [CA]; GOERTZEN CHRISTOPHER J [CA]; KITTLITZ CHRISTIAN [CA]; TAYLOR RICHARD C [CA]; WELHAM MICHAEL [DE] + (PYKE, CRAIK R, ; HERN, WILLIAM, ; THOMPSON, ROGER L, ; CARON, SERGE S, ; MOUNJI, HALIMA H, ; EWOTI, CHARLES B, ; GOERENS, MICHAEL, ; STRENG, PETE J, ; GOERTZEN, CHRISTOPHER J, ; KITTLITZ, CHRISTIAN, ; TAYLOR, RICHARD C, ; WELHAM, MICHAEL)

Applicant(s): NORTEL NETWORKS LTD [CA] + (NORTEL NETWORKS LTD)

Classification: - international: ***H04L12/26; H04L12/56; H04L29/06; H04M3/22; H04M7/00***
- cooperative: **H04L29/06**; **H04L63/30**; **H04L69/22**; **H04M3/2281**; **H04M7/006**; H04Q2213/13034; H04Q2213/13196; H04Q2213/13372; H04Q2213/13389

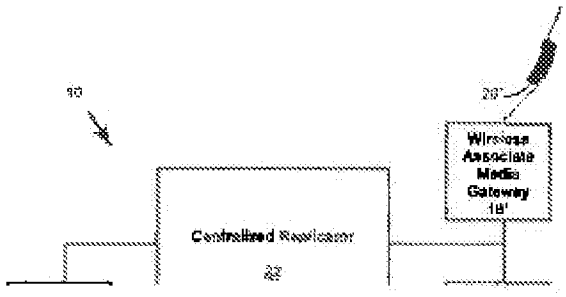
Application number: DE2001633316T 20011009

Priority number(s): US20000239048P 20001010 ; WO2001US31548 20011009

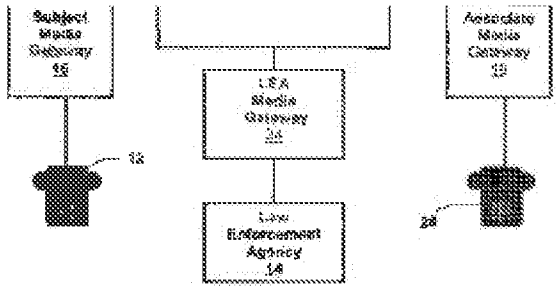
Also published as: WO02082782 (A2) WO02082782 (A3) US2003179747 (A1) EP1362456 (A2) EP1362456 (A4) EP1362456 (B1) CA2437275 (A1) AU2001297701 (A1) less

Abstract not available for DE60133316 (T2)
Abstract of corresponding document: WO02082782 (A2)

A system and method for intercepting a telecommunication signal are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload and



PETITIONER APPLE INC. EX. 1004-582



adding a second header to replicated payload and directing the replicated payload to the address associated with the second.;A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 601 33 316 T2** 2008.07.10

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 362 456 B1**
(21) Deutsches Aktenzeichen: **601 33 316.0**
(86) PCT-Aktenzeichen: **PCT/US01/31548**
(96) Europäisches Aktenzeichen: **01 273 516.3**
(87) PCT-Veröffentlichungs-Nr.: **WO 2002/082782**
(86) PCT-Anmeldetag: **09.10.2001**
(87) Veröffentlichungstag der PCT-Anmeldung: **17.10.2002**
(97) Erstveröffentlichung durch das EPA: **19.11.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **19.03.2008**
(47) Veröffentlichungstag im Patentblatt: **10.07.2008**

(51) Int Cl.[8]: ***H04L 12/56*** (2006.01)

(30) Unionspriorität:
239048 P **10.10.2000** **US**

(73) Patentinhaber:
Nortel Networks Ltd., St. Laurent, Quebec, CA

(74) Vertreter:
Patentanwälte Wallach, Koch & Partner, 80339 München

(84) Benannte Vertragsstaaten:
DE, FR, GB

(72) Erfinder:
PYKE, Craik R., Nepean, ON K2H 8A6, CA; HERN, William, Knowl hill, Reading RG 10 9UP, GB; THOMPSON, Roger L., RTP, NC 27709, US; CARON, Serge S., Gatineau, PQ J8V 1X9, CA; MOUNJI, Halima H., Kanata, ON K2T 1E2, CA; EWOTI, Charles B., 88677, Markdorf, DE; GOERENS, Michael, 88045 Friedrichshafen, DE; STRENG, Pete J., Manotick, ON K4M 1G5, CA; GOERTZEN, Christopher J., Ottawa, ON K1G 6N6, CA; KITTLITZ, Christian, Ottawa, ON K1V 8G1, CA; TAYLOR, Richard C., Manotick, ON K4M 1A2, CA; WELHAM, Michael, 88662 Lippertsreute, DE

(54) Bezeichnung: **SYSTEM UND VERFAHREN ZUM ABFANGEN VON TELEKOMMUNIKATIONEN**

Beschreibung

Hintergrund der Erfindung

[0001] Bei der Durchsetzung von Gesetzen ist es in manchen Fällen erforderlich, eine Person oder eine Gruppe von Personen zu überwachen, um Anschuldigungen hinsichtlich einer illegalen Aktivität zu stützen. Tatsächlich fordern viele Länder, dass Telekommunikations-Diensteanbieter und Ausrüstungs-Hersteller einer Exekutiv- oder Vollstreckungsbehörde die Fähigkeit geben, auf gesetzlicher Grundlage ein Abfangen oder Abhören von Telekommunikationen zu und von einer Person durchzuführen, die überwacht wird.

[0002] In der Vergangenheit bestand das gesetzlich genehmigte Abhören darin, dass Krokodilklemmen verwendet werden, mit denen eine Exekutivbehörde physikalisch die Telekommunikations-Leitung einer Person (des überwachten Teilnehmers) angezapft hat, um Anrufe an oder von einem Partner (den bzw. dem die Person anrufenden oder von der Person angerufenen Teilnehmer) zu überwachen.

[0003] Es gibt zwei Kategorien des Abfangens, nämlich Anruf-Daten und Anruf-Inhalt. Das Abfangen von Anruf-Daten schließt die Überwachung von Anruf-Ereignissen ein, beispielsweise die Uberwachung, ob die Person einen Anruf ausführt, oder ob ein Anruf an die Person gerichtet wird, oder ob ein Anruf an irgendeine andere Stelle gelenkt wird. Diese Art der Überwachung, die als Stammregister bekannt ist, liefert die Telefonnummer sowohl der angerufenen Person als auch der anrufenden Person, zusammen mit Anruf-Ereignissen und Zeit-Datums-Stempeln darüber, wann das Ereignis eingetreten ist. Im Gegensatz hierzu schließt der Anruf-Inhalt den tatsächlichen Inhalt des Anrufs ein, das heißt die Unterhaltung, die erfolgt, plus den Anruf-Daten. Der Anruf-Inhalt wird an die Polizei- oder Exekutivbehörde in Echtzeit übertragen, so dass die Polizeibehörde die Unterhaltung verfolgen kann, während sie erfolgt. Diese Übertragung muss für die Person und deren Partner transparent sein, so dass sie nicht erkennen, dass sie überwacht werden.

[0004] Mit der Weiterentwicklung von Telekommunikations-Ausrüstungen wurden Module in der Telekommunikations-Vermittlung bereitgestellt, die der Exekutivbehörde die Möglichkeit gaben, auf gesetzlicher Grundlage Telekommunikationen abzufangen oder abzuhören. Beispielsweise ergibt in einer Zeitmultiplex-(TDM-)Vermittlung, wie z. B. der DMS-100-Vermittlung der Firma Nortel Networks eine Netzwerk-Vermittlungsstruktur einen Zugangspunkt, der es einer Exekutivbehörde ermöglicht, die Telefonleitung einer Person anzuzapfen. Diese Art des zentral angeordneten Zugangspunktes ist als ein Abhör- oder Abfang-Zugangspunkt (IAP) bekannt. Die resultierende Information wird dann an die Polizeibehörde geliefert.

[0005] Mit der Entwicklung der Telekommunikation zu paketbasierten Kommunikationen in Richtung auf die Einführung des Internetprotokolls (IP) und der asynchronen Übertragungsbetriebsart-(ATM-)Protokolle hat die sich ändernde Architektur der Telekommunikations-Vermittlungen notwendigerweise das Abfangen oder Abhören von Inhalten schwieriger gemacht.

[0006] Eine Möglichkeit, mit der versucht wurde, diese Schwierigkeit zu überwinden, ist in der internationalen Patentanmeldung 99/17499 beschrieben. Bei dieser Anmeldung wird die Verwendung eines gesetzeskonformen Abhörknotens beschrieben, von dem zumindest einige der Pakete, die von einer derartigen Mobilstation ausgehen oder an dieser enden, an zumindest einen Unterstützungsknoten (SGSN, GGSN) über den gesetzeskonformen Abhörknoten (LIN) an die Exekutivbehörde gelenkt und/oder kopiert werden. Weil jedoch der LIN den Unterstützungsknoten als ein sendender oder empfangender Knoten erscheint, kann das System nicht vollständig transparent sein.

[0007] Ein Verfahren, mit dem das Abhören oder Abfangen eingeleitet werden kann, ist weiterhin in der internationalen Patentanmeldung 00/56029 beschrieben. Diese Patentanmeldung beschreibt eine Abhör-Datensammelfunktion, die in einem vorhandenen Netzwerkknoten, wie z. B. einen GPRS-Unterstützungsknoten implementiert werden kann und eine flexible. Implementierung des Abhörsystems ermöglicht. Schließlich ist ein Verfahren zur Übertragung abgehörter oder abgefangener Pakete von einem Abfang-Netzwerk-Element an eine Exekutivbehörde in der internationalen Patentanmeldung 00/42742 beschrieben. Bei dieser Anwendung werden Daten, die an die Exekutivbehörde gesandt werden, über einen sicheren Tunnel gesendet, der durch Verschlüsselungs-Verarbeitung geschaffen wird.

[0008] Im September 1998 erließ das Federal Communications Committee (FCC) eine Regel, dass neue TDM-Ausrüstungen eine gesetzeskonforme Abhörmöglichkeit eingebaut haben müssen. Weiterhin erließ die FCC im August 1999 die Regelung, dass eine Paket-Kommunikations-Abhörfähigkeit ab 30. September 2001 erforderlich ist.

[0009] Entsprechend besteht eine Notwendigkeit, in der Lage zu sein, Sprache-über-Paket-Kommunikationen in einer Weise abzufangen oder abzuhören, die Regierungsanforderungen erfüllt, für die abgehörte Person und deren Partner transparent ist, in Echtzeit abläuft und mit Standard-Protokollen arbeitet, wie z. B. IP- und ATM-Anwendungen.

Zusammenfassung der Erfindung

[0010] Die Erfindung ergibt sich aus der Erkenntnis, dass wirklich effiziente und wirkungsvolle Systeme und Verfahren zum Abfangen oder Abhören von Sprache-über-Paket-Kommunikationen erzielt werden, bei denen ein Paket-Kommunikations-Signal zu oder von der abzuhörenden Person von einem zentralisierten Replikator empfangen wird. Das Kopffeld wird von dem Paket abgestreift, so dass lediglich die Nutzdaten verbleiben, und die Nutzdaten werden repliziert, ein Kopffeld wird zu den replizierten Nutzdaten hinzugefügt, und die replizierten Nutzdaten werden an eine Exekutivbehörde gesandt. Ein Kopffeld wird zu den ursprünglichen Nutzdaten hinzugefügt, und das Paket wird erneut an den vorgesehenen Empfänger abgesandt. Alternativ kann das gesamte Paket repliziert werden und die Kopffelder können sowohl von dem ursprünglichen Paket als auch dem replizierten Paket abgestreift werden, und ein neues Kopffeld wird zu allen Nutzdaten hinzugefügt. Die Nutzdaten werden dann zu dem vorgesehenen Empfänger und an die Exekutivbehörde gesendet.

[0011] Gemäß einem Gesichtspunkt der vorliegenden Erfindung wird ein Verfahren zum Abfangen oder Abhören eines Telekommunikations-Signals geschaffen, das zwischen einer ersten Medien-Überleiteinrichtung und einer zweiten Medien-Überleiteinrichtung übertragen wird, wie dies im Anspruch 1 angegeben ist. Gemäß einem zweiten Gesichtspunkt der vorliegenden Erfindung wird ein System zum Abfangen oder Abhören eines Telekommunikations-Signals geschaffen, das zwischen einer ersten Medien-Überleiteinrichtung und einer zweiten Medien-Überleiteinrichtung übertragen wird, wie es im Anspruch 9 angegeben ist.

[0012] In einer Ausführungsform wird ein Verfahren zum Abfangen eines Telekommunikations-Signals geschaffen, das den Empfang eines Telekommunikations-Paketes, das ein vorgegebenes Kopffeld und Nutzdaten umfasst, das Entfernen des vorgegebenen Kopffeldes von dem Paket, das Replizieren der Nutzdaten, das Hinzufügen eines neuen Kopffeldes zu den replizierten Nutzdaten und das Lenken der replizierten Nutzdaten an die dem neuen Kopffeld zugeordnete Adresse einschließt. Es kann festgestellt werden, ob ein Telekommunikations-Paket zu überwachen ist. Das neue Kopffeld kann entweder dem vorgesehenen Empfänger oder einer Exekutivbehörde zugeordnet sein. Das vorgegebene Kopffeld kann durch ein zweites vorgegebenes Kopffeld ersetzt werden. Dieser Ersatz kann vor oder nach dem Replizieren der Nutzdaten erfolgen. Das zweite vorgegebene Kopffeld kann dem anderen von dem vorgesehenen Empfänger und der Exekutivbehörde zugeordnet werden. Die Nutzdaten können an die dem zweiten vorgegebenen Kopffeld zugeordnete Adresse gelenkt werden.

[0013] Bei einer weiteren Ausführungsform wird ein System zum Abfangen eines Telekommunikations-Signals geschaffen. Das System schließt einen auf ein Telekommunikations-Signal ansprechenden Audio-Server zum Empfang eines Telekommunikations-Paketes, das ein vorgegebenes Kopffeld und Nutzdaten umfasst, einen Abschluss- oder Zielpunkt zum Entfernen des vorgegebenen Kopffeldes von dem Paket, zum Replizieren der Nutzdaten und zum Hinzufügen eines neuen Kopffeldes zu den replizierten Nutzdaten, und einen Relais-Punkt zum Lenken der replizierten Nutzdaten an die dem neuen Kopffeld zugeordnete Adresse ein.

[0014] Das neue Kopffeld kann entweder dem vorgesehenen Empfänger oder einer Exekutivbehörde zugeordnet sein. Es kann eine Medien-Überleiteinrichtung zum Lenken des Telekommunikations-Signals an den Audio-Server und außerdem eine Medien-Überleiteinrichtungs-Steuerung vorgesehen sein, die auf die Medien-Überleiteinrichtung anspricht, um festzustellen, ob das Telekommunikations-Paket abzufangen ist. Die Medien-Überleiteinrichtung-Steuerung kann einen Anruf-Diskriminator einschließen, der auf das Telekommunikations-Signal anspricht, um festzustellen, dass das Telekommunikations-Signal einem Abfangen zu unterwerfen ist. Es kann einen zweiten Abschluss- oder Zielpunkt zum Hinzufügen eines zweiten vorgegebenen Kopffeldes zu den Nutzdaten geben. Das zweite vorgegebene Kopffeld kann dem anderen von dem vorgesehenen Empfänger und der Exekutivbehörde zugeordnet sein. Es kann einen zweiten Relais-Punkt zum Lenken der Nutzdaten an die dem zweiten vorgegebenen Kopffeld zugeordnete Adresse geben.

[0015] Bei einer weiteren Ausführungsform wird ein Verfahren zum Abfangen eines Telekommunikations-Signals durch Empfangen eines Telekommunikations-Paketes, das ein vorgegebenes Kopffeld und Nutzdaten umfasst, durch Entfernen des vorgegebenen Kopffeldes von dem Paket, durch Replizieren der Nutzdaten, durch Hinzufügen eines neuen Kopffeldes zu den replizierten Nutzdaten und zum Lenken der replizierten Nutzdaten an die Adresse umfasst, die dem neuen Kopffeld zugeordnet ist.

[0016] Es kann festgestellt werden, ob das Telekommunikations-Paket abzufangen ist. Das neue Kopffeld kann einem von einem vorgesehenen Empfänger und einer Exekutivbehörde zugeordnet sein. Das vorgegebene Kopffeld kann von den Nutzdaten entfernt und durch ein zweites vorgegebenes Kopffeld ersetzt werden. Dieser Ersatz kann vor oder nach dem Replizieren der Nutzdaten erfolgen. Das zweite vorgegebene Kopffeld kann dem anderen von dem vorgesehen Empfänger und der Exekutivbehörde zugeordnet sein. Die Nutzdaten können an die dem zweiten vorgegebenen Kopffeld zugeordnete Adresse gelenkt werden.

[0017] Es wird weiterhin ein Verfahren zum Umlenken eines Telekommunikations-Signals geschaffen. Das Verfahren schließt den Empfang eines ein Kopffeld und Nutzdaten umfassenden Telekommunikations-Paketes, das Entfernen des vorgegebenen Kopffeldes von dem Paket, das Hinzufügen eines zweiten vorgegebenen Kopffeldes zu den Nutzdaten und das Lenken der replizierten Nutzdaten an die dem zweiten vorgegebenen Kopffeld zugeordnete Adresse ein.

[0018] Es kann festgestellt werden, ob ein Telekommunikations-Paket umzulenken ist. Das zweite vorgegebene Kopffeld kann einen von dem vorgesehenen Empfänger und einer Exekutivbehörde zugeordnet werden. Die Nutzdaten können repliziert werden. Dieses Replizieren kann vor oder nach dem Entfernen des vorgegebenen Kopffeldes erfolgen. Ein neues Kopffeld kann zu den replizierten Nutzdaten hinzugefügt werden, und die replizierten Nutzdaten können an die Adresse gelenkt werden, die dem zweiten vorgegebenen Kopffeld zugeordnet ist. Das neue Kopffeld kann dem anderen von dem vorgesehenen Empfänger und der Exekutivbehörde zugeordnet sein.

[0019] Es wird weiterhin ein Verfahren zur Überwachung eines Telekommunikations-Signals zu oder von einer zu überwachenden Person von oder zu einem Partner geschaffen. Das Verfahren schließt die Feststellung, dass ein Telekommunikations-Signal zu überwachen ist, den Aufbau einer Verbindung zwischen einer ersten Überleiteinrichtung, die einem von der zu überwachenden Person und einem Partner zugeordnet ist, und einem ersten Abschluss- oder Zielpunkt, der eine zweite Überleiteinrichtung darstellt, die mit dem anderen von dem Partner und der zu überwachenden Person zugeordnet ist, den Aufbau einer Verbindung zwischen der zweiten Überleiteinrichtung und einen zweiten Abschluss- oder Zielpunkt, der die erste Überleiteinrichtung darstellt, und den Aufbau einer Verbindung zwischen dem ersten Ziel- oder Abschlusspunkt und dem zweiten Ziel- oder Abschlusspunkt zum Aufbau eines Trägerkanals zwischen der zu überwachenden Person und dem Partner ein, wobei die ersten und zweiten Überleiteinrichtungen in direkter Verbindung zu stehen scheinen.

[0020] Eine Verbindung kann von zumindest einem der ersten und zweiten Abschluss- oder Zielpunkte zu einer Überleiteinrichtung aufgebaut werden, die dem anderen von der zu überwachenden Person und dem Partner zugeordnet ist, und zwar gleichzeitig mit der Verbindung zwischen dem ersten Ziel- oder Abschlusspunkt und dem zweiten Ziel- oder Abschlusspunkt.

[0021] Es wird schließlich ein weiteres Verfahren zum Umlenken eines Telekommunikations-Signals, das für einen einer zu überwachenden Person und einen Partner bestimmt ist, durch Zuordnen eines ersten Ziel- oder Abschlusspunktes zu einem ersten vorgesehenen Ziel- oder Abschlusspunkt einer ersten Medien-Überleiteinrichtung, durch Zuordnen eines zweiten Ziel- oder Abschlusspunktes zu einem zweiten vorgesehenen Ziel- oder Abschlusspunkt einer zweiten Medien-Überleiteinrichtung, durch Aufbauen einer Verbindung zwischen dem ersten vorgesehenen Ziel- oder Abschlusspunkt und dem zweiten Ziel- oder Abschlusspunkt, durch Aufbauen einer Verbindung zwischen dem zweiten vorgesehenen Ziel- oder Abschlusspunkt und dem ersten Ziel- oder Abschlusspunkt, und durch Aufbauen einer Verbindung zwischen dem ersten Ziel- oder Abschlusspunkt und dem zweiten Ziel- oder Abschlusspunkt, wobei der erste vorgesehene Ziel- oder Abschlusspunkt und der zweite Ziel- oder Abschlusspunkt direkt miteinander verbunden zu sein scheinen.

Kurze Beschreibung der Zeichnungen

[0022] Fig. 1 ist eine schematische Blockdarstellung, die allgemein ein System zum Abfangen von Paket-Kommunikationen darstellt und einen zentralisierten Replikator gemäß der vorliegenden Erfindung einschließt;

[0023] Fig. 2 ist ein ausführlicheres Blockschaltbild ähnlich der Fig. 1, das eine Medien-Überleiteinrichtungs-Steuerung einschließt, die jeder Medien-Überleiteinrichtung zugeordnet ist, um die notwendigen Verbindungen zum Bewirken eines Abfangens von Paket-Kommunikationen zu implementieren;

[0024] Fig. 3 ist ein schematisches Blockschaltbild ähnlich der Fig. 1, das die tatsächlichen und vorübergehenden Verbindungen beim Implementieren eines Anruf-Abfangens gemäß einem Gesichtspunkt der vorliegenden Erfindung zeigt;

[0025] Fig. 4 ist ein schematisches Blockschaltbild, das zugehörige Verbindungen im Inneren des zentralisierten Replikators zum Durchführen einer Trägerkanal-Tandembildung zum Abfangen von Paket-Kommunikationen zeigt;

[0026] Fig. 5 ist ein schematisches Blockschaltbild, das eine Trägerkanal-Tandembildung durch den Anruf-Diskriminator als Antwort auf eine Notwendigkeit zum Abfallen von Paket-Kommunikationen darstellt;

[0027] Fig. 6 ist ein Ablaufdiagramm, das ein Verfahren zum Abfangen von Paket-Kommunikationen gemäß der vorliegenden Erfindung zeigt;

[0028] Fig. 7 ist ein schematisches Blockschaltbild ähnlich der Fig. 2, in der ein zweiter Partner einen Anruf zu einer überwachten Person aufbaut und ein Anruf-Anklopf-Merkmal aufgerufen wird;

[0029] Fig. 8 ist ein schematisches Blockschaltbild ähnlich der Fig. 4, das die Verbindungs-Topologie innerhalb des zentralisierten Replikators zeigt, wenn das Anruf-Anklopf-Merkmal aufgerufen wird; und

[0030] Fig. 9 ist ein schematisches Blockschaltbild ähnlich der Fig. 8, das die Verbindungs-Topologie in dem zentralisierten Replikator zeigt, wenn ein Konferenzgespräch-Merkmal aufgerufen wird.

Ausführliche Beschreibung

[0031] Gemäß der vorliegenden Erfindung wird allgemein ein System **10**, Fig. 1, geschaffen, das ein Paket-Telekommunikations-Signal zu oder von einer überwachten Person **12** abfangen oder anhören kann, beispielsweise durch eine Exekutivbehörde (LEA) **14**. Es gibt eine erste oder Teilnehmer-Medien-Überleiteinrichtung **16**, die einem Teilnehmer oder einer Person **12** zugeordnet ist, der bzw. die überwacht wird, und eine zweite oder Partner-Medien-Überleiteinrichtung **18**, die einem Partner **20** zugeordnet ist, der den Teilnehmer anruft oder von diesem angerufen wird. Es kann weiterhin eine drahtlose Partner-Medien-Überleiteinrichtung **18'** geben, wenn ein Partner **20'** mit dem Teilnehmer **12** über ein drahtloses Telefon kommuniziert.

[0032] Ein Anruf wird zwischen dem Teilnehmer **12** und dem Partner **20** aufgebaut. Es wird festgestellt, dass das Telekommunikations-Signal ein für eine Überwachung ausgewähltes Telekommunikations-Signal ist und abzufangen ist. Entsprechend wird für einen Anruf von dem Partner **20** an den Teilnehmer **18** das Telekommunikations-Signal statt direkt der vorgesehenen Partner-Medien-Überleiteinrichtung **18** zugesandt zu werden, von der Teilnehmer-Medien-Überleiteinrichtung **16** an einen zentralisierten Replikator **22** umgelenkt, der beispielsweise einen universellen Audio-Server umfassen kann, der der LEA **14** zugeordnet ist. Wenn der zentralisierte Replikator **22** das Telekommunikations-Signal empfängt, das aus einzelnen Paketen besteht, wobei jedes Paket ein Kopffeld und Nutzdaten einschließt, so entfernt der zentralisierte Replikator **22** das Kopffeld von dem Paket, wobei die Nutzdaten intakt bleiben. Der zentralisierte Replikator **22** repliziert die Nutzdaten, fügt ein Kopffeld zu den replizierten Nutzdaten hinzu und sendet die replizierten Nutzdaten an eine Exekutivbehörden-Überleiteinrichtung **24**. Sobald die Nutzdaten repliziert wurden, wird ein Kopffeld zu den ursprünglichen Nutzdaten hinzugefügt, und dieses Paket wird von dem zentralisierten Replikator **22** an die Partner-Medien-Überleiteinrichtung **18/18'** zur Zustellung an den Partner **20/20'** erneut ausgesandt.

[0033] Alternativ kann das gesamte ankommende Paket unter Einschluss des Kopffeldes und der Nutzdaten repliziert werden. Sobald das Paket repliziert wurde, werden die Kopffelder der ursprünglichen und replizierten Pakete entfernt. Ein neues Kopffeld wird zu den replizierten Nutzdaten zur Zustellung an die Exekutivbehörde **14** hinzugefügt, und ein neues Kopffeld wird zu den ursprünglichen Nutzdaten zur Zustellung an den jeweiligen vorgesehenen Empfänger, den Teilnehmer **12** oder den Partner **20**, hinzugefügt.

[0034] Es wird nunmehr auf die Fig. 2 Bezug genommen, aus der zu erkennen ist, dass jeder Medien-Überleiteinrichtung **16**, **24** und **18** eine Medien-Überleiteinrichtungs-Steuerung **26**, **28** bzw. **30** zugeordnet sein kann. Wie der Begriff hier verwendet wird, bezieht sich eine Medien-Überleiteinrichtungs-Steuerung auf eine oder mehrere Geräte, deren Funktionalität die Durchführung von Medien-Überleiteinrichtungs-Steuer-, Signalisierungs- und Anruf-Verarbeitungs-Funktionen einschließen kann. Jede zugehörige Überleiteinrichtungs-Steuerung kann einen Anruf-Diskriminator **32** einschließen, der Anruf-Verarbeitungs-Software umfasst, die feststellt, ob ein Anruf von oder zwischen zugehörigen Überleiteinrichtungen, beispielsweise der Teilnehmer-Medien-Überleiteinrichtung **16** zu der Partner-Medien-Überleiteinrichtung **18**, tatsächlich einer Überwachung unterworfen ist. Es kann in dem Diskriminator **32** beispielsweise eine Datenbank für ein gesetzeskonformes Abfangen oder Abhören enthalten sein, die Teilnehmer, beispielsweise den Teilnehmer **12** identifiziert, die Gegenstand einer Überwachungs-Anordnung sind.

[0035] Sobald festgestellt wurde, dass der Anruf einer Überwachung unterworfen ist, sendet die Medien-Überleiteinrichtungs-Steuerung **26** eine erste Nachricht, beispielsweise unter Verwendung des Medien-Überleiteinrichtungs-Steuerprotokolls (MGCP) oder des H.248-Protokolls, an die LEA-Medien-Überleiteinrichtung **28**, um eine Verbindung zwischen der Teilnehmer-Medien-Überleiteinrichtung **16** und dem zentralisierten Replikator **22** herzustellen, und eine weitere Nachricht zum Herstellen einer Verbindung zwischen der Partner-Medien-Überleiteinrichtung **18** und dem zentralisierten Replikator **22**. Die Umlenkung des Anrufs durch den zentralisierten Replikator **22** ist für die Anruf-Bearbeitungs- und Dienste-Funktionen transparent, und der Anruf erscheint so, als ob er normal aufgebaut sein würde, das heißt als ob die Teilnehmer-Medien-Überleiteinrichtung **16** und Partner-Medien-Überleiteinrichtung **18** direkt verbunden sein würden. Das vorstehende Beispiel nimmt an, dass der Teilnehmer **12** und der Partner **20** eine Überleiteinrichtung nicht gemeinsam nutzen. Eine gemeinsam genutzte Überleiteinrichtung würde jedoch die Betriebsweise der vorliegenden Erfindung nicht ändern, weil die Feststellung und die Paket-Replikation in der gleichen für den Anrufer transparenten Weise erfolgen würde.

[0036] Die LEA-Medien-Überleiteinrichtungs-Steu-

erung **28** bewirkt ein Umlenken des Anrufes von dem vorgesehenen Empfänger, und liefert Befehle an den zentralisierten Replikator **22** dafür, dass dieser interne Verbindungen, die als eine Trägerkanal-Tandembildung bezeichnet werden, herstellt, um die Paket-Replikation zu ermöglichen, wie dies weiter anhand der Fig. 4 erläutert wird. Sobald die Medien-Überleiteinrichtungs-Steuerung **28** die erforderlichen Verbindungen zwischen der Teilnehmer-Medien-Überleiteinrichtung **16**, dem zentralisierten Replikator **22** und der Partner-Medien-Überleiteinrichtung **18** hergestellt hat, leitet die Medien-Überleiteinrichtungs-Steuerung **28** die Verbindungen zwischen dem zentralisierten Replikator **22** und der Exekutivbehörden-Medien-Überleiteinrichtung **24** ein, die dann mit der LEA **14** verbunden wird.

[0037] Entsprechend wird ein einer Überwachung unterworfener Anruf Pakete enthalten, deren Kopffelder geändert oder ersetzt wurden, derart, dass anstelle einer Übermittlung der Pakete direkt zu und von den Überleiteinrichtungen **16** und **18** (den vorgesehenen Empfängern), die Pakete zu dem zentralisierten Replikator **22** zur Replikation umgelenkt werden. Die Medien-Überleiteinrichtungs-Steuerung **28** ändert die Adresseninformation der Nachrichten derart, dass es der Teilnehmer-Medien-Überleiteinrichtung **16** so erscheint, dass die Nachricht von der Partner-Medien-Überleiteinrichtung **18** kommt, und Nachrichten, die an die Partner-Medien-Überleiteinrichtung **18** gesandt werden, scheinen von der Teilnehmer-Medien-Überleiteinrichtung **16** zu kommen.

[0038] Wie dies in Fig. 3 gezeigt ist, sendet die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** eine Nachricht **27** mit der Sitzungs-Beschreibungs-Information, beispielsweise unter Verwendung eines Protokolls, wie z. B. des Sitzungs-Beschreibungs-Protokolls (SDP) der Teilnehmer-Medien-Überleiteinrichtung **16** an die LEA-Medien-Überleiteinrichtungs-Steuerung **28**. Die Medien-Überleiteinrichtungs-Steuerung **28** sendet eine Nachricht **29** unter Einschluss der Sitzungsinformation der Medien-Überleiteinrichtung **16** an die zugehörige Medien-Überleiteinrichtungs-Steuerung **30**, jedoch mit der Adresse des zentralisierten Replikators **22**.

[0039] In ähnlicher Weise sendet die Partner-Medien-Überleiteinrichtungs-Steuerung **30** eine Nachricht **31**, die die Sitzungs-Beschreibung der Medien-Überleiteinrichtung **16** bestätigt, mit der Sitzungs-Beschreibung der Partner-Medien-Überleiteinrichtung **18**. Die LEA-Medien-Überleiteinrichtungs-Steuerung **28** sendet eine Nachricht **33**, die die Sitzungs-Beschreibung der Teilnehmer-Medien-Überleiteinrichtung **16** bestätigt, mit der Sitzungs-Beschreibung der Partner-Medien-Überleiteinrichtung **18**, jedoch mit der Adresse des zentralisierten Replikators **22**.

[0040] Entsprechend verläuft ein Kommunikationspfad von der Teilnehmer-Medien-Überleiteinrichtung **16** zu der Partner-Medien-Überleiteinrichtung **18** im Tandem durch den zentralisierten Replikator **22**, ist jedoch transparent für den Teilnehmer **12** oder den Partner **30**.

[0041] Fig. 4 zeigt weiterhin, wie die Trägerkanal-Tandembildung über den zentralisierten Replikator **22** durch Modifizieren der Zuordnung zwischen Paketströmen und Endpunkten bewirkt werden kann, um die Verbindungen und Darstellungen zu bewirken, die in Fig. 3 gezeigt sind.

[0042] Paketströme **34**, **36**, **38** und **40** gehen von den zugehörigen Endpunkten **42**, **44**, **46** bzw. **48** aus. Entsprechend sind die jeweiligen Sende- und Empfangs-Ströme **34/36** des Endpunktes **32** dem Endpunkt **44** innerhalb des zentralisierten Replikators **22** zugeordnet, obwohl sie dem Endpunkt **46** (Partner-Medien-Überleiteinrichtung **18**) zugeordnet zu sein scheinen. In ähnlicher Weise sind jeweilige Sende- und Empfangs-Ströme **38/40** des Endpunktes **46** dem Endpunkt **48** zugeordnet, obwohl sie dem Endpunkt **42** (Teilnehmer-Medien-Überleiteinrichtung **16**) zugeordnet zu sein scheinen. Schließlich sind die internen Ströme **50** und **52** den Endpunkten **44** und **48** zugeordnet. Verbindungen zu den Endpunkten **42**, **44**, **46** und **48** werden von der Medien-Überleiteinrichtungs-Steuerung **28** (Fig. 3) eingeleitet, wobei die Endpunkte **42** und **46** die erkannten Ursprungs- und Ziel-Endpunkte sind.

[0043] Die Endpunkte **42** und **46** sind typischerweise so konfiguriert, dass sie die TDM-Information von dem Teilnehmer **12** oder dem Partner **20** in beispielsweise IP- oder ATM-Pakete oder Zellen umwandeln, in Abhängigkeit von der Struktur des zentralisierten Replikators **22**. In ähnlicher Weise wird an diesen Endpunkten von dem zentralisierten Replikator **22** empfangene Information von IP/ATM auf TDM umgewandelt. Im Gegensatz hierzu sind die Endpunkte **44** und **48** in dem zentralisierten Replikator **22** lediglich als Paket-Relais-Punkte konfiguriert und ergeben keine Transcodierungs- oder Jitter-Korrektur, um die Latenz zu einem Minimum zu machen und um die Gefahr einer Entdeckung der Überwachung durch den Teilnehmer **12** oder den Partner **20** zu verringern. Datenstrom-Steuerpuffer (nicht gezeigt) können zur Vermeidung eines Paketverlustes vorgesehen sein.

[0044] Die Paket-Relais-Endpunkte **44** bzw. **48** streifen das Kopffeld von ankommenden Paketströmen **34** und **38**, die sie von jeweiligen Endpunkten **42** und **46** empfangen, ab, sie replizieren die Nutzdaten, sie fügen ein neues Kopffeld zu den replizierten Nutzdaten hinzu, und sie senden die replizierten Paket-Datenströme **54** und **56** an die Exekutivbehörden-Überleiteinrichtung **24** über Endpunkte **58** und **60**. Die Paket-Relais-Endpunkte **44** und **48** senden die ursprünglichen Nutzdaten außerdem über die Da-

tenströme **50** bzw. **52** zueinander, wobei neue Kopffelder hinzugefügt werden, die die Pakete an jeweilige Überleiteinrichtungen **16** und **18** lenken. Entsprechend kann das gesamte Paket repliziert werden, worauf die replizierten Kopffelder abgestreift werden und neue Kopffelder hinzugefügt werden, um die replizierten Pakete an ihre jeweiligen Überleiteinrichtungen zu lenken.

[0045] Um eine Transparenz für den Teilnehmer **12** und den Partner **20** des Abfangvorganges sicherzustellen, sollten die für die Exekutivbehörde **14** bestimmten Datenströme **54** und **56** einseitig gerichtet sein. Entsprechend sollten die Endpunkte **58** und **60** so konfiguriert sein, dass sie lediglich in Richtung auf die Exekutivbehörden-Überleiteinrichtung **24** senden. Die Endpunkte **58** und **60** sollten von dem gleichen Ressourcen-Pool wie die Endpunkte **44** und **48** sein, so dass die Ressourcen-Pools wiedergeben, welche Endpunkte innerhalb des zentralisierten Replikators **22** interne Verbindungen zwischen sich aufweisen, so dass die Medien-Überleiteinrichtungs-Steuerung **28** die geeigneten Verbindungsmöglichkeits-Nachrichten an den zentralisierten Replikator **22** senden. Entsprechend ist eine Ressourcen-Verwaltung **62** vorgesehen. Weiterhin sollten die Endpunkte **58** und **60** ebenso wie die Paket-Relais-Endpunkte **44** und **48** eine Übertragungszeit zwischen Endpunkten erzielen, die eine niedrige Latenz aufrechterhält, so dass die Gesamt-Umlauf-Verzögerung der Pakete unter Einschluss der Zeit zum Durchqueren des zentralisierten Replikators **22** den konstruktiv bedingten Schwellenwert der Echo-Kompensationseinrichtungen der jeweiligen Medien-Überleiteinrichtungen nicht übersteigt.

[0046] Die Ressourcen-Verwaltung **62** führt mehrere grundlegende Funktionen unter Einschluss der Zuteilung von Ressourcen, der Rückgabe der Ressourcen an einen freien Pool und des Berichts über die Ressourcen aus. Die Ressourcen-Verwaltung **62** kann eine Schnittstelle für Betriebspersonal ergeben, um anzuzeigen, welche Ressourcen in dem zentralisierten Replikator **22** für die Trägerkanal-Tandembildung zu verwenden sind. Die Verbindung zu der Exekutivbehörde **14** kann in verschiedenen Formen erfolgen, unter Einschluss von dedizierten Leitungen, vermittelten örtlichen Verbindungsstrecken, dedizierten Bündelleitungen oder vermittelten Fern-Verbindungsstrecken, ohne von dem Schutzumfang der Erfindung abzuweichen.

[0047] Ein Überwachungspunkt **64** in der Exekutivbehörde **14**, der ein Audio-Gerät einschließen kann, kann den Anruf-Inhalt über eine multiplexierte TDM-Misch-Brücke **66** empfangen. Der Überwachungspunkt **64** empfängt den Anruf-Inhalt in Echtzeit, so dass zur gleichen Zeit wie der Teilnehmer **12** den Rufton von dem Partner **20** hört, die Exekutivbehörde **14** ebenfalls den Rufton hört. Wie dies für den Fachmann zu erkennen ist, sollte die Exekutivbehörden-Überleiteinrichtung **24** in der Lage sein, alle möglichen CODEC's zu unterstützen, die zwischen einem Teilnehmer **12** und einem Partner **20** ausgehandelt werden können.

[0048] Obwohl das System **10** so beschrieben wurde, als ob es lediglich eine einzige Replikation für eine einzige Exekutivbehörde ausführt, sollte es verständlich sein, dass dies keine Beschränkung der vorliegenden Erfindung ist, weil die ankommenden Paket-Datenströme an den Endpunkten **44** und **48** mehrmals repliziert werden können, in Abhängigkeit von der Anzahl von Exekutivbehörden, die den Teilnehmer **12** überwachen, indem die die Endpunkte **44** und **48** bildende Hardware für mehrfache Replikationen konfiguriert wird.

[0049] Trotz der Änderungen in den Verbindungs-Nachrichten, wie sie vorstehend beschrieben wurden, wird weder dem Teilnehmer **12** noch dem Partner **20** eine Anzeige dafür geliefert, dass der Anruf über den zentralisierten Replikator **22** umgelenkt wird.

[0050] Wenn festgestellt wird, dass ein Anruf zu überwachen ist, kann die Standard-Verbindungsmöglichkeits-Nachricht von dem Anruf-Server entweder geändert werden, um die geeignete Verbindung auszuführen, oder die Nachricht kann in mehrfache Nachrichten aufgeteilt werden, um die angeforderte Verbindung auszuführen.

[0051] Beispielsweise wird die Verbindungs-Operation von dem Anruf-Server, der eine Verbindung zwischen dem Teilnehmer **12** und dem Partner **20** anfordert, in drei getrennte Verbindungsmöglichkeits-Operationen modifiziert. Dies erfolgt durch Anfordern getrennter Verbindungen von den Endpunkten **42** und **44**, von den Endpunkten **44** und **48** und von den Endpunkten **44** bis **48**.

[0052] Wie dies in Fig. 5 gezeigt ist, gibt ein Anruf-Agent oder eine Anruf-Verarbeitung **68** als Antwort auf die elektronische Überwachungs-Software **69** eine Verbindungsfähigkeits- oder Konnektivitäts-Nachricht **70** an den Anruf-Diskriminator **32** ab, um eine Teilnehmer-zu-Partner-Verbindung von einer Diskriminator-Ebene in der Konnektivitäts-Software **72** zu einer Trägerkanal-Tandembildungs-Konnektivitäts-Software **74** herzustellen, die drei getrennte Medien-Überleiteinrichtungs-Steuernachrichten abgibt. Eine erste Nachricht **76** kann eine Verbindung von der Teilnehmer-Medien-Überleiteinrichtung **16** (Fig. 4) zu dem zentralisierten Replikator **22** einleiten. Eine zweite Nachricht **78** kann eine Verbindung von der Partner-Medien-Überleiteinrichtung (**18**) zu dem zentralisierten Replikator **22** einleiten. Eine dritte Nachricht **80** kann einen Befehl an den zentralisierten Replikator **22** liefern, um eine interne Zuordnung

zwischen dem zentralisierten Replikator **22** zu der Verbindung für die Teilnehmer-Medien-Überleiteinrichtung **16** und dem zentralisierten Replikator **22** zur Verbindung der Partner-Medien-Überleiteinrichtung **18** herzustellen.

[0053] Sobald die zugehörige Verbindung zwischen dem Teilnehmer **12** und dem Partner **20** konfiguriert wurde, leitet die Medien-Überleiteinrichtungs-Steuerung **28** (Fig. 3) die jeweiligen Verbindungen zu der Exekutiv-Medien-Überleiteinrichtung **24** dadurch ein, dass zwei Verbindungen von den Endpunkten **44** nach **58** und **48** nach **60** (Fig. 4) in dem zentralisierten Replikator **22** zu der Exekutiv-Medien-Überleiteinrichtung **24** angefordert werden, wobei die Endpunkte **58** und **60** mit der Exekutiv-Medien-Überleiteinrichtung **24** verbunden sind, wie dies in der vorstehenden Fig. 4 gezeigt ist.

[0054] Ein Ablaufdiagramm der vorliegenden Erfindung ist in Fig. 6 dargestellt. Ein Anruf wird zwischen einem Teilnehmer und einem Partner eingeleitet, Block **82**. Die Medien-Überleiteinrichtungs-Steuerung, die dem überwachten Teilnehmer zugeordnet ist, stellt fest, dass der Anruf zu überwachen ist, Block **84**, und lenkt den Anruf an die Medien-Überleiteinrichtungs-Steuerung der LEA durch Zuordnen der LEA-Medien-Überleiteinrichtung zu der Ziel-(Partner-)Medien-Überleiteinrichtung um, Block **86**. Die Medien-Überleiteinrichtungs-Steuerung, die der Exekutivbehörde zugeordnet ist, führt eine Kanal-Tandembildung durch Zuordnen der Endpunkte der Teilnehmer- und Partner-Medien-Überleiteinrichtungen zu Endpunkten in dem zentralisierten Replikator aus, Block **88**.

[0055] Nachdem die Tandembildung des Trägerkanals durchgeführt wurde, werden Pakete zu und von dem Teilnehmer zu dem zentralisierten Replikator umgelenkt, Block **90**, wo die Nutzdaten repliziert werden, Block **92**, und neue Kopffelder sowohl zu den replizierten Nutzdaten als auch zu den ursprünglichen Nutzdaten hinzugefügt werden, Block **94**. Die jeweiligen Nutzdaten werden dann an den vorgesehenen Empfänger, den Teilnehmer oder den Partner, und die LEA gesendet, Block **96**.

[0056] Fig. 7 stellt allgemein die Situation dar, bei der ein Anklopf- oder Anruf-Wartet-Merkmal aufgerufen wird. Zu Erläuterungszwecken wird jeder Agent durch eine andere Medien-Überleiteinrichtungs-Steuerung mit Diensten versorgt. Ein Anruf wird zwischen dem Teilnehmer **12** und einem ersten Partner **20** aufgebaut, wie dies weiter oben erläutert wurde, bis der Teilnehmer **12** und der erste Partner **20** in den Gesprächszustand eintreten, wie dies vorstehend erläutert wurde, wobei die Exekutivbehörde **14** den Anruf-Inhalt empfängt.

[0057] Ein zweiter Partner **20'** führt einen Anruf an den Teilnehmer **12** aus. Die Partner-Medien-Überleiteinrichtungs-Steuerung **30'** führt eine Anruf-Verarbeitung aus, die den Anruf an die Teilnehmer-Medien-Überleiteinrichtung **16** lenkt, und es wird festgestellt, dass der Anruf einem Abfangen oder einem Abhören unterworfen ist. Der zentralisierte Replikator **22** erkennt, dass der Teilnehmer **12** mit einem vorhandenen Anruf beschäftigt und besetzt ist. Die LEA-Medien-Überleiteinrichtungs-Steuerung **28** liefert einen Befehl an die Medien-Überleiteinrichtung **16** für das Abspielen eines Anklopf- oder Anruf-Wartet-Tons für den Teilnehmer **12**.

[0058] Es wird nunmehr auf die Fig. 8 Bezug genommen, in der gezeigt ist, dass der Teilnehmer **12** ein Sondermerkmal aufruft, um den Anruf anzunehmen, der von dem zweiten Teilnehmer **20'** ausgeht. Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** (Fig. 7) liefert einen Befehl an den zentralisierten Replikator **22** zum Unterbrechen der Verbindung zwischen dem Teilnehmer **12** und dem ersten Partner **20**. Die Tandembildungs-Konnektivitäts-Software **74** (Fig. 5) fängt jedoch diese Nachricht ab und ändert sie so, dass lediglich die Verbindung zwischen den Endpunkten **42** und **44** (gestrichelt gezeigt) unterbrochen wird. Die elektronische Überwachungs-Software **69** (Fig. 5) liefert weiterhin Anweisungen für ein Unterbrechen der Verbindungen mit der LEA **14**, so dass die Verbindungen zwischen den Endpunkten **44** und **58** und **48** und **60** unterbrochen werden (gestrichelt gezeigt), dass jedoch die Verbindung zwischen den Endpunkten **44** und **48** und **48** und **46** intakt bleibt.

[0059] Die Tandembildungs-Konnektivitäts-Software **74** gewinnt zwei weitere Endpunkte **44'** und **48'** von der Ressourcen-Verwaltung **62**, um den Anruf zwischen dem Teilnehmer **12**, dem zweiten Partner **20'** und der LEA **14** in Tandem weiterzuleiten. Die Tandembildungs-Konnektivitäts-Software **74** leitet eine Verbindung zwischen den Endpunkten **42** und **44'** ein. Die Tandembildungs-Konnektivitäts-Software **74** leitet weiterhin eine Verbindung zwischen den Endpunkten **44'** und **48'** innerhalb des zentralisierten Replikators ein. Die Sitzungs-Beschreibungs-Information der Endpunkte **42** und **44'** wird ausgetauscht, und die Sitzungs-Beschreibungs-Information von **44'** und **48'** wird ausgetauscht, um den Aufbau des Trägerkanals zu ermöglichen.

[0060] Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** bestätigt den Endpunkt **46'** und antwortet mit einer Sitzungs-Information des Endpunktes **48'**, um die Fertigstellung der Trägerkanal-Konfiguration zu ermöglichen.

[0061] An dieser Stelle ist ein Trägerkanal zwischen den Endpunkten **42** und **44'**, **44'** und **48'** und **48'** und **46'** konfiguriert. Der Teilnehmer **12** und der zweite Partner **20'** treten nunmehr in den Gesprächszustand

ein, wobei die Exekutivbehörde **14** den Anruf-Inhalt empfängt. Der zweite Partner **20'** beendet den Anruf und der Teilnehmer **12** ruft ein Sondermerkmal auf, um zu dem ersten Partner zurückzukehren. Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** sendet eine Nachricht zum Unterbrechen der Verbindung zwischen dem Teilnehmer **12**, und die Nachricht wird abgefangen und so geändert, dass sie lediglich die Verbindung zwischen den Endpunkten **42** und **44'** unterbricht. Die Verbindung mit der Exekutivbehörde **14** wird ebenfalls unterbrochen, doch bleiben die Verbindungen zwischen den Endpunkten **44'** und **48'** und **48'** und **46'** intakt. Die Medien-Überleiteinrichtungs-Steuerung **30'** des Partners (nicht gezeigt) leitet eine Auslöse-Vorwärts-Nachricht an die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26**, die Anweisungen an die Konnektivität gibt, die Verbindung mit dem zweiten Partner **20'** zu unterbrechen. Die Tandembildungs-Konnektivitäts-Software **74** (Fig. 5) fängt die Nachricht ab und liefert bei der Feststellung, dass der andere externe Agent aus dem Trägerkanal-Tandem entfernt wurde, einen Befehl zur Unterbrechung der Verbindungen zwischen den Endpunkten **44'** und **48'** und **48'** und **46'**.

[0062] Die Endpunkte **44'** und **46'** werden an die Ressourcen-Verwaltung **62** zurückgegeben, so dass sie in den freien Pool neu eingeführt werden können. Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** (Fig. 7) sendet eine Nachricht zur Wiederherstellung einer Verbindung zwischen dem Teilnehmer **12** und dem ersten Partner **20**. Die Tandembildungs-Konnektivitäts-Software **74** (Fig. 5) fängt diese Nachricht ab, stellt fest, dass die vorgegebene Kommunikation bereits einer Tandem-Verbindung zugeordnet ist und gewinnt die verwendeten Endpunkte zurück, und sie liefert Konnektivitäts-Nachrichten zur Wiederherstellung der Verbindung zwischen den Endpunkten **42** und **44**.

[0063] Die Sitzungs-Information der Endpunkte **42** und **44** wird ausgetauscht, wie dies weiter oben erläutert wurde, wodurch das Trägerkanal-Tandem fertiggestellt wird. Die elektronische Überwachungs-Software **69** (Fig. 5) fordert eine Benachrichtigung an, dass die Endpunkte zur Tandembildung des Trägerkanals durch den zentralisierten Replikator **22** verwendet werden. Die Endpunkte **58** und **60** werden dann mit der LEA-Medien-Überleiteinrichtung **24** verbunden, um ein Abfangen oder Abhören des Anruf-Inhaltes zu liefern. Der Teilnehmer **12** und der Partner **20** stehen wieder in einem Gesprächsverbindungs-Zustand über den Trägerkanal, der über die Endpunkte **42** und **44**, **44** und **48** und **48** und **46** aufgebaut wurde.

[0064] Unter erneuter Bezugnahme auf Fig. 7 wird ein Konferenzgespräch-Merkmal in einer Weise ähnlich dem Anklopfen ausgebildet. Ein Anruf zwischen dem Teilnehmer **12** und dem ersten Partner **20** wird aufgebaut. Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** stellt fest, dass der Anruf einer Überwachung unterworfen ist, und eine Trägerkanal-Tandembildung wird eingeleitet, die die Teilnehmer-Medien-Überleiteinrichtung **16** und die Partner-Medien-Überleiteinrichtung **18** über den zentralisierten Replikator **22** durch die LEA-Medien-Überleiteinrichtung **26** einleitet, wie dies weiter oben erläutert wurde, wobei jeweilige Endpunkte in dem zentralisierten Replikator **22** der Teilnehmer-Medien-Überleiteinrichtung **16** und der Partner-Medien-Überleiteinrichtung **18** zugeordnet werden. Eine Verbindung wird dann zwischen den Endpunkten in dem zentralisierten Replikator **22** eingeleitet.

[0065] Die Partner-Medien-Überleiteinrichtung **18** bestätigt den zugehörigen Endpunkt innerhalb des zentralisierten Replikators **22** so, als ob sie die Teilnehmer-Medien-Überleiteinrichtung **16** bestätigen würde, wie dies weiter oben anhand der Fig. 3 erläutert wurde, und anwortet mit der Sitzungs-Beschreibungs-Information der Partner-Medien-Überleiteinrichtung **18**, und ein Trägerkanal wird zwischen den Endpunkten **42**, **44**, **46** und **48** konfiguriert (Fig. 4).

[0066] Eine Verbindung zwischen der Exekutivbehörden-Überleiteinrichtung **24** und den Endpunkten innerhalb des zentralisierten Replikators **22** wird aufgebaut, wie dies weiter oben anhand der Fig. 4 beschrieben wurde. Der Teilnehmer **12** und der Partner **20** treten nunmehr in einen Gesprächszustand ein, und die Exekutivbehörde **14** empfängt die replizierten Paket-Datenströme und überwacht den Anruf.

[0067] Unter erneuter Bezugnahme auf Fig. 8 ist zu erkennen, dass der Teilnehmer **12** ein Sondermerkmal aufrufen kann und einen Anruf an einen zweiten Partner **20'** aufbauen oder von diesem empfangen kann. Die Teilnehmer-Medien-Überleiteinrichtungs-Steuerung **26** (Fig. 7) empfängt eine Nachricht von dem Anruf-Agenten des Teilnehmers **12** zum Unterbrechen der Verbindung mit dem ersten Teilnehmer **20**, die aufgrund der Trägerkanal-Tandembildung abgefangen wird, und die Medien-Überleiteinrichtungs-Steuerung **28** sendet eine modifizierte Nachricht an den zentralisierten Replikator **22** (statt an die Partner-Medien-Überleiteinrichtung **18**) zum Unterbrechen der Konnektivität der Endpunkte **42** und **44** (gestrichelt gezeigt). Die elektronische Überwachungs-Software **69** (Fig. 5) fordert weiterhin die Unterbrechung der Verbindungen mit der LEA **14** an, und somit werden die Verbindungen zwischen dem Endpunkt **44** und **58** und **48** und **60** unterbrochen (gestrichelt gezeigt), doch bleibt die Verbindung zwischen den Endpunkten **44** und **48** und **48** und **46** vorübergehend intakt.

[0068] Hinsichtlich des neuen Anrufers stellt die Medien-Überleiteinrichtung fest, dass der Anruf einer Überwachung unterworfen ist, und es werden zwei

weitere Endpunkte **44'** und **48'** in dem zentralisierten Replikator **22** von der Ressourcen-Verwaltung **62** zugeteilt und konfiguriert, um die Tandembildung des Anrufs an den zweiten Partner **20'** zu bewirken. Eine Verbindung wird dann zwischen den Endpunkten **42** und **44'** eingeleitet, und die Medien-Überleiteinrichtungs-Steuerung **28** leitet den Endpunkt von **48'** an die Medien-Überleiteinrichtungs-Steuerung **30'**, die dem zweiten Partner **20'** zugeordnet ist. Eine Verbindung wird dann zwischen **44'** und **48'** innerhalb des zentralisierten Replikators **22** eingeleitet. Die Sitzungs-Beschreibungs-Information von **42** und **44'** werden ausgetauscht, und die Sitzungs-Beschreibungs-Information von **44'** und **48'** wird ausgetauscht, um den Aufbau der Trägerkanal-Tandembildung zu ermöglichen.

[0069] An diesem Punkt wird ein Trägerkanal zwischen **42** und **44'**, **44'** und **48'** und **48'** und **46'** konfiguriert. Eine Verbindung wird dann von dem zentralisierten Replikator **22** an die LEA **14** über die Endpunkte **44'** und **58'** und **48'** und **60'** eingeleitet. Der Teilnehmer **12** kann nunmehr mit dem zweiten Partner **20'** sprechen, und die LEA **14** kann den Inhalt abfangen oder abhören. Der Teilnehmer ruft dann das Sondermerkmal auf, um den ersten Partner **20** in einen Zweiweg-Gespräch einzubinden. Die Konnektivitäts-Software (Fig. 5) fordert an, dass alle Verbindungen, die mit den früheren Zweigen verbunden waren, unterbrochen werden (gestrichelt gezeigt), um das Dreiweg-Gespräch zu ermöglichen. Entsprechend werden die Verbindungen der Endpunkte **44** und **48**, **48** und **46** und **44'** und **48'** und **48'** und **46'** zusammen mit der entsprechenden LEA-Verbindung unterbrochen, und alle Ressourcen werden an den Ressourcen-Pool zurückgegeben. Die Medien-Überleiteinrichtungs-Steuerung **28** fordert eine Verbindung zwischen dem Teilnehmer **12**, dem ersten Partner **20** und dem zweiten Partner **20'** über die Konferenz-Ports **98**, **100** und **102** an, wie dies in Fig. 9 gezeigt ist.

Patentansprüche

1. Verfahren zum Abfangen eines Telekommunikationssignals, das zwischen einer ersten Medien-Überleiteinrichtung (**16**, **18**) und einer zweiten Medien-Überleiteinrichtung (**16**, **18**) in einem Netzwerk übertragen wird, wobei das Verfahren Folgendes umfasst:
(a) Empfangen eines Telekommunikations-Paketes von der ersten Medien-Überleiteinrichtung (**16**, **18**), das ein vorgegebenes Kopffeld und eine Nutzinformation enthält;
(b) Entfernen des vorgegebenen Kopffeldes von dem Paket;
(c) Replizieren der Nutzinformation;
(d) Hinzufügen eines neuen Kopffeldes zu der replizierten Nutzinformation; und
(e) Lenken der replizierten Nutzinformation an die Adresse, die dem neuen Ziel-Kopffeld zugeordnet ist, und gekennzeichnet durch:
(f) Hinzufügen eines geänderten vorgegebenen Kopffeldes oder Ersatz-Kopffeldes zu dem Telekommunikations-Paket oder der replizierten Nutzinformation, und Lenken des Paketes oder der Nutzinformation an die zweite Medien-Überleiteinrichtung, wobei das geänderte vorgegebene Kopffeld oder Ersatz-Kopffeld eine Adresseninformation derart hat, dass es der zweiten Medien-Überleiteinrichtung (**16**, **18**) erscheint, dass die Mitteilung von der ersten Medien-Überleiteinrichtung (**16**, **18**) kommt.

2. Verfahren nach Anspruch 1, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket zu überwachen ist, umfasst.

3. Verfahren nach Anspruch 1, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket abzufangen ist, umfasst.

4. Verfahren nach Anspruch 1, das weiterhin die Umlenkung des Telekommunikationssignals umfasst.

5. Verfahren nach Anspruch 4, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket umzulenken ist, umfasst.

6. Verfahren nach Anspruch 1, das weiterhin den Schritt der Zuordnung des neuen Ziel-Kopffeldes zu einem beabsichtigen Empfänger oder einer Vollstreckungsbehörde (**14**) umfasst.

7. Verfahren nach Anspruch 1, das weiterhin den Schritt des Ersetzens des vorgegebenen Kopffeldes durch ein zweites neues Ziel umfasst.

8. Verfahren nach Anspruch 7, das weiterhin den Schritt der Zuordnung des zweiten neuen Ziel-Kopffeldes zu dem anderen von dem vorgesehenen Empfänger oder der Vollstreckungsbehörde (**14**) umfasst.

9. Verfahren nach Anspruch 7, bei dem der Schritt des Ersetzens nach dem Schritt des Replizierens erfolgt.

10. System zum Abfangen eines Telekommunikationssignals, das zwischen einer ersten Medien-Überleiteinrichtung (**16**, **18**) und einer zweiten Medien-Überleiteinrichtung (**16**, **18**) in einem Netzwerk übertragen wird, wobei das System einen Replikator (**22**) umfasst, der Folgendes einschließt:
(a) einen Audio-Server, der auf ein Telekommunikationssignal anspricht, um ein Telekommunikations-Paket von der ersten Medien-Überleiteinrichtung (**16**, **18**) zu empfangen, wobei das Telekommunikations-Paket ein vorgegebenes Kopffeld und eine Nutzinformation umfasst; wobei der Replikator (**22**) dadurch gekennzeichnet ist, dass er weiterhin Folgendes einschließt:

(b) einen Abschluss-Punkt zum Entfernen des vorgegebenen Kopffeldes von dem Paket, zum Replizieren der Nutzinformation und zum Hinzufügen eines neuen Kopffeldes zu der replizierten Nutzinformation (**16**, **18**); und
(c) einen Relais-Punkt zum Lenken der replizierten Nutzinformation an die Adresse, die dem neuen Ziel-Kopffeld zugeordnet ist, und dadurch gekennzeichnet, dass:
(d) der Abschluss-Punkt so angeordnet ist, dass er ein abgeändertes vorgegebenes Kopffeld oder ein Ersatz-Kopffeld zu dem Telekommunikations-Paket oder der replizierten Nutzinformation hinzufügt, und dass der Relais-Punkt so angeordnet ist, dass er dieses Paket oder die Nutzinformation an die zweite Medien-Überleiteinrichtung lenkt, wobei das geänderte vorgegebene Kopffeld oder das Ersatz-Kopffeld eine derartige Adresseninformation hat, dass es der zweiten Medien-Überleiteinrichtung (**16**, **18**) erscheint, dass die Mitteilung von der ersten Medien-Überleiteinrichtung kommt.

11. System nach Anspruch 9, bei dem die erste Medien-Überleiteinrichtung (**16**, **18**) so ausgebildet ist, dass sie das Telekommunikationssignal an den Audio-Server lenkt.

12. System nach Anspruch 9, das weiterhin einen zweiten Abschluss-Punkt zum Hinzufügen eines zweiten vorgegebenen Kopffeldes zu der Nutzinformation umfasst.

13. System nach Anspruch 11, bei dem ein neues Ziel-Kopffeld zu der replizierten Nutzinformation hinzugefügt wird, wobei das zweite neue Ziel-Kopffeld einer Vollstreckungsbehörde (**14**) zugeordnet ist.

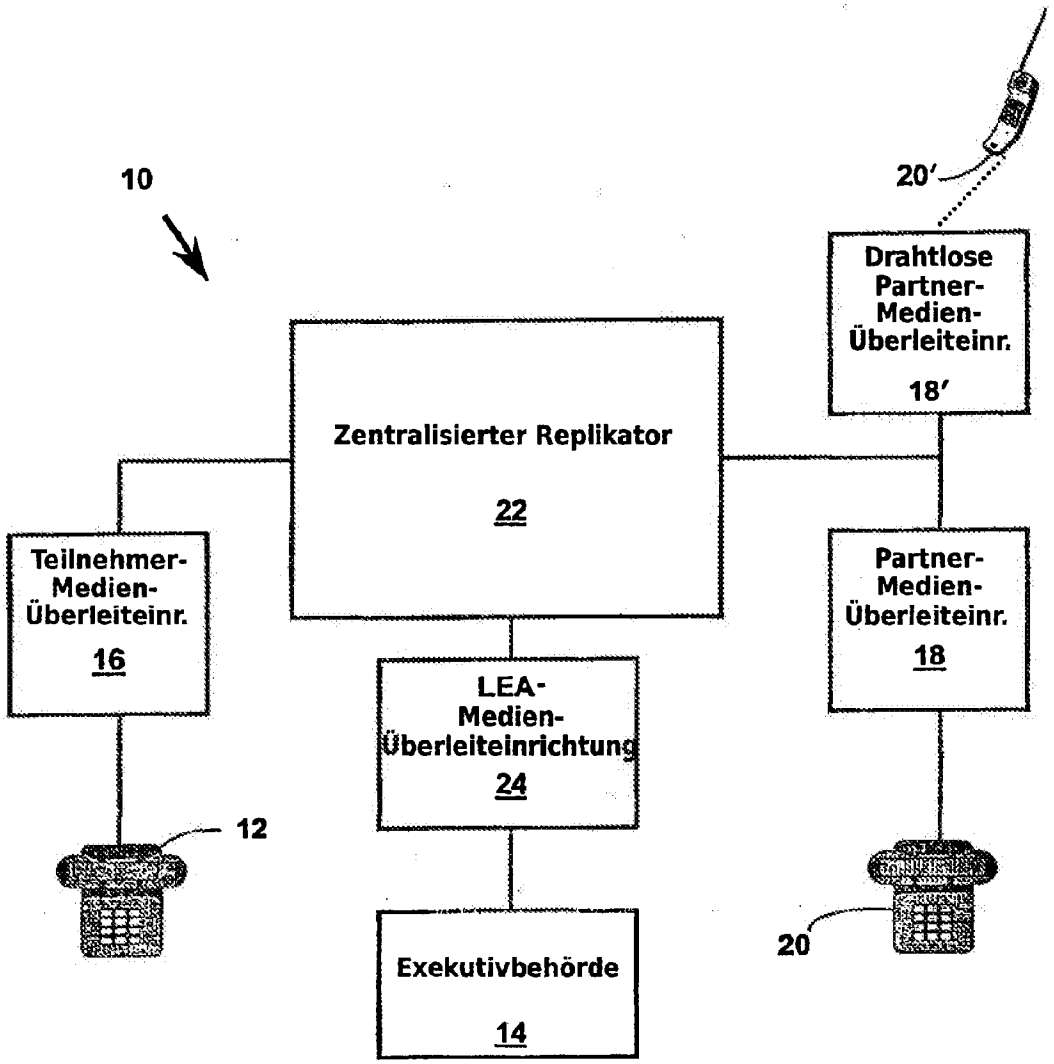
14. System nach Anspruch 11 oder 13, das weiterhin einen zweiten Relais-Punkt zum Lenken der Nutzinformation an die Adresse umfasst, die dem zweiten vorgegebenen Kopffeld zugeordnet ist.

15. System nach Anspruch 9, das weiterhin eine Medien-Überleiteinrichtungs-Steuerung (**26**, **30**) umfasst, die auf die erste oder zweite Medien-Überleiteinrichtung (**16**, **18**) anspricht, um festzustellen, dass ein Telekommunikations-Paket abzufangen ist.

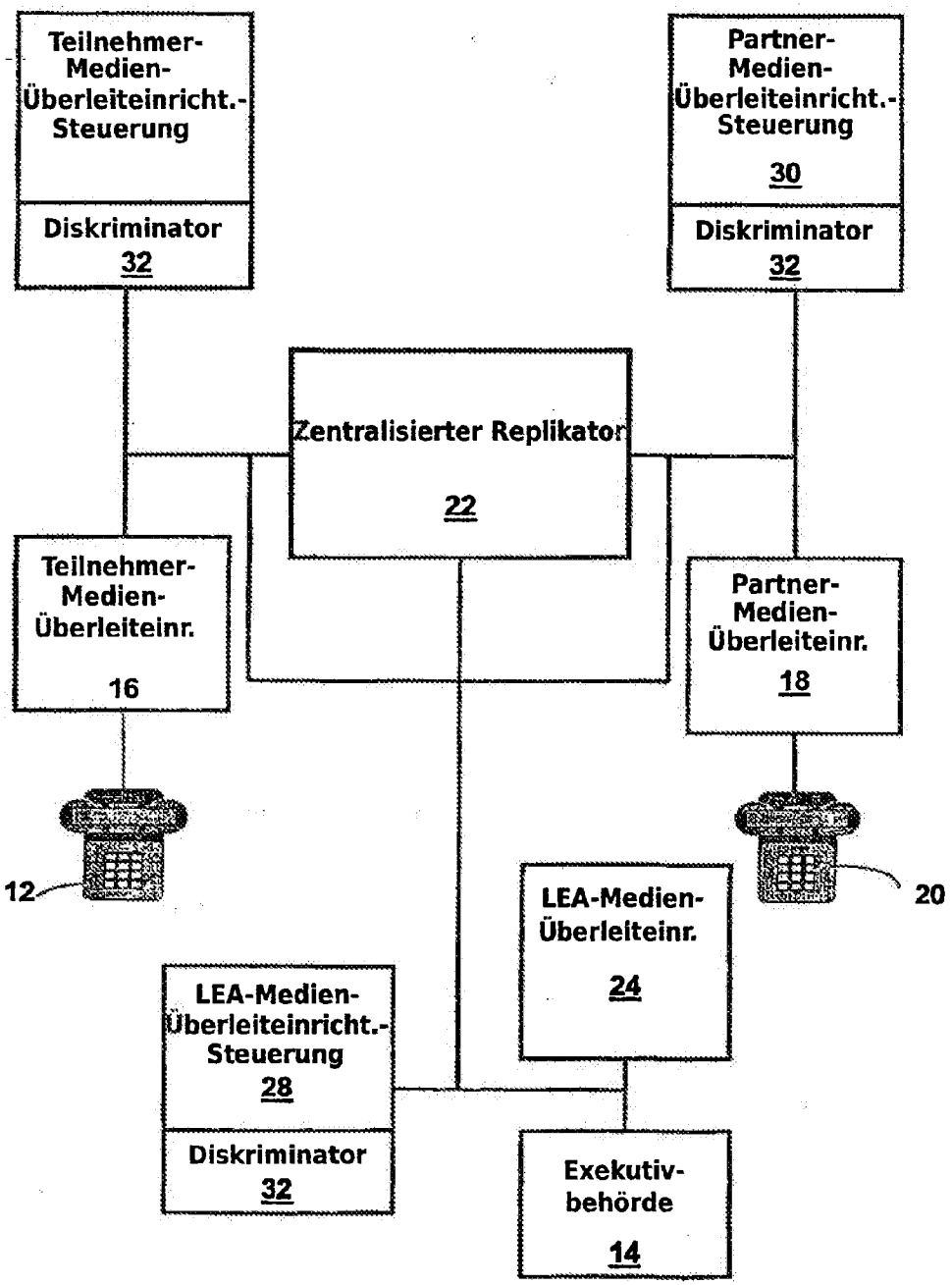
16. System nach Anspruch 13, bei dem die Medien-Überleiteinrichtungs-Steuerung (**26**, **30**) einen Anruf-Diskriminator (**32**) einschließt, der auf das Telekommunikationssignal anspricht, um festzustellen, dass das Telekommunikationssignal einem Abfangen unterworfen ist.

Es folgen 9 Blatt Zeichnungen

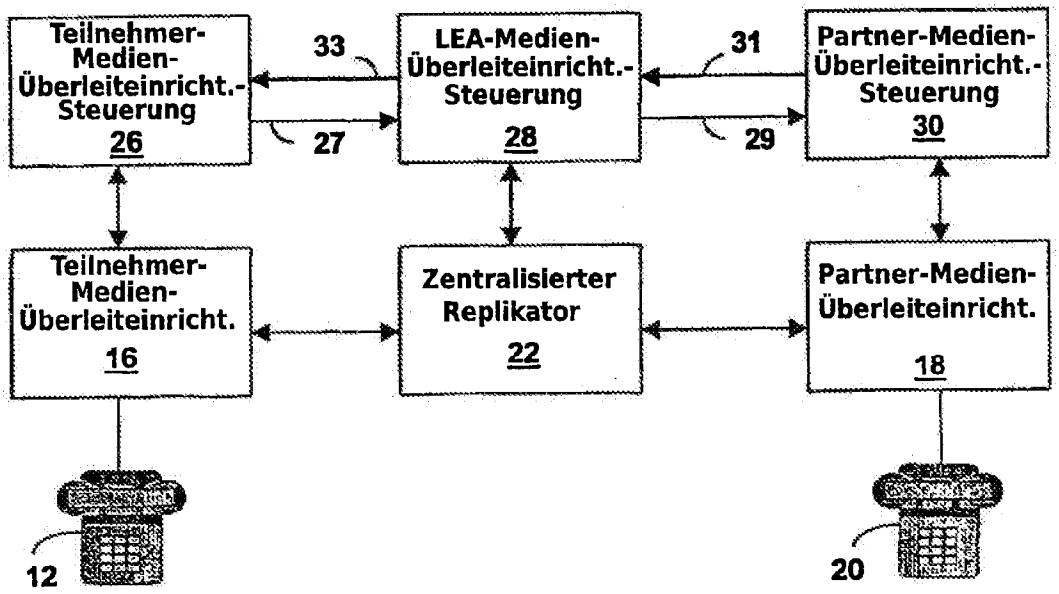
Anhängende Zeichnungen



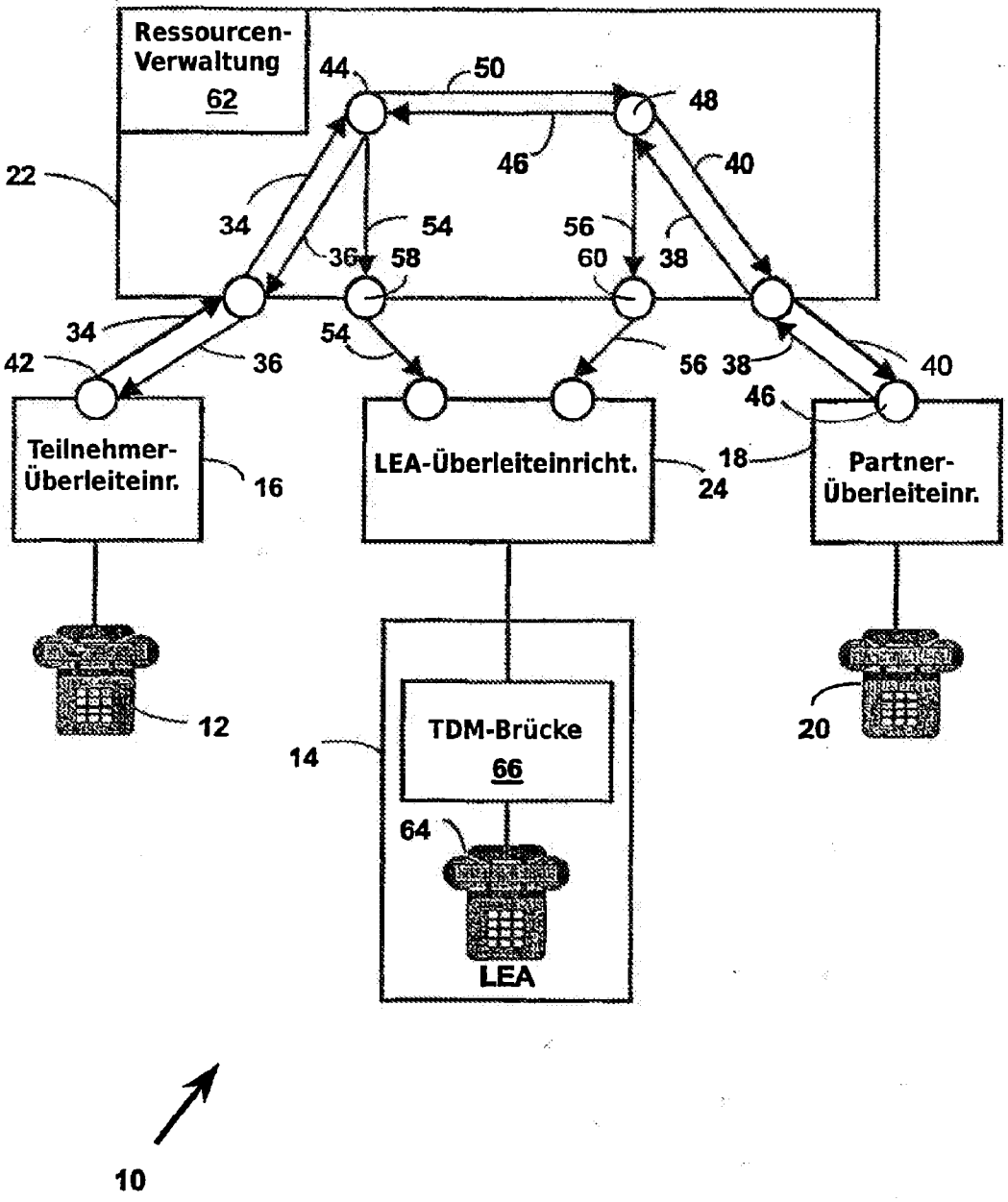
Figur 1



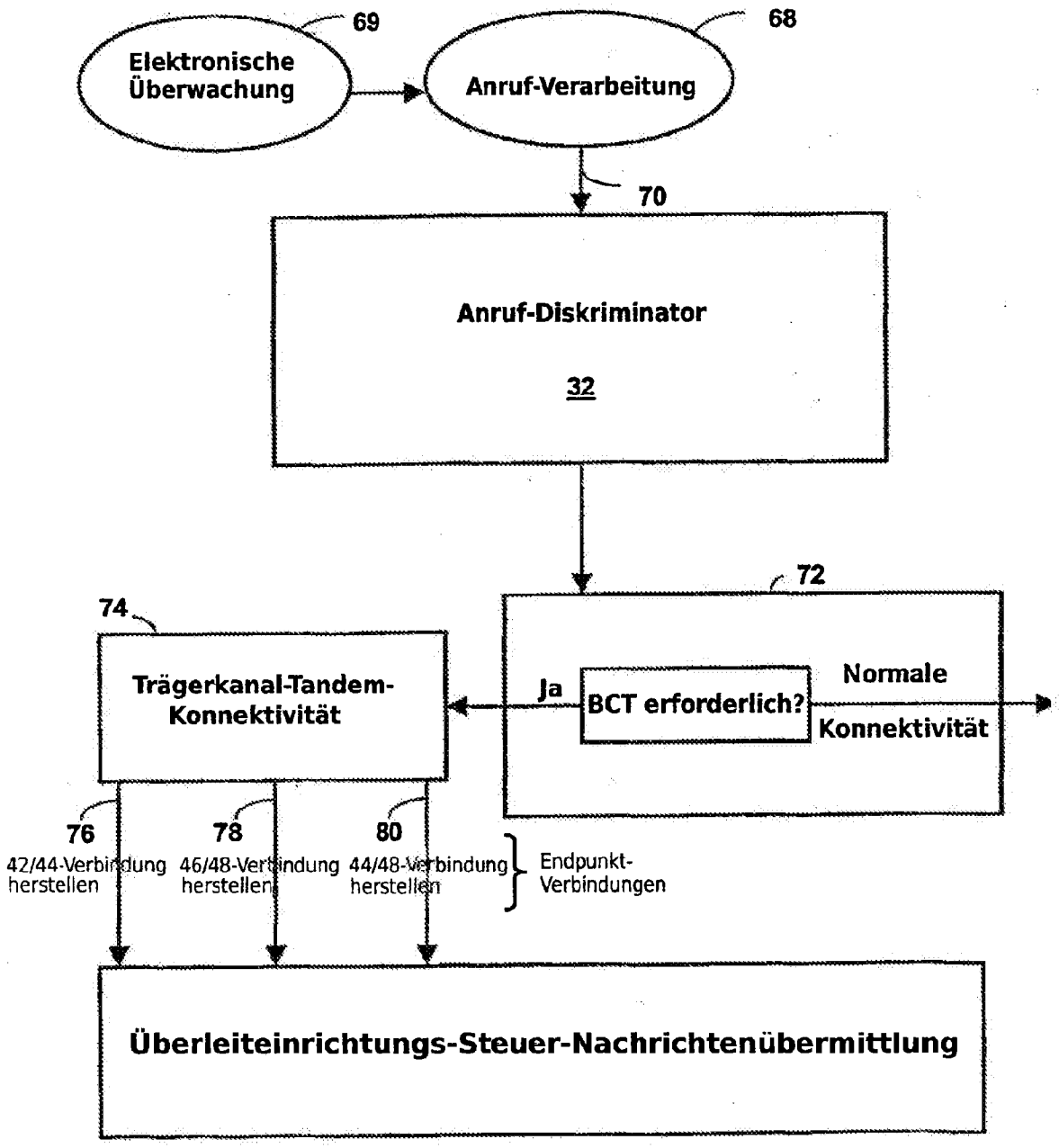
Figur 2



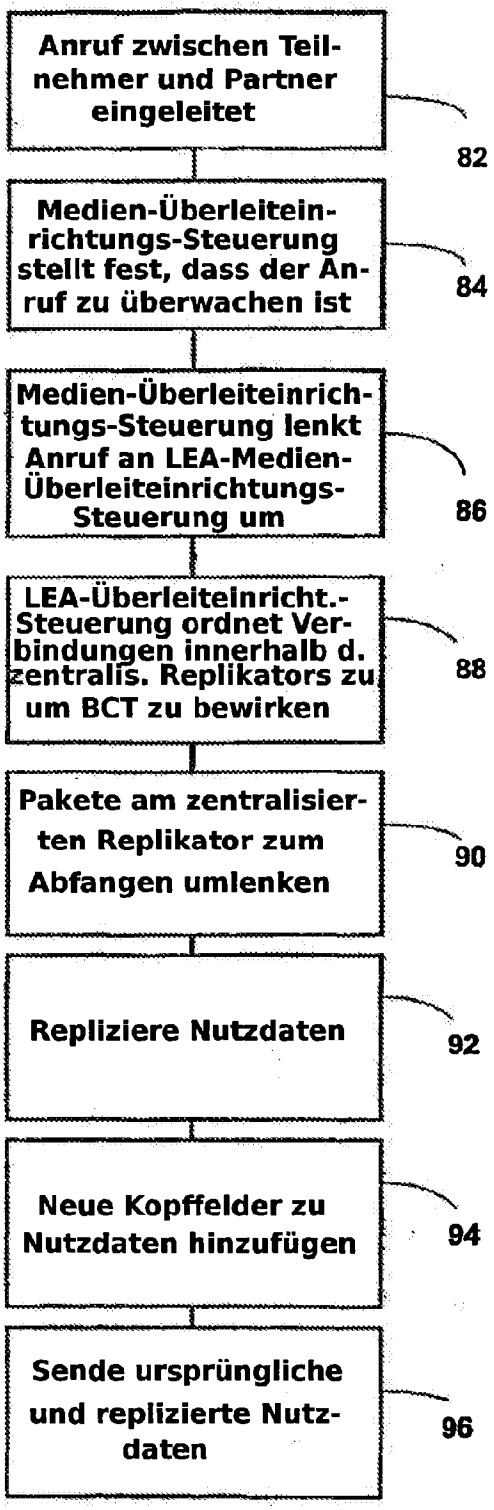
Figur 3



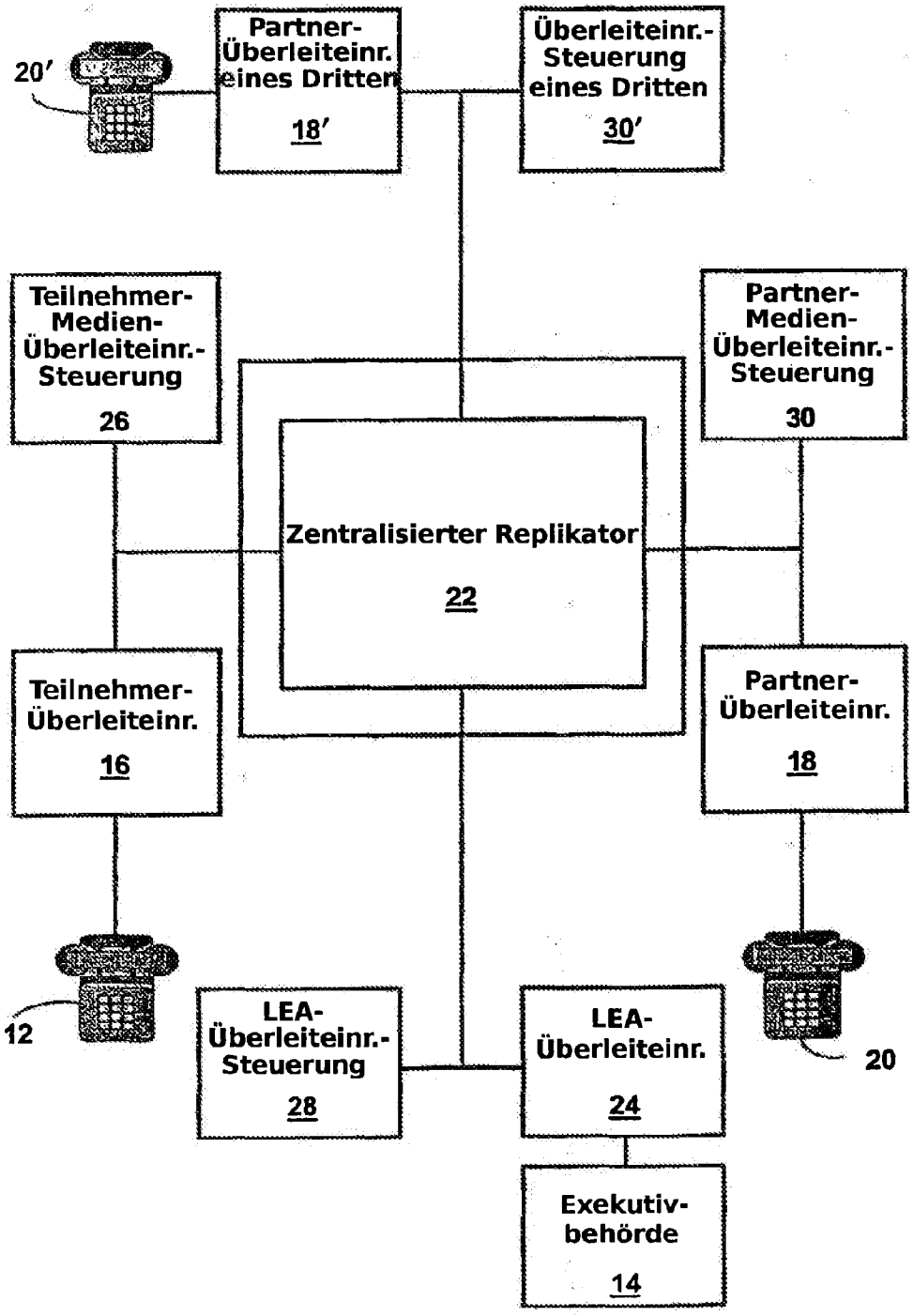
Figur 4



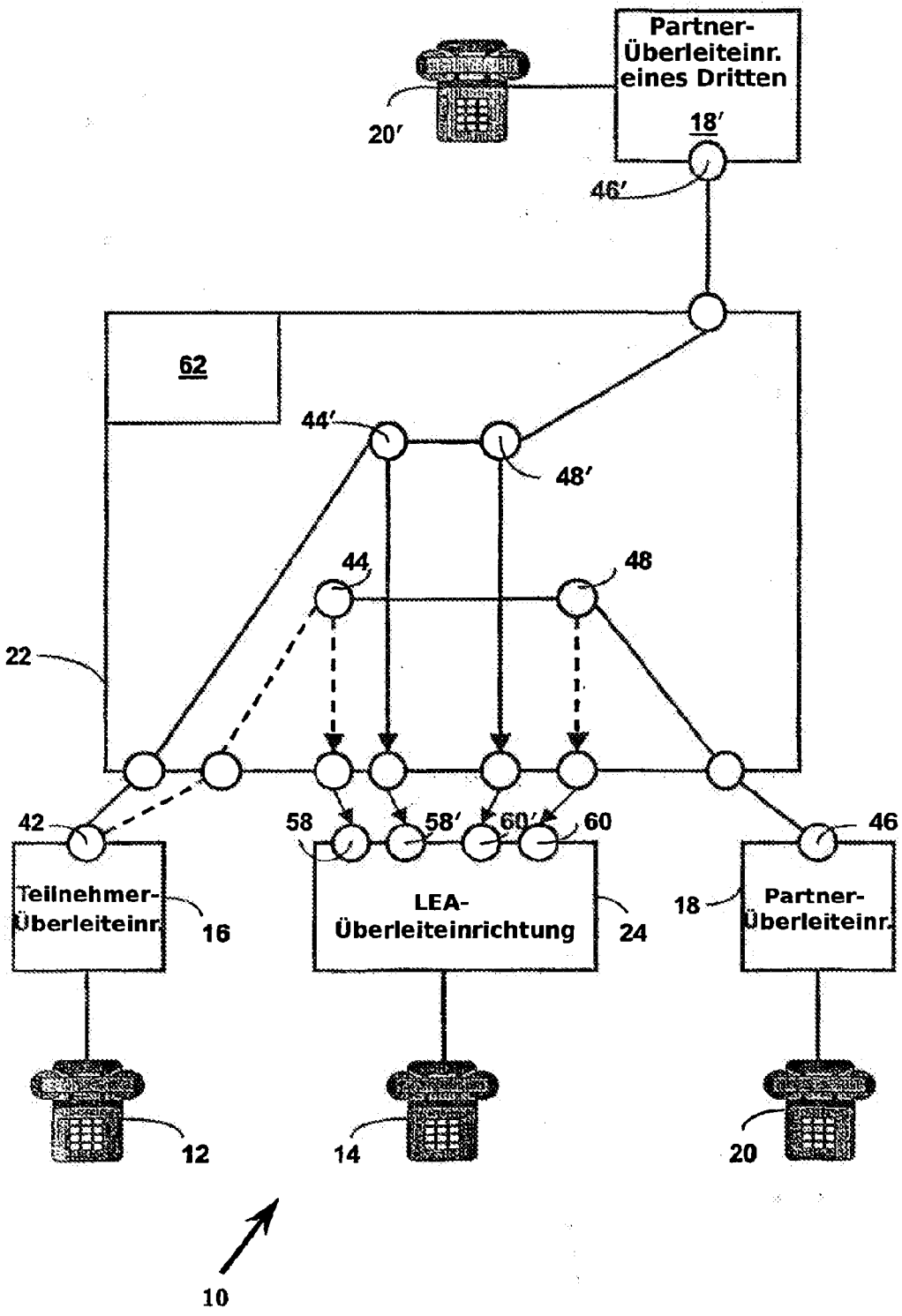
Figur 5



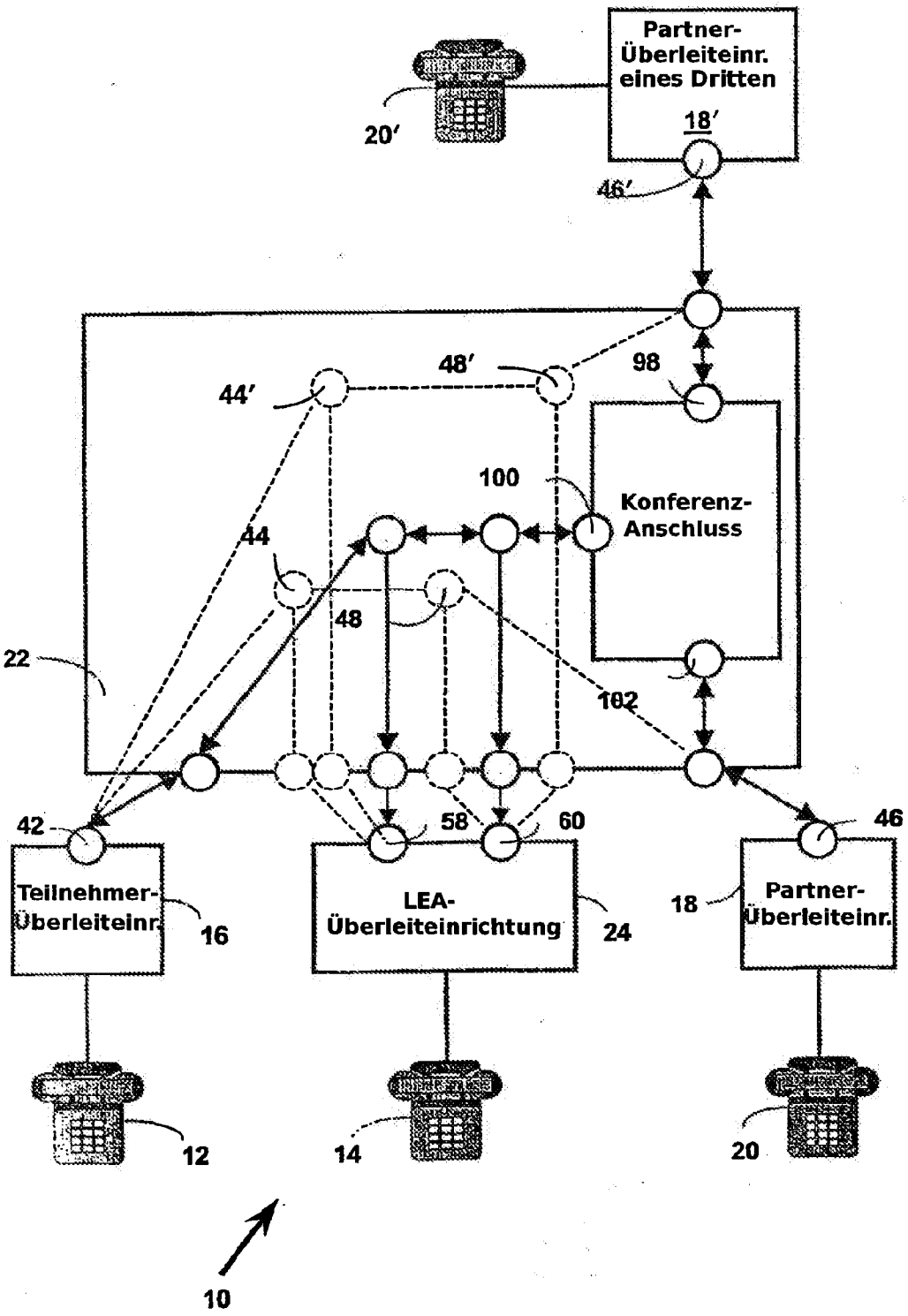
Figur 6



Figur 7



Figur 8



Figur 9

Espacenet

Bibliographic data: DE60317751 (T2) — 2008-11-06

An emergency call back method

Inventor(s): CHIN MARY [US]; ROLLENDER DOUGLAS [US] + (CHIN, MARY, ; ROLLENDER, DOUGLAS)

Applicant(s): LUCENT TECHNOLOGIES INC [US] + (LUCENT TECHNOLOGIES INC)

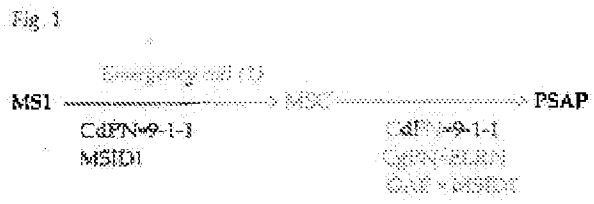
Classification: - international: ***H04B7/26; H04M1/26; H04M11/04; H04M3/42; H04W4/16; H04W4/22; H04W76/02***
- cooperative: **H04W4/22; H04W76/007**

Application number: DE2003617751T 20031009

Priority number(s): US20020270629 20021016

Also published as: EP1411743 (A1) EP1411743 (B1) US2004203565 (A1) US7676215 (B2) KR20040034410 (A) KR101010868 (B1) JP2004140838 (A) JP4335636 (B2) ES2295524 (T3) CN1498029 (A) CN1498029 (B) AT379940 (T) less

Abstract not available for DE60317751 (T2)



(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 603 17 751 T2** 2008.11.06

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 411 743 B1**
(21) Deutsches Aktenzeichen: **603 17 751.4**
(96) Europäisches Aktenzeichen: **03 256 372.8**
(96) Europäischer Anmeldetag: **09.10.2003**
(97) Erstveröffentlichung durch das EPA: **21.04.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.11.2007**
(47) Veröffentlichungstag im Patentblatt: **06.11.2008**

(51) Int Cl.[8]: ***H04Q 7/38*** (2006.01)
H04M 11/04 (2006.01)

(30) Unionspriorität:
270629 **16.10.2002** **US**

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(73) Patentinhaber:
Lucent Technologies Inc., Murray Hill, N.J., US

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
Chin, Mary, Westmont, Illinois 60559, US;
Rollender, Douglas, Bridgewater, New Jersey 08807, US

(54) Bezeichnung: **Verfahren für einen Notfall Rückruf**

Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] In Nordamerika werden Notdienstrufe durch Wählen von „9-1-1" eingeleitet. Andere Teile der Welt können irgendeine andere abgekürzte Kette wählbarer Ziffern wie beispielsweise „6-1-1" in Mexiko verwenden; alle teilen sich die Absicht, für den Anrufer auf eine leichte Weise mit einer leicht zu merkenden Rufnummer nach Hilfe zu rufen bereitzustellen. Diese Rufe werden zu einer örtlichen öffentlichen Dienstabfragestelle (PSAP – Public Service Answering Point) geleitet, wo eine Notreaktion eingeleitet werden kann (Polizei, Feuerwehr, Straßenreparatur, Krankenwagen usw.), während der Anrufer am Telefon gehalten wird. Wenn die Verbindung irgendwie abgetrennt oder fallengelassen wird, ehe der Notfall vollständig gemeldet worden ist oder die reagierende Stelle ankommt, kann der PSAP den Urheber unter Verwendung einer über seine Datenbanken bereitgestellten Rückrufnummer zurückrufen.

[0002] Beispielsweise können die Verbindungsdaten für eine durch ein Drahtnetz eingeleiteten 911-Ruf-ANI (Automatic Line Identification – automatische Anschlußkennung) oder die Telefonnummer der Anschlußleitung, von der der Ruf stammte, enthalten. Die Mobilrufnummer (MDN – Mobile Directory Number) oder Telefonnummer eines drahtlosen Teilnehmers ist jedoch nicht einem physikalischen Anschluß oder einer Mobilstation zugeordnet. Statt dessen werden Anrufe eines drahtlosen Teilnehmers über die MSID (Mobile Station Identification – Mobilgerätekennung), nicht die MDN, zur Mobilstation geleitet. Dementsprechend werden bei der Durchführung eines Notfall-Rückrufs zu einer Mobilstation Hindernisse angetroffen, die beispielsweise bei Festleitungsvorrichtungen nicht angetroffen werden.

[0003] Typischerweise ist die MSID entweder eine 10-ziffrige Mobilidentifikationsnummer (MIN) oder eine 15-ziffrige internationale Mobilteilnehmerkennung (IMSI – International Mobile Subscriber Identifier), die in einer Mobilstation durch einen Diensteanbieter einprogrammiert ist, mit dem der Benutzer der Mobilstation eine Dienstvereinbarung getroffen hat. Dementsprechend ist die MSID nicht unbedingt eine wählbare Nummer.

[0004] Die MDN einer Mobilstation ist eine wählbare Nummer. Die MDN wird von einem Anrufer gewählt und zur Leitung eines Rufs durch das Netz zum Heimatsystem des drahtlosen Teilnehmers benutzt. In dem Heimatsystem des Teilnehmers enthält das Heimatregister (HLR – Home Location Register) die der Teilnehmer-MDN zugeordnete MSID. Dann wird MSID, und nicht die MDN, zum Leiten des Rufs durch das Netz zu dem versorgenden drahtlosen System und zum Rufen des Teilnehmers benutzt. Die MDN des Teilnehmers wird vom Heimatsystem in einer getrennten, Teilnehmerprofil genannten Datei für das versorgende System bereitgestellt.

[0005] Die Benutzung einer getrennten Nummer für MDN und MSID ist für einige Systeme neu. Ursprünglich war in TIA/EIA-41-Systemen vor Implementierung von drahtloser Rufnummernportabilität (WNP – Wireless Number Portability) oder Tausender-Blockrufnummern-Pooling (TBNP – Thousands Block Number Pooling) auf Grundlage des LRN-Verfahrens (Local Routing Number – lokale Leitwegnummer) und Auslands-Roaming (IR – International Roaming) die Mobilidentifikationsnummer (MIN) einer Mobilstation die gleiche wie die MDN. Mit WNP und TBNP wurde jedoch die MDN „portierbar" oder „zusammenfaßbar" von einem Diensteanbieter zu einem anderen Diensteanbieter. Da MSID nicht portierbar oder zusammenfaßbar ist, wird eine neue MSID für einen Teilnehmer vom Empfangs-Diensteanbieter mit einer einportierten oder zusammengefaßten MDN zugewiesen.

[0006] Durch internationales Roaming wurde auch die Trennung von MSID und MDN erzwungen. Während die MIN eine nach der 10-ziffrigen MDN des nordamerikanischen Nummerierungsplans modellierte 10-ziffrige Nummer ist, wird von den Trägern anderer Nationen mit einem unterschiedlichen Rufnummerierungsplan möglicherweise nicht zugelassen, daß ihre MDN dem international anerkannten MIN-Format gleichwertig ist. Eine weitere Standard-MSID ist die IMSI. Sie wird sowohl in TIA/EIA-41- als auch GSM-Systemen in der ganzen Welt benutzt. Die IMSI ist eine 15-ziffrige Nummer und kann daher nicht als eine 10-ziffrige MDN dienen.

[0007] Ursprünglich, als die MDN die gleiche wie die MIN war, würde die MIN an einen PSAP abgeliefert werden und würde als Rückrufnummer benutzt werden. Mit der Trennung von MIN und MDN wie oben beschrieben wurde es notwendig, die MDN als getrennte Rückrufnummer an die PSAP abzugeben, zusammen mit der MSID des Anrufers. Mit der Implementierung dieser Lösung sind gewisse Probleme verbunden. Das Hauptproblem besteht darin, daß das betreuende System möglicherweise nicht die MDN des Anrufers und nur die MSID besitzt, um sie der PSAP mit dem Ruf darzubieten. Einige der Gründe dafür beziehen sich auf die Art und Weise, auf die MSID-MDN-Trennung gemäß den Standards implementiert worden ist.

[0008] WNP, TBNP oder IR werden durch ein altes versorgendes TIA/EIA-41-System möglicherweise nicht unterstützt. Das bedeutet, daß das ältere versorgende System erwarten könnte, daß MIN und MDN die gleichen sind. Das ältere System würde nicht einmal wissen, daß es nach einer getrennten MDN im Dienstprofil des Teilnehmers (das auf MIN

und nicht MDN ausgerichtet ist) suchen muß. Bei dieser Einschränkung dürfen diese Teilnehmer möglicherweise nicht Grunddienste benutzen, aber es muß ihnen erlaubt sein, Notdienste anzurufen. Infolgedessen wird der Ruf eines Roamers, der „9-1-1" wählt, während er sich in einem alten System befindet, an die PSAP mit einer MSID aber keiner MDN abgeliefert. Dementsprechend ist kein Rückruf möglich.

[0009] Ein neueres versorgendes System mit WNP- und IR-Fähigkeit kann möglicherweise MDN nicht an die PSAP abliefern. Dies würde geschehen, wenn die rufende Mobilstation nicht bei irgendeinem Dienstanbieter registriert ist (beispielsweise gibt es Mobiltelefone, die nur für Notrufe benutzt werden). Auch ist es möglich, daß ein Teilnehmer einen Notruf einleitet, bevor das HLR dem versorgenden System mit dem die MDN enthaltenden Dienstprofil des Teilnehmers geantwortet hat.

[0010] Für einen internationalen Roamer würde die Rückruf-MDN erfordern, daß die PSAP eine internationale Verbindung zum Erreichen eines Teilnehmers in seiner lokalen Notdienstzone (ESZ – Emergency Service Zone) einleitet. Dies ist keine praktische, zeitgerechte oder ausreichend zuverlässige Lösung für eine PSAP, die normalerweise keine internationalen Verbindungen einleitet und sofortige Rückrufinformationen erfordern könnte, um das Leben einer Person zu retten. Zusätzlich wird der PSAP möglicherweise nicht die gesamte internationale MDN (bis zu 15 Ziffern einschließlich einer Länderkennzahl) zum Rückruf dargeboten.

[0011] Eine vorgeschlagene Lösung dieser Probleme erfordert die Abgabe von 9-1-1+ die letzten sieben Ziffern der elektronischen Seriennummer (ESN) der rufenden Mobilstation an die PSAP als Rückrufnummer, wenn die MDN nicht zur Verfügung steht. Während dies zum Identifizieren des Anrufers für die PSAP und das versorgende System dienen könnte, kann diese „9-1-1+ESN7" nicht durch das Netz geleitet werden und nicht zum Einleiten eines Rückrufs benutzt werden.

[0012] US-B-5 689 548 offenbart einen Notfall-Rückruf mit MSC-Nummern. Sie offenbart eine MSC-Rufnummer in der Cdpn zwischen der versorgenden MSC/VLR und dem PSAP. Die MSC-Rufnummer ist ein gebräuchliches Leitwegwerkzeug zum Leiten aller Arten von Nachrichtenübermittlung zu und von der MSC.

KURZE BESCHREIBUNG DER ERFINDUNG

[0013] Erfindungsgemäße Verfahren entsprechen den unabhängigen Ansprüchen. Bevorzugte Ausführungsformen sind in den abhängigen Ansprüchen aufgeführt. In dem Rückrufverfahren gemäß der vorliegenden Erfindung wird jeder Vermittlung in einem drahtlosen Netz eine lokale Not-Leitwegnummer (ELRN – Emergency Local Routing Number) zugewiesen. Wenn eine Vermittlung des drahtlosen Netzes einen Notruf zu einer öffentlichen Dienstabfragestelle (PSAP – Public Service Answering Point) leitet, sendet die Vermittlung die lokale Not-Leitwegnummer als die Rufnummer des Anrufers (CgPN – Calling Party Number) und stellt der PSAP die Kennung der Mobilstation (MSID) bereit. Bei Abfall des Notrufs führt die PSAP unter Verwendung der Not-Leitwegnummer als die Rufnummer des Angerufenen (CdPN – Called Party Number) einen Rückruf durch. Als Ergebnis wird von der Vermittlung, die den Notruf von der Mobilstation zur PSAP leitete, der Rückruf empfangen. Die PSAP sendet auch die Kennung der Mobilstation zur Vermittlung. Diese MSID wird zum Rufen der richtigen Mobilstation benutzt. In einer Ausführungsform der vorliegenden Erfindung wird die Mobilstationskennung von der PSAP in einem generischen Adressenparameter zur Vermittlung signalisiert.

[0014] Wenn eine Vermittlung ihre lokale Not-Leitwegnummer als Rufnummer des gerufenen Teilnehmers empfängt, erkennt die Vermittlung eine Notfall-Rückrufsituation und ruft die durch die in Verbindung mit der Not-Leitwegnummer empfangene Mobilstationskennung identifizierte Mobilstation. In einer Ausführungsform der vorliegenden Erfindung wird von der Vermittlung der Bearbeitung des Rückrufs eine höhere Priorität erteilt, als anderen Aufgaben, wenn eine ELRN die CdPN ist. Auf diese Weise wird die PSAP wieder mit der Mobilstation verbunden.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0015] Die vorliegende Erfindung wird besser verständlich aus der unten stehend gegebenen ausführlichen Beschreibung und den beiliegenden Zeichnungen, die nur beispielhafterweise gegeben sind, wobei gleiche Bezugsziffern entsprechende Teile in den verschiedenen Zeichnungen bezeichnen und in denen:

[0016] Fig. 1–Fig. 6 Kommunikationsflußdiagramme sind, die die Funktionsweise des Rückrufverfahrens gemäß der vorliegenden Erfindung darstellen.

AUSFÜHRLICHE BESCHREIBUNG VON AUSFÜHRUNGSFORMEN

[0017] In dem Rückrufverfahren gemäß der vorliegenden Erfindung wird jeder Vermittlung (z. B. eine Mobilvermittlungsstelle (MSC – Mobile Switching Centre)) in einem drahtlosen Kommunikationssystem eine einmalige leitbare Rückrufnummer zugewiesen. Diese Nummer wird hiernach als „lokale Not-Leitwegnummer" bzw. ELRN (Emergency Local Routing Number) bezeichnet. Man kann sich die ELRN als

ähnlich der jeder lokalen Vermittlung zum Implementieren von WNP (Wireless Number Portability – drahtlose Nummernportabilität) oder TBNP (Thousands Block Number Pooling – Tausender-Blocknummerzusammensetzung) zugewiesenen lokalen Leitwegnummer (LRN – Local Routing Number) vorstellen. Eine ELRN kann jedoch nur zu der Vermittlung geleitet werden, die die Nummer besitzt und die ELRN für jede Vermittlung ist einmalig und ist nicht portierbar.

[0018] Wie bekannt ist wird, wenn eine Mobilstation einen Notruf tätigt, die Mobilstationskennung (MSID) in Verbindung mit dem Notruf zugeführt. Beispielsweise ist die MSID die Mobilkennungsnummer (MIN), eine 10-ziffrige IRM (International Roaming Mobile Identification Number) für die zehnziffrigen Rufnummern, die außerhalb des Bereichs des nordamerikanischen Nummerierungsplans liegen, oder die IMSI (International Mobile Subscriber Identifier – internationale Mobilteilnehmerkennung). Wenn eine Vermittlung des drahtlosen Systems einen Notruf (z. B. einen 9-1-1-Ruf) von einer Mobilstation, besonders einer Mobilstation ohne MDN empfängt, sendet die Vermittlung die ELRN der Vermittlung zu der die Vermittlung versorgenden PSAP (Public Service Answering Point – öffentlichen Dienstabfragestelle). Von der Vermittlung wird die ELRN als die Rufnummer des Anrufers (CgPN – Calling Party Number) geliefert und auch die MSID der Mobilstation für die PSAP bereitgestellt. Zum Beispiel wird die MSID beispielsweise in dem ISUP-GAP (Generic Address Parameter – generischen Adressenparameter) signalisiert.

[0019] Bei Abfall des Notrufs wird von der PSAP ein Rückruf unter Verwendung der ERLN als die Rufnummer des gerufenen Teilnehmers (CdPN – Called Party Number) durchgeführt. Im Ergebnis empfängt die Vermittlung, die den Notruf von der Mobilstation zur PSAP geleitet hat, den Rückruf. Auch sendet die PSAP die Kennung der Mobilstation zur Vermittlung. Zum Beispiel wird die MSID beispielsweise im ISUP-GAP (Generic Address Parameter – generischen Adressenparameter) mit dem Rückruf signalisiert.

[0020] Wenn eine Vermittlung ihre Not-Leitwegnummer als die Rufnummer des gerufenen Teilnehmers empfängt, wird von der Vermittlung eine Notfall-Rückrufsituation erkannt und die durch die in Verbindung mit der ERLN empfangene MSID identifizierte Mobilstation gerufen und der Notfall-Rückruf hergestellt. Dieses ERNL-Verfahren kann auch mit Prioritätswarteschlangenbildung in den Vermittlungen versehen sein; wobei die Vermittlung die Rückrufnummer mit einer höheren Priorität als mit anderen Verbindungen verbundene Aufgaben bearbeitet. Das sollte die Notfall-Rückruf-Abfertigungsrate selbst während Zeiten des Spitzenverkehrs an der Vermittlung verbessern. Obwohl weiterhin die Verwendung des Verfahrens als für alle Notrufe durchgeführt beschrieben ist, kann sie nur auf durch Mobilstationen mit keinen oder nicht verfügbaren MDN getätigte Notrufe begrenzt sein.

[0021] Fig. 1–Fig. 6 sind Kommunikationsflußdiagramme, die die Funktionsweise des Rückrufverfahrens gemäß der vorliegenden Erfindung darstellen. Nach der Darstellung in Fig. 1 leitet eine erste Mobilstation MS1 einen Notruf, einen 9-1-1-Ruf im vorliegenden Beispiel, ein, der von einer MSC empfangen wird. Dementsprechend ist die Rufnummer des gerufenen Teilnehmers 9-1-1 und die MSID1 der ersten Mobilstation MS1 wird auch der MSC zugeführt. Von der MSC wird dann der Notruf zur versorgenden PSAP geleitet. Dabei bleibt die Rufnummer des gerufenen Teilnehmers 9-1-1, aber die MSC liefert ihre ERLN als die Rufnummer des rufenden Teilnehmers. Auch liefert die MSC die MSID1 der ersten Mobilstation MS1 im generischen Adressenparameter (GAP).

[0022] Bei Abfall des Notrufs wird von der PSAP ein Rückruf unter Verwendung der ERLN als die Rufnummer des gerufenen Teilnehmers durchgeführt, da die ERLN der PSAP als die Rufnummer des rufenden Teilnehmers zugeführt wurde. Das Ergebnis ist, daß der Rückruf wie in Fig. 2 gezeigt zur MSC geleitet wird. Wie weiterhin in Fig. 2 dargestellt wird die MSID1 der ersten Mobilstation mit dem Rückruf im ISUP GAP signalisiert. Nach der Darstellung in Fig. 3 benutzt die MSC die MSID1 der ersten Mobilstation MS1 zum Rufen der ersten Mobilstation MS1 und Vollendung des Rückrufs.

[0023] Angenommen, daß, während der Rückruf zur ersten Mobilstation MS1 im Gang ist, eine zweite Mobilstation MS2 wie in Fig. 4 gezeigt einen 9-1-1-Notruf einleitet.

[0024] Wie bei dem Notruf von der ersten Mobilstation MS1 liefert die zweite Mobilstation MS2 die Mobilstationskennung MSID2 zusammen mit dem Notruf (z. B. ist die Rufnummer des gerufenen Teilnehmers 9-1-1). Dann wird von der MSC der Notruf zur PSAP geleitet. Dabei bleibt die Rufnummer des gerufenen Teilnehmers 9-1-1, aber die MSC liefert ihre ERLN als die Rufnummer des rufenden Teilnehmers. Auch liefert die MSC die MSID2 der zweiten Mobilstation MS2 zur PSAP. Dementsprechend zeigt die Fig. 4, daß die MSC die gleiche Rufnummer des rufenden Teilnehmers (d. h. die ERLN) für beide Notrufe zur PSAP liefert.

[0025] Bei Abfall des zweiten Notrufs wird von der PSAP ein Rückruf unter Verwendung der ERLN als die Rufnummer des gerufenen Teilnehmers durchgeführt, da die ERLN als Rufnummer des rufenden Teilnehmers zur PSAP zugeführt wurde. Das Ergebnis ist, daß wie in Fig. 5 gezeigt ein zweiter Rückruf zur MSC geleitet wird. Wie weiter in Fig. 5 gezeigt wird die MSID2 der zweiten Mobilstation mit dem zweiten

Rückruf im ISUP GAP signalisiert. Wie in Fig. 6 gezeigt benutzt die MSC die MSID2 der zweiten Mobilstation MS2 zum Rufen der zweiten Mobilstation MS2 und Fertigstellung des Rückrufs.

[0026] Durch das Notfall-Rückrufverfahren der vorliegenden Erfindung wird sichergestellt, daß mit jedem Notruf von einer Mobilstation eine leitbare Rückrufnummer für eine PSAP bereitgestellt wird. Insbesondere ist die ELRN eine Nummer, die zum Leiten von einem oder vielen Notfall-Rückrufen zur Ursprungsvermittlung (z. B. MSC) benutzt wird. Die ELRN der Ursprungsvermittlung wird der PSAP als Rufnummer des rufenden Teilnehmers (CgPN – Calling Party Number) signalisiert, besonders, wenn keine lokale MDN zum Begleiten eines Notrufs zur Verfügung steht.

[0027] Im nordamerikanischen Numerierungsplan ist die ELRN eine 10-ziffrige Nummer (NPA-NXX-XXXX), wobei die führenden 6 Ziffern (NPA-NXX) eindeutig jeder lokalen Vermittlung in Nordamerika für Rufleitungszwecke zugewiesen sind. Die nachfolgenden vier Ziffern sind dem Vermittlungsbetreiber zugewiesen. Das Notfall-Rückrufverfahren ist jedoch in einem öffentlichen Wählnetz überall in der Welt anwendbar. Die ELRN enthält nämlich diejenigen Ziffern, die von jedem nationalen Numerierungsplan zum Leiten von Verbindungen zu einer bestimmten Vermittlung zugewiesen sind. Auch kann das Notfall-Rückrufverfahren mit jedem Mobildienst oder jeder drahtlosen Zugangstechnologie angewandt werden.

[0028] Das Notfall-Rückrufverfahren ist unabhängig von Nummernportabilität und Nummernzusammenstellung. Diese Netzfähigkeiten sind von den LRN-Verfahren (Local Routing Number – lokale Leitwegnummer) zum Leiten einer Verbindung zu einer versorgenden Vermittlung auf Grundlage der einer portierten oder gepoolten gewählten Nummer zugeordneten LRN abhängig. Im Vergleich ist die ELRN nicht einer gewählten Nummer sondern einer Vermittlung zugeordnet.

[0029] Auf manche Weisen funktioniert die ELRN im öffentlichen Netz wie die für lokale Nummernportabilität erforderte lokale Leitwegnummer (LRN – Local Routing Number); beispielsweise fungieren beide als einzige Nummer zum Leiten von vielen Verbindungen zu einer bestimmten Vermittlung. Es ist jedoch keine Datenbankabfrage zum Identifizieren der zum Leiten einer Verbindung zu einer versorgenden MSC erforderlichen ELRN erforderlich. Als Ergebnis kann die ELRN, wenn sie als die Rufnummer des gerufenen Teilnehmers (CdPN – Called Party Number) zum Leiten eines Rückrufs von einer PSAP zur versorgenden MSC benutzt wird, von der ISUP-FCI (Forward Call Indicator – Vorwärts-Rufanzeige) begleitet sein, die eingestellt ist, um anzuzeigen, daß keine Nummernportabilitätsdatenbankabfrage erforderlich ist.

[0030] Wie oben besprochen ist eine ELRN nicht mit irgendeiner bestimmten MDN verbunden und wird zum Leiten eines Rückrufs direkt zur versorgenden Vermittlung und nicht dem Heimatsystem benutzt. Die ELRN beseitigt das Erfordernis, daß die PSAP eine MDN zum Einleiten eines Notfall-Rückrufs benutzt. Es ist nicht nötig, eine MDN oder eine LRN anzufordern, um einen Rückruf durch ein Heimatsystem zu leiten wie nach bestehenden MAP-Standards (Mobile Application Part – Mobilanwendungsteil). Auch ist es nicht nötig, eine internationale Verbindung durch ein fremdes Heimatsystem einzuleiten, um einen internationalen Roamer im lokalen Bereich zurückzurufen. Dadurch wird Signalisierung verringert, Zeit gespart und die Dienstezuverlässigkeit verbessert. Weiterhin besteht kein Bedarf an einer TLDN (Temporary Long Distance Number – zeitweilige Fernrufnummer) wie in TIA/EIA-41-Netzen oder einer MSRN (Mobile Station Routing Number – Mobilstations-Leitwegnummer) wie in GSM-Netzen, um einen Rückruf vom Heimatsystem zum versorgenden System zu leiten. Dadurch wird Signalisierung verringert, Zeit gespart und kein Bedarf an der Versorgung von TLDN oder MSRN erhoben.

[0031] Nach dieser Beschreibung der Erfindung wird es klar sein, daß sie auf viele Weisen verändert werden kann. Solche Veränderungen sind nicht als Abweichung von dem Rahmen der Erfindung anzusehen und alle derartigen Abänderungen sollen im Rahmen der nachfolgenden Ansprüche enthalten sein.

Patentansprüche

1. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:
Zuweisen einer Not-Leitwegnummer zu jeder Vermittlung in einem drahtlosen Netz nur zur Verwendung als die Rufnummer des Anrufers von durch jede Vermittlung zu einer öffentlichen Dienstabfragestelle geleiteten drahtlosen Notrufen;
Senden der Not-Leitwegnummer einer Vermittlung in dem drahtlosen Netz, die die Kommunikationsbedürfnisse einer Mobilstation bearbeitet, die einen Notruf einleitet, und einer Kennung der Mobilstation zu einer öffentlichen Dienstabfragestelle.

2. Verfahren nach Anspruch 1, wobei jede zugewiesene Not-Leitwegnummer nicht portabel ist.

3. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:
Empfangen einer Not-Leitwegnummer einer Vermittlung in einem drahtlosen Netz, die Kommunikationsbedürfnisse einer einen Notruf einleitenden Mobilstation bearbeitet, und einer Kennung der Mobilstation an einer öffentlichen Dienstabfragestelle, wobei die

Not-Leitwegnummer nur zur Verwendung als die Rufnummer des Anrufers des Notrufes zugewiesen wird; und
Einleiten eines Rückrufs zur Mobilstation an der öffentlichen Dienstabfragestelle durch Rufen der Not-Leitwegnummer, wenn der durch die Mobilstation getätigte Notruf abfällt, so daß die die ihr als die Rufnummer des angerufenen in einer Verbindung zugewiesene Not-Leitwegnummer empfangende Vermittlung die Verbindung als einen Notfall-Rückruf erkennt.

4. Verfahren nach Anspruch 1, weiterhin mit folgendem:
Signalisierung der Kennung der Mobilstation an die Vermittlung bei Einleitung des Rückrufs.

5. Verfahren nach Anspruch 4, wobei der Schritt des Signalisierens die Kennung der Mobilstation in einem generischen Adressenparameter sendet.

6. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:
Zuweisen einer Not-Leitwegnummer zu jeder Vermittlung in einem drahtlosen Netz nur zur Verwendung als die Rufnummer des Anrufers von zu einer öffentlichen Dienstabfragestelle geleiteten drahtlosen Notrufen durch jede Vermittlung;
Empfangen an einer Vermittlung des drahtlosen Netzes einer Rufnummer des Angerufenen und einer Mobilstationskennung; und
Rufen einer durch die Mobilstationskennung identifizierten Mobilstation, wenn die Rufnummer des Angerufenen der der Vermittlung zugewiesenen Not-Leitwegnummer entspricht.

7. Verfahren nach Anspruch 6, wobei der Schritt des Empfangens die Kennung der Mobilstation in einem generischen Adressenparameter empfängt.

8. Verfahren nach Anspruch 6, wobei der Schritt des Rufens mit Priorität gegenüber anderen Aufgaben an der Vermittlung durchgeführt wird.

9. Verfahren nach Anspruch 6, wobei die Vermittlung eine Mobilvermittlungsstelle ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1

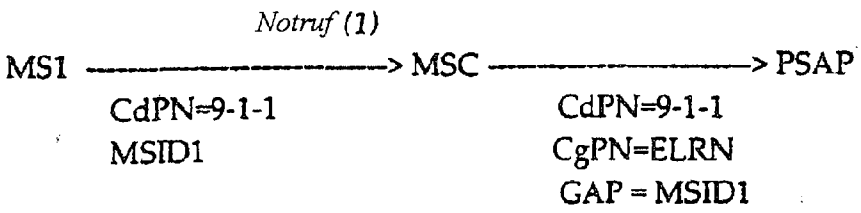


Fig. 2

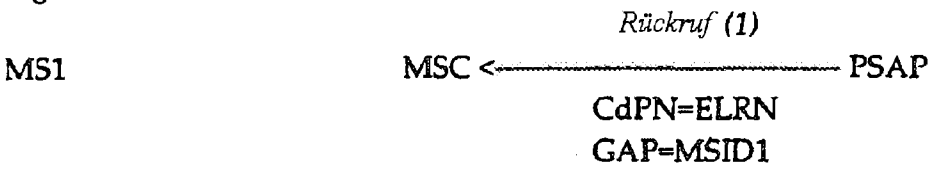


Fig. 3

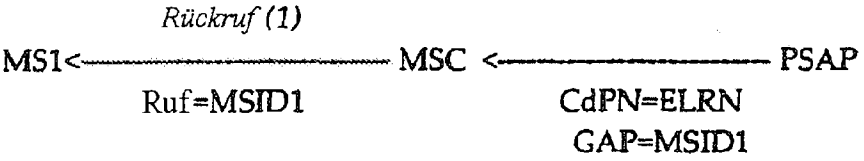


Fig. 4

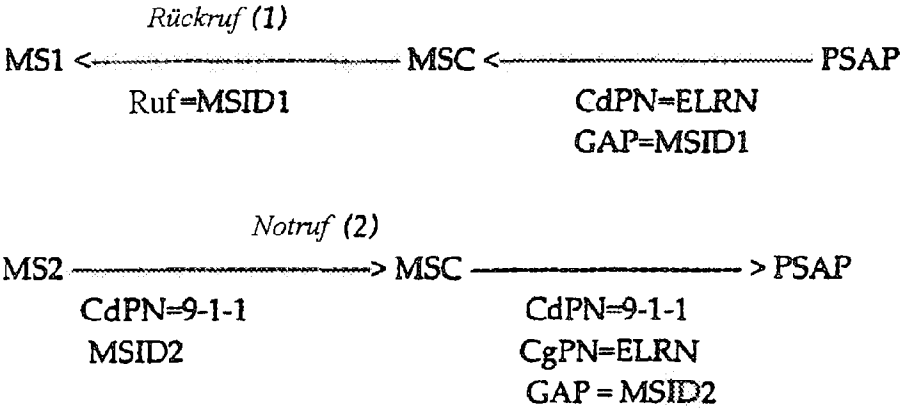


Fig. 5

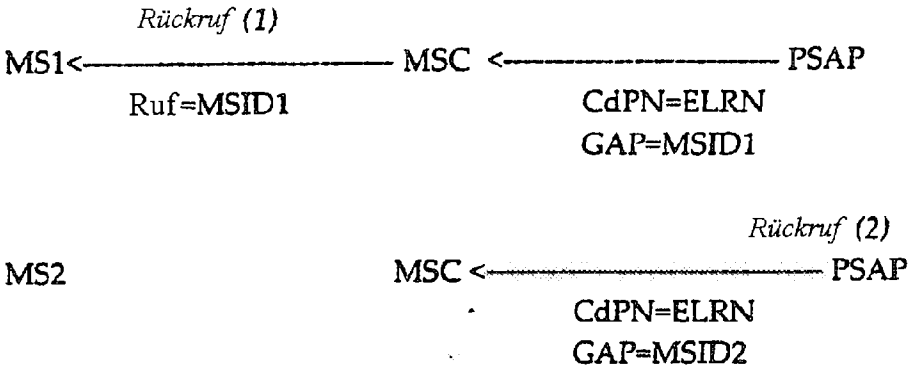
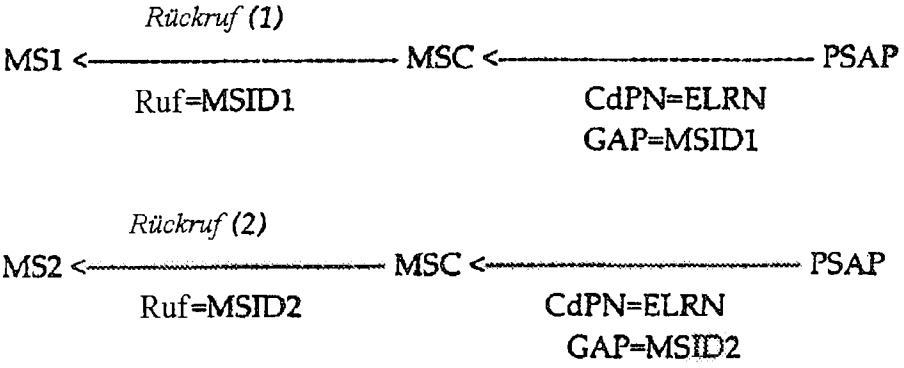


Fig. 6



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 841 832 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.05.1998 Bulletin 1998/20

(51) Int Cl.[6]: **H04Q 11/04**

(21) Application number: **97308622.6**

(22) Date of filing: **29.10.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **08.11.1996 US 746364**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

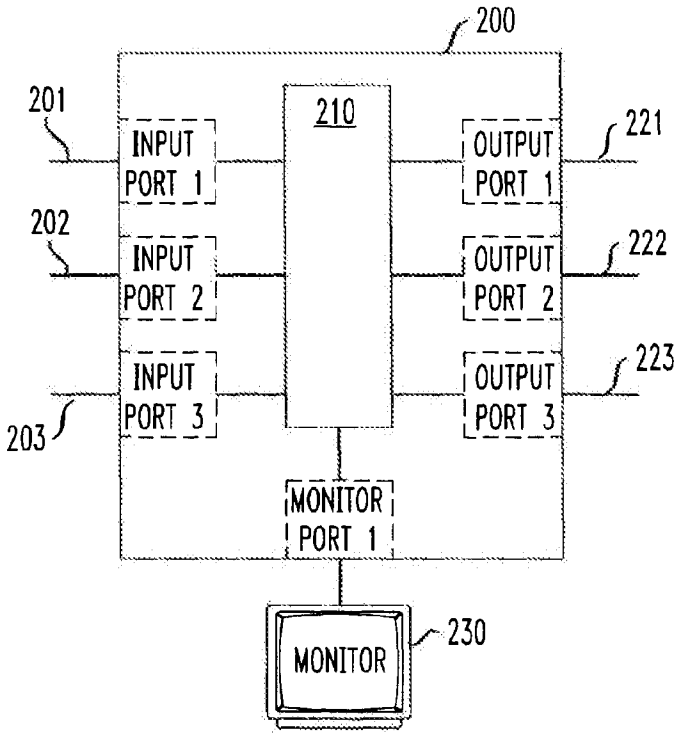
(72) Inventor: **Ramakrishnan, Kadangode K.**
Berkeley Heights, New Jersey 07922 (US)

(74) Representative: **Harding, Richard Patrick et al**
Marks & Clerk,
4220 Nash Court,
Oxford Business Park South
Oxford OX4 2RU (GB)

(54) Promiscuous network monitoring utilizing multicasting within a switch

(57) Multicasting within a switch is utilized to promiscuously monitor switched communication networks. The switch routes data packets from input ports to data output ports and routes copies of the data packets to a monitor output port. A monitor processor is connected to the switch to receive copies of all data packets received at the switch, and thereby monitor the communication network.

FIG. 3



EP 0 841 832 A2

Description

FIELD OF THE INVENTION

The present invention relates to promiscuous monitoring of communication networks. Specifically, this invention relates to a method and apparatus for providing promiscuous monitoring of a communication network through the use of multicasting within an ATM switch.

BACKGROUND

A communication network needs to be monitored to evaluate its performance and to diagnosis any potential problems. Typically, an end-station communication device(s) is connected to the network in such a manner that the end-station(s) receive all the data transmitted within the network: this is known as promiscuous monitoring. The configurations by which promiscuous monitoring can be performed will vary depending upon the type of network.

Multi-access networks, such as an FDDI (fiber distributed data interface) and Ethernet local-area network (LAN), allow multiple points of access. In these multi-access networks, a monitoring point can be easily established through which all of the network communication traffic passes. In such a case, an end-station can be connected to the network to easily perform promiscuous monitoring of the network. By disabling the end-station's filtering functions, it can receive and promiscuously monitor all communication traffic transmitted over the network.

With asynchronous transfer mode (ATM) and other switched networks, however, such as switched Fast Ethernet or switched FDDI, promiscuous monitoring cannot be as easily performed because the links are point to point. Thus, in such networks, no one place exists within the network where a promiscuous monitor can be located to receive all the data packets/frames. A typical prior art approach is to promiscuously monitor each link going out of a switch output port by inserting a T-connector, such as an optical splitter, into the link.

Fig. 1 illustrates a prior art approach for promiscuous monitoring of a communication network. Sender communication devices 100a and 100b are connected to switch 110 which is connected to receiver communication devices 120a and 120b on links 130a and 130b, respectively. The communication network shown in Fig. 1 is simplified for illustrative purposes; thus, a typical communication network has a vast number of nodes with switches, sender and receiver communication devices, and links interconnecting the switches. Unlike the simple case shown in Fig. 1 having a single switch 110, communication data sent by a sender communication device will typically pass through multiple switches 110 before reaching a receiver communication device.

Using T-connector 140a and 140b, a copy of the packets transmitted on links 130a and 130b, respectively, will be received by not only the intended receiver, 120a and 120b, respectively, but also can be received by an end-station performing promiscuous monitoring. Within a communication network, the point of access for promiscuous monitoring is usually selected at the switch through which most of the communication traffic passes. Promiscuous monitors 150a and 150b are connected to each T-connector 140a and 140b, respectively, thereby monitoring links 130a and 130b, respectively. Alternatively, a single promiscuous monitor can be connected to multiple T-connectors through multiple input ports in the promiscuous monitor thereby monitoring several individual links at the same monitor.

The prior art configurations present several shortcomings. As the number of switch output ports increases, the necessary number of T-connectors increases, and correspondingly the required number of monitoring end-stations or input ports at the monitoring end-station also increases. Of course, with such a monitoring configuration, monitoring costs will increase as the number of switch output ports increase. Additionally, such hardware-based monitoring techniques lack the flexibility to change as the network characteristics change. For example, although the amount of traffic over certain links may change over time, the configuration of the monitoring systems can be modified only inconveniently by changing the hardware connections or by having a large number of T-connectors and selectively enabling the reception of the ports in the promiscuous monitor.

SUMMARY OF THE INVENTION

The present invention utilizes multicasting within a switch to promiscuously monitor a switched communication network at a single point in the network. At least one port per switch is established as a monitor port, where the switch has sufficient capacity to allow the port to be used for monitoring. The switch comprises input ports, data output ports, and monitor output ports. An interconnection network within the switch is connected to the input ports, the data output ports, and the monitor output port. The interconnection network routes data packets from input ports to data output ports and routes copies of the data packets to the monitor output port. A monitor processor is connected to the switch at the monitor output port to receive copies of data packets received at the switch, and thereby monitor the communication network. The promiscuous monitor can receive copies of all data packets received at the switch or receive copies of just a selective set of data packets received at the switch.

In another embodiment of the present invention, the switch routes copies of the data packets from some of the input ports or output ports to one monitor output port and routes copies of the data packets arriving at the remaining input ports or output ports, respectively, to another monitor output port. The present invention can also allow modification of which input ports' or output

ports' data packet copies are routed to which monitor output ports. Of course, the present invention can be configured with more than two monitor output ports.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a prior art approach for promiscuous monitoring of a communication network.

Fig. 2 shows a wide area network illustrative of the configuration and operation of a contemporary communications network.

Fig. 3 illustrates a switch and promiscuous monitor according to an embodiment of the present invention.

Fig. 4 illustrates a multicasting routing methodology to perform promiscuous monitoring within the switch shown in Fig. 3.

Figs. 5A and 5B shows a switch with multiple monitor output ports according to a second embodiment of the present invention.

Fig. 6 shows a switch with multiple monitor output ports and output port-based monitoring according to a third embodiment of the present invention.

DETAILED DESCRIPTION

Networks are a principal means of exchanging or transferring information (e.g., data, voice, text, video, etc.) among communications devices (i.e., devices for inputting and/or outputting information such as computer terminals, multimedia workstations, fax machines, printers, servers, telephones, videophones, etc.) connected to the network(s). A network typically comprises switching nodes connected to each other, and to communication devices, by links.

Fig. 2 shows a wide area network illustrative of the configuration and operation of a contemporary communications network. Network 10 comprises a plurality of switching nodes 20 and links 30. Each of the switching nodes 20 may also have associated therewith a buffer of predetermined size and each of the links 30 will have associated therewith a predetermined traffic handling capacity. Note that the depiction of a network comprising only five switching nodes is for convenience of illustration, and that an operating network may have a much larger number of switching nodes and associated connecting links.

Various switching nodes are shown illustratively connected to communications devices 40. It should be understood that the single communications devices shown connected to the switching nodes in the figure are used for simplicity of illustration, and that an actual implementation of such a network would ordinarily have a number of communications devices connected at such switching nodes. Note, as well, that the illustrated communications devices may also represent another network, such as a LAN, which is connected to network 10.

Each communications device 40 generates information for use by, or receives information from, other communications devices in the network. The term "information" as used herein is intended to include data, text, voice, video, etc. Information from communications device 40 is characterized by a set of transmission and/or rate parameters related to network link and buffer requirements needed to accommodate transmission of such information. Control information can be communicated from communication device 40 to a switch at switching node 20 to specify the rate/buffer requirements.

Communications networks will often use a networking protocol called Asynchronous Transfer Mode (ATM). In these networks, all communication at the ATM layer is in terms of fixed-size information segments, called "cells" in ATM terminology. An ATM cell consists of 48 bytes of payload and 5 bytes for the ATM-layer header. Routing of cells is accomplished through cell switches. Packets of information may be broken up (or segmented) into multiple cells, each cell carrying the 48 bytes of information sequentially. The destination reassembles the cells received into the original packet.

ATM cells can be carried on a virtual circuit (VC) that must be set up such that received cells can be routed to multiple ports at a switch. Permanent VC connections can be easily set up through switch management; switched VC connections, however, need to be set up on a more dynamic basis.

Fig. 3 illustrates a switch and promiscuous monitor according to an embodiment of the present invention. As shown in Fig. 3, switch 200 has three input ports, three data output ports, and a monitor output port. Although switch 200 shown in Fig. 3 has a certain number of ports for illustrative purposes, the present invention is equally applicable for any switch having any number of ports.

Input links 201, 202 and 203 are connected to switch 200 at input ports 1, 2 and 3, respectively, which are connected to interconnection network 210. Interconnection network 210 is connected to data output ports 1, 2 and 3. Output links 221, 222 and 223 are connected to data output ports 1, 2 and 3, respectively. Interconnection network 210 is also connected to monitor port 1 which is connected to promiscuous monitor processor 230.

Interconnection network 210 routes data packets received at an input port to the appropriate destination data output port(s). The number of input ports and/or output ports for switch 200 can exceed the number of links of the network connected to switch 200. Additional output ports therefore are available for connecting one or more promiscuous monitors. In addition to switching communication data packets between the input ports and the data output ports, interconnection network 210 also routes a copy of data packets received at each input port or output port to the monitor output port 1 through the use of known point-to-multipoint multicasting techniques within a single switch. Point-to-multipoint multicasting is the routing of a single message to multiple

recipients. Typically, multicasting is utilized to allow a single sender to transmit a message, through the various switches of a network, to multiple senders connected to the network at various locations. To support such multicasting, switches incorporate internal mechanisms to multicast incoming data to more than one output port; at least one of these additional output ports can then act as a monitor port. The present invention takes advantage of this multicasting capability of the network by treating traffic on each input port of the switch as being from a sender which has receivers downstream on more than one output port. Thus, by multicasting within the switch, the network data traffic that passes through this switch can be promiscuously monitored.

Fig. 4 illustrates a multicasting routing methodology to perform promiscuous monitoring within the switch shown in Fig. 3. As a data packet is received at input port 2, interconnection network 210 routes the data packet to the destination data output port, for example, data output port 1; this is represented in Fig. 4 as a dotted line. Interconnection network 210 also routes a copy of the data packet to monitor output port 1; this is represented in Fig. 4 as a solid line. Similarly, as a data packet is received at input port 1, interconnection network 210 routes the data packet to the destination data output port, for example, data output port 3; this is represent in Fig. 4 as a dotted line. Interconnection network 210 also routes a copy of the data packet to monitor output port 1; this is represented in Fig. 4 as a solid line. Although not shown in Fig. 4, interconnection network 210 routes each data packet received at each input port to the appropriate destination data output port(s), while also routing a copy of all data packets or routing a selective set of data packets to monitor output port 1.

In a second embodiment of the present invention, multiple monitor output ports are connected to the switch. By configuring the switch with multiple monitor output ports, the present invention can perform load balancing to better distribute the data packets copied for promiscuous monitoring among multiple monitor output ports. Thus, if certain input ports receive more communication data traffic than other input ports, the task of promiscuously monitoring these input ports having heavy communication traffic can be divided among the various monitor processors connected to the various monitor output ports of the switch. A similar function can be used to balance the load among output ports as well. Therefore, no one monitor processor is disproportionally monitoring more communication data than the other monitor processors.

Figs. 5A and 5B shows a switch with multiple monitor output ports according to the second embodiment of the present invention. Switch 300, as shown in Figs. 5A and 5B, has three input ports, three data output ports and two monitor output ports. Fig. 5A illustrates a configuration where as a data packet is received at input port 1 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor output port 2. Also shown in Fig. 5A, as a data packet is received at either input port 2 or input port 3 and forwarded to the proper destination output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor output port 1. The routing of the data packet copies to the monitor output ports are shown in Fig. 5A as solid lines.

Fig. 5B illustrates an alternative configuration where as a data packet is received at either input port 1 or input port 2 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the data packet to monitor output port 2. Also shown in Fig. 5B, as a data is received at input port 3 and forwarded to the proper destination data output port(s) (not shown), interconnection network 310 also routes a copy of the packet to monitor output port 1.

In a third embodiment of the present invention, the multicasting can be based on the data packets having been forwarded to output ports, rather than the data packets received at input ports as was the case with Figs. 4, 5A and 5B. Fig. 6 shows a switch with multiple monitor output ports and output port-based monitoring according to the third embodiment of the present invention. Switch 400, as shown in Fig. 6, has three input ports, three data output ports and two monitor output ports. As a data packet is received at input ports 1 and 2, interconnection network 410 routes a copy of the data packet to destination data output port 1; this is represented in Fig. 6 as dotted lines. Interconnection network 410 also routes a copy of the data packet to monitor output port 2; this is represented as solid lines. Similarly, as a data packet is received at input ports 1 and 3, interconnection network 410 routes a copy of the data packet to destination data output port 3; this is represented as dotted lines. Interconnection network 410 also routes a copy of the data packet to monitor output port 2; this is represented in Fig. 6 as solid lines.

In embodiments of the present invention having multiple monitor output ports, the characteristics of the interconnection network controlling the routing of data between input ports and monitor output ports can be modified as the traffic patterns of the connected links change over time. Modifications to the interconnection network can be performed easily because the routing of data is controlled through software rather than through the hardware configurations of the prior art, such as optical splitters, which are comparatively inflexible.

It should, of course, be understood that while the present invention has been described in reference to switches having particular characteristics, switches of other characteristics should be apparent to those of ordinary skill in the art. For example, the switch can have any number of input ports, data output ports and monitor output ports. Similarly, any number of promiscuous monitor processors can be connected to the switch on monitor output ports, or in other words, output ports not

being utilized. The present invention is equally applicable for any type of switch, such as an input-buffered switch, output-buffered switch and shared-memory switch.

Claims

1. A switch, within a switched communication network, for enabling promiscuous monitoring, comprising:

   a plurality of input ports including a first input port, said plurality of input ports receiving a plurality of data packets including a first data packet and a second data packet;
   a plurality of data output ports including a first data output port and a second data output port;
   a first monitor output port; and
   an interconnection network connected to i) said plurality of input ports, ii) said plurality of output ports, and iii) said first monitor output port, said interconnection network routing the first data packet from the first input port to the first data output port, said interconnection network routing a copy of the first data packet to said first monitor output port.

2. The switch of claim 1, wherein a copy of each data packet of the plurality of data packets is routed to said first monitor output port.

3. The switch of claim 1, wherein a copy of a subset of the plurality of data packets is routed to said first monitor output port.

4. The switch of claim 1, wherein said interconnection network routes a copy of each data packet received at the first input port to said first monitor output port.

5. The switch of claim 1, wherein said interconnection network selects a subset of the plurality of data packets received at the first input port and routes a copy of the subset to said first monitor output port.

6. The switch of claim 5, wherein said interconnection network selects the subset on a dynamic basis.

7. The switch of claim 5, wherein said interconnection network selects the subset on a virtual circuit basis.

8. The switch of claim 1, wherein said interconnection network routes to said first monitor output port a copy of each data packet forwarded to the first data output port.

9. The switch of claim 1, wherein said interconnection network selects a subset of the plurality of data packets forwarded to the first data output port and routes a copy of the subset to said first monitor output port.

10. The switch of claim 9, wherein said interconnection network selects the subset on a dynamic basis.

11. The switch of claim 9, wherein said interconnection network selects the subset on a virtual circuit basis.

12. The switch of claim 1, further comprising:

    a second monitor output port connected to said interconnection network;
    said interconnection network routes the second data packet from the second input port to the second data output port and routes a copy of the second data packet to said second monitor output port.

13. The switch of claim 12, wherein said interconnection network selects a first subset of the plurality of data packets and routes a copy of the first subset to said first monitor output port, said interconnection network selects a second subset of the plurality of data packets and routes a copy of the second subset to said second monitor output port.

14. The switch of claim 13, wherein said interconnection network balances the load between data packets routed to said first monitor output port and data packets routed to said second monitor output port.

15. The switch of claim 13, wherein said interconnection network selects the first subset or second subset on a dynamic basis.

16. The switch of claim 13, wherein said interconnection network selects the first subset or second subset on a virtual circuit basis.

FIG. 1

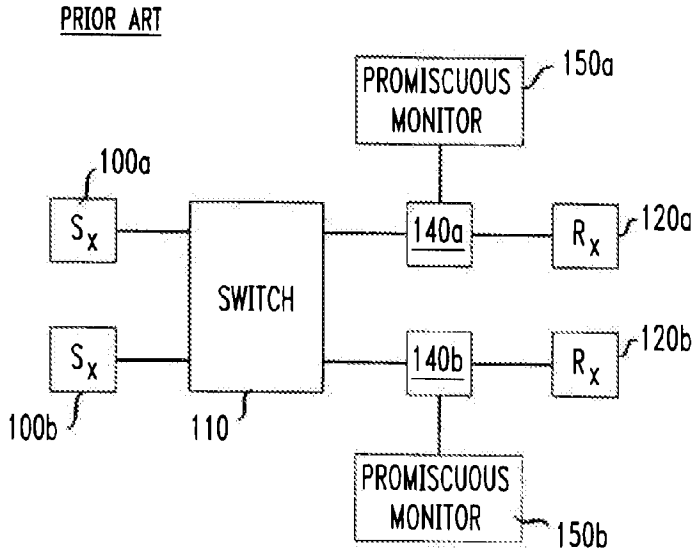


FIG. 2

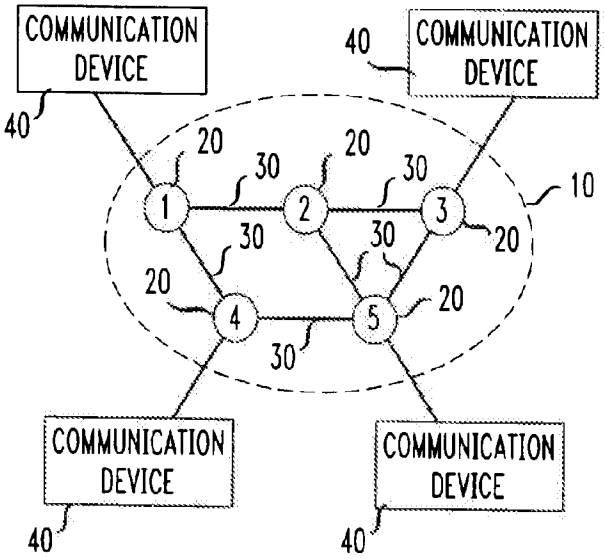


FIG. 3

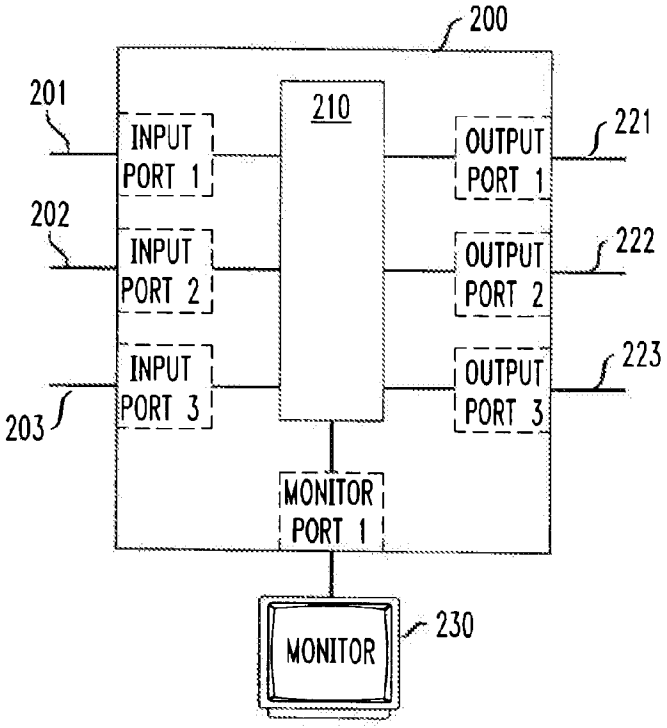


FIG. 4

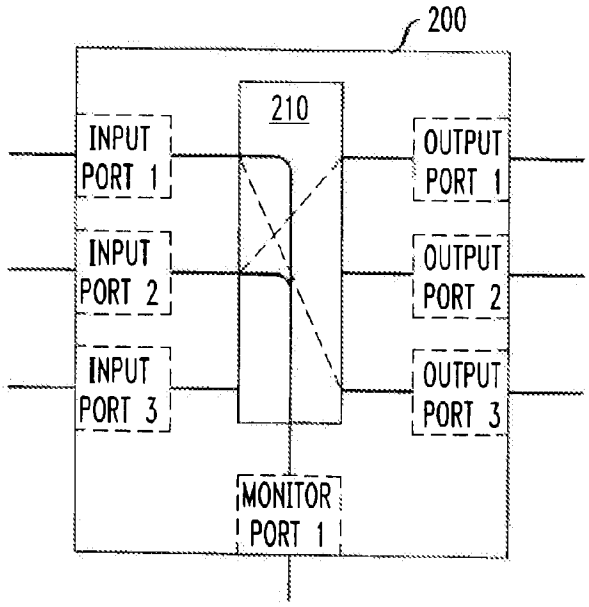


FIG. 5A

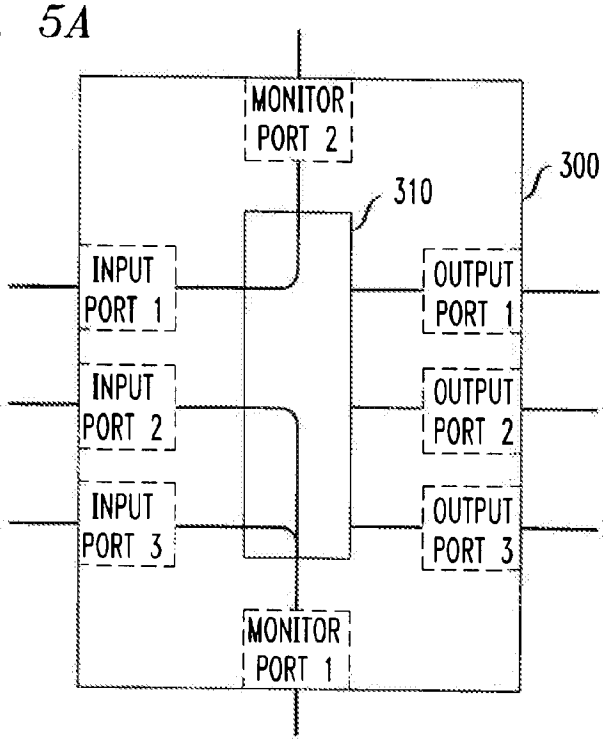


FIG. 5B

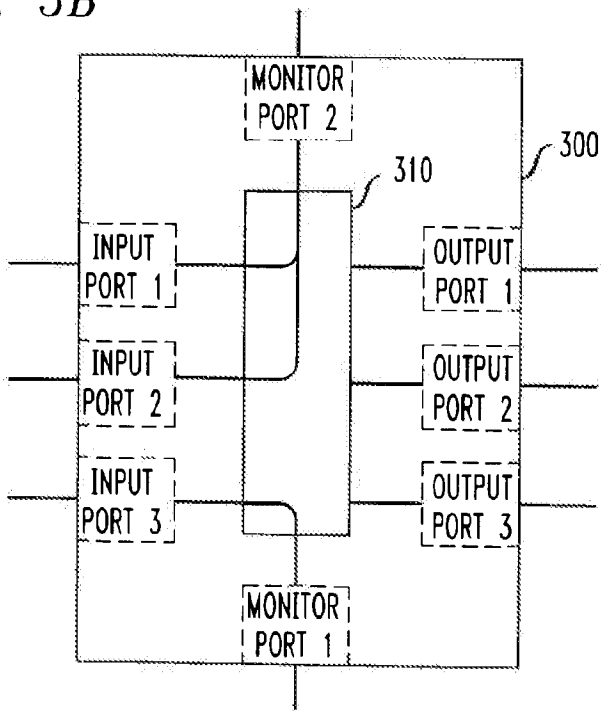
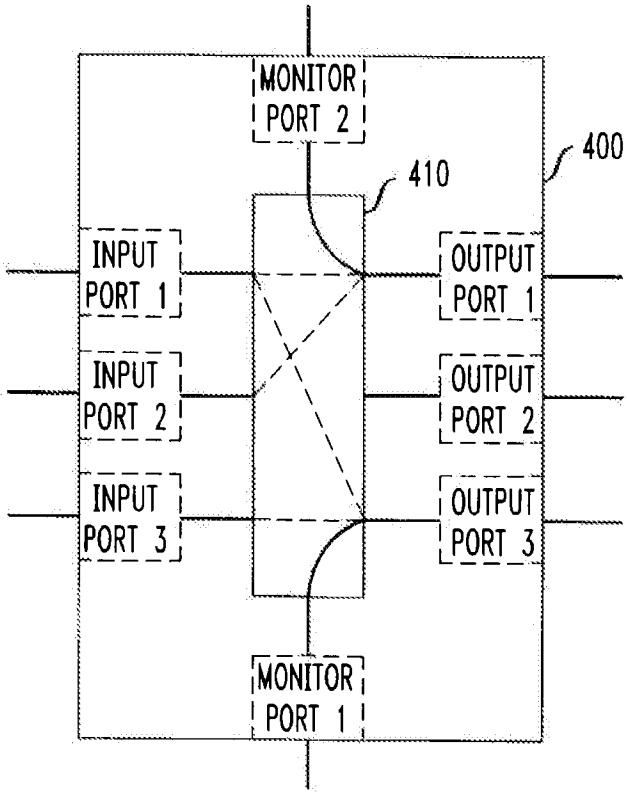


FIG. 6



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 841 832 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
19.05.1999 Bulletin 1999/20

(43) Date of publication A2:
13.05.1998 Bulletin 1998/20

(21) Application number: **97308622.6**

(22) Date of filing: **29.10.1997**

(51) Int Cl.[6]: **H04Q 11/04**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: **08.11.1996 US 746364**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

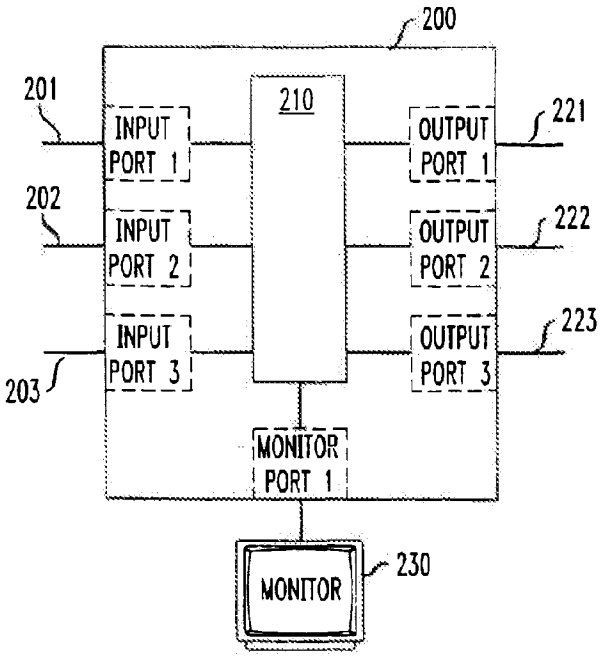
(72) Inventor: **Ramakrishnan, Kadangode K.**
Berkeley Heights, New Jersey 07922 (US)

(74) Representative: **Harding, Richard Patrick et al**
Marks & Clerk,
Nash Court,
Oxford Business Park South
Oxford OX4 2RU (GB)

(54) Promiscuous network monitoring utilizing multicasting within a switch

(57) Multicasting within a switch is utilized to promiscuously monitor switched communication networks. The switch routes data packets from input ports to data output ports and routes copies of the data packets to a monitor output port. A monitor processor is connected to the switch to receive copies of all data packets received at the switch, and thereby monitor the communication network.

FIG. 3



EP 0 841 832 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 8622

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	HENRION M A ET AL: "TECHNOLOGY, DISTRIBUTED CONTROL AND PERFORMANCE OF A MULTIPATH SELF-ROUTING SWITCH" PROCEEDINGS OF THE INTERNATIONAL SWITCHING SYMPOSIUM, YOKOHAMA, OCT. 25 - 30, 1992, vol. 2, no. SYMP. 14, 25 October 1992, pages 2-6, XP000337691 INSTITUTE OF ELECTRONICS;INFORMATION AND COMMUNICATION ENGINEERS * figure 2 * ---	1-16	H04Q11/04
A	LARSEN A K: "RMON COMES UP TO SPEED HIGH-SPEED LAN PROBES HAVE ARRIVED, BUT THEY'RE NOT THE ONLY MONITORING OPTION" DATA COMMUNICATIONS, vol. 25, no. 5, 1 April 1996, page 49/50, 52 XP000582659 * page 50, right-hand column, line 46 - line 55 * * page 52, middle column, line 49 - right-hand column, line 3 * ---	1	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	E. RABINOVITCH: "(Barely) managing ATM " AVAILABLE FROM INTERNET,1 August 1996, pages 1-9, XP002097454 http://www.sunworld.com/sunworldonline/swo1-08-1996/swol-08-ATM.HTML * page 3, line 33 - page 4, line 17 * --- -/--	1-11	H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 March 1999	Staessen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 8622

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document w th indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	ITOH A ET AL: "FUNCTION TEST METHODS USING TEST CELLS FOR ATM SWITCHING SYSTEM" COMMUNICATIONS - GATEWAY TO GLOBALIZATION. PROCEEDINGS OF THE CONFERENCE ON COMMUNICATIONS, SEATTLE, JUNE 18 - 22, 1995, vol. 2, 18 June 1995, pages 982-987, XP000533145 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS * the whole document *	1	
P,X	"Remote Monitoring MIB extensions for ATM networks" THE ATM FORUM TECHNICAL COMITTEE: , 1 May 1997, XP002097455 FTP://FTP.ATMFORUM.COM/PUB/APPROVED-SPECS/AF-NM-TEST-0080.000.pdf * paragraph 3.4 *	1-11	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 March 1999	Staessen, B

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 032 224 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.08.2000 Bulletin 2000/35

(51) Int. Cl.[7]: **H04Q 7/24**

(21) Application number: **00301375.2**

(22) Date of filing: **22.02.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **22.02.1999 US 120925 P**

(71) Applicant:
Selex Communications LLC.
Atlanta, Georgia 30324 (US)

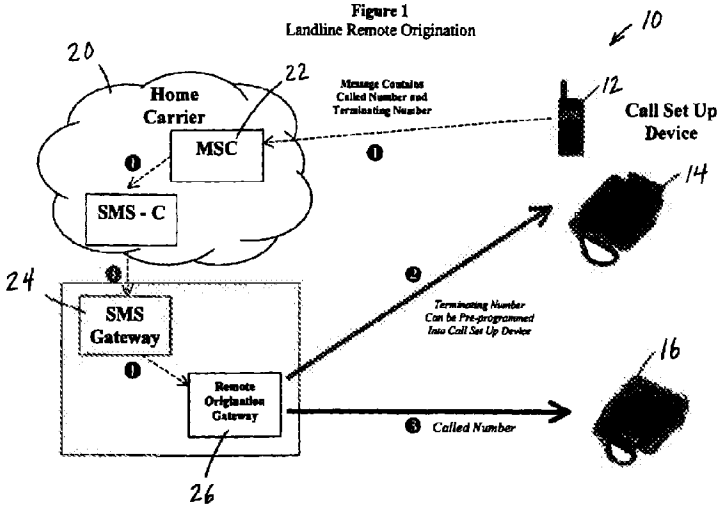
(72) Inventor: **Roach, Peter O., Jr.**
Atlanta, Georgia 30319 (US)

(74) Representative:
Orchard, Oliver John
JOHN ORCHARD & CO.
Staple Inn Buildings North
High Holborn
London WC1V 7PZ (GB)

(54) Method and apparatus for providing quasi mobile telephone service

(57) A telephone system and method allowing a user to set up landline calls using a mobile telephone. A user initiates outgoing calls by inputting into the mobile phone the phone numbers of a remote phone of a called party and a local landline phone convenient for use by the user. A message containing these phone numbers is sent by the mobile telephone to a remote telephone call origination platform, which establishes a bridging connection between the remote phone and the local phone. An incoming call is received by signaling the user of an incoming call on the mobile phone. The user inputs the number of a convenient landline phone into the mobile phone, which in turn signals the remote telephone call origination platform to forward the incoming call to the designated landline phone. The system and method are adaptable to PBX systems. Advantages of both mobile and landline phones are combined, and calling card-like billing/charging can be provided without the inconvenience of inputting calling card numbers and identification codes.

Figure 1
Landline Remote Origination



EP 1 032 224 A2

Description

[0001] The present invention relates generally to telephone systems and related telephone service methods and apparatus, and in particular it relates to a system and method combining features and advantages of mobile telephone, landline telephone, and calling card telephone systems and methods.

[0002] Currently, in many areas of the world there is limited competition in local, long distance, and international long distance telephone services. This limited competition may be due to several causes, such as regulatory constraints, exclusive concessions of the public switched telephone networks, and the high cost of service in a widely dispersed population in some locations, etc. In most instances, limited competition causes the local, long distance, and/or international long distance rates to the subscriber to be substantially higher than exist in competitive markets.

[0003] In a number of these areas around the world, there exists a local cellular carrier that competes with the local (landline) service provider. Oftentimes, these cellular carriers compete for a higher tier service (customers who can pay a higher cost) by providing mobility to the customer. Many of these cellular carriers desire to offer a service to lower tier customers- (customers with rather limited financial means). However, the higher cost of the infrastructure for cellular carriers and/or the restricted capacity of voice channels on cellular networks limit the ability of the cellular carriers effectively to reach these lower tier customers.

[0004] In the past, cellular carriers have attempted several methods to reach this lower tier customer group. Cellular carriers have used for example, pricing packages that offer free air time during off-peak hours, prepaid services, or restricted use packages (e.g. no roaming, inbound calling only, etc.) Most of these promotional techniques have met with limited success in attracting the lower tier customer groups. This is mainly due to the limited functionality of these cellular service packages as well as the continued high cost of the infrastructure required to offer such services. Thus, it has been found that a need exists for improved systems and methods of providing a telephone service combining the lower rates typical of a landline service with the mobility of a cellular service.

[0005] In addition, it has been found that many mobile cellular telephone users prefer to use a standard landline telephone when available, rather than a mobile phone. This preference can be due to the actual or the perceived differences in connection quality or service reliability, lower cost, or certain additional features provided by a landline service as compared to a mobile service. Also, many users prefer to use a landline service provided through a private branch exchange ("PBX") system or switchboard, when available. Because many users store frequently called telephone numbers in the memory of their mobile phones, however, it would be desirable to permit a user to utilize the automatic dialing features and stored number menus of their mobile phone when placing a call over a landline phone.

[0006] Many users also find it desirable to place calls utilizing a calling card, which may be a prepaid calling card or a periodically billed calling card. These calling cards permit users to take advantage of more favorable rates and/or consolidated billing for calls originated from different mobile and/or landline telephones. The use of a calling card, however, is often inconvenient as the user typically must input a calling card number and a personal identification number ("PIN") when placing a call for billing, identification and fraud-prevention purposes. Many times, a calling card user must also dial a service provider access number to originate a calling card call. It would be desirable to provide a system and method enabling users to obtain the benefits of calling card calling without suffering the disadvantages and inconveniences typically related thereto.

[0007] Accordingly, it can be seen that a need yet remains for a method and apparatus for providing a telephone service that is similar or in some ways comparable to a mobile telephone service, but which can be provided at a substantially lower cost. There is also a need for a system and method permitting a user to utilize memory and other features of a mobile phone to set up a landline call. In addition, a need remains for a system and method for providing calling card-like features without a number of the inconveniences typically found to result from the use of a calling card. It is to the provision of a method, system and associated apparatus meeting these and other needs that the present invention is primarily directed.

[0008] Briefly described, in a first preferred form a method illustrative of the present invention includes providing quasi-mobile telephone service using a mobile telephone, a data network, and a Remote Telephone Call Origination ("RTCO") platform. The mobile telephone is of the type which is capable of communicating with the data network. The method includes the steps of using the mobile telephone to dial a first telephone number and a second telephone number. The first and second telephone numbers are captured by the mobile telephone and are transmitted in a data message to a data network. The data message is relayed from the data network to the RTCO platform. The RTCO platform places a first call from the RTCO platform to the first telephone number. RTCO platform also places a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

[0009] Preferably, the mobile telephone uses short messaging for communicating with the data network.

[0010] Stated another way, preferably a cellular telephone is modified and is specially programmed to allow the user to specify not only the call (destination) telephone number (the first telephone number), but also the calling (origination) telephone number of a conven-

ient, nearby landline phone. The mobile telephone is programmed to originate a short message containing the calling number and the called number. This short message is transmitted to a platform that is programmed to originate a call to the calling telephone number (such as a nearby landline phone) that was specified by the user. The platform is programmed to originate another call to the called telephone number specified by the subscriber. The platform is programmed to connect (bridge) the two calls together in order to allow the call to be completed. This allows the user to use the cellular telephone to setup and initiate a call, and then to use a standard (lower cost) landline telephone to actually complete the voice path of the call.

[0011] In another aspect, a system illustrative of the present invention includes means for providing communication between a local device and a remote device. The system preferably includes an initiating device for receiving an input identifier of the remote device, and means for communicating a message containing the identifier of the remote device to a telecommunications network. The system preferably also includes remote telephone call origination means for receiving the message containing the identifier of the remote device from a telecommunications network, and for effecting a bridging connection between the local device and the remote device.

[0012] In a further arrangement illustrative of the present invention includes a system for providing communication between a remote device and a local device includes remote telephone call origination means for receiving an incoming call from the remote device over a telecommunications network and for communicating a message to announce the incoming call to an initiating device. The initiating device preferably includes means for inputting an identifier of the local device and communicating a message containing the identifier of the local device to the remote telephone call origination means. The remote telephone call origination means preferably receives the message containing the identifier of the local device and effects a bridging connection between the local device and the remote device.

[0013] Yet another method of establishing communication between a local device and a remote device to be described below, by way of example in illustration of the present invention, includes inputting an identifier of the remote device into an initiating device, communicating a message containing the identifier of the remote device via a telecommunications network to a remote telephone call origination means, and effecting a bridging connection between the local device and the remote device.

[0014] A further method for providing communication between a remote device and a local device to be described below by way of example in illustration of the present invention, includes receiving an incoming call from the remote device, via a telecommunications network, into a remote telephone call origination means. The method preferably also includes communicating a message to announce the incoming call to an initiating device, inputting into the initiating device an identifier of the local device, and communicating a message containing the identifier of the local device to the remote telephone call origination means, whereby a bridging connection can be effected between the local device and the remote device.

[0015] Yet a further illustrative method includes charging for the cost of a telephone call. The method preferably includes initiating a telephone call between a local device and a remote device using an initiating device, communicating a message containing information identifying the initiating device to a communications network, effecting a bridging connection between the local device and the remote device, and collecting billing information regarding the telephone call and charging at least a portion of the cost of the communication to an account associated with the initiating device.

[0016] By allowing the user to setup and initiate the call using a cellular network and actually to complete the call using a standard Public Switch Telephone Network ("PSTN), the user can have the benefits of both technologies. It provides the user with substantial mobility similar to a cellular service, while allowing the user to enjoy the lower cost and dependable voice transmission over the public switch telephone network.

[0017] A system and a method to be described below, by way of example in illustration of the present invention also advantageously enables a user to utilize the automatic calling menus, memory-stored telephone number registers and other features of their cellular mobile phones when placing (and/or receiving) calls over a landline phone, including a PBX or switchboard connected landline phone. For example, the user can remotely originate a landline telephone connection using their mobile phone, taking advantage of any automatic calling menus, memory-stored telephone number registers or other features available through the mobile phone.

[0018] The illustrative system and method to be described can also function as a "Virtual Calling Card," whereby the user obtains many benefits typically associated with a standard calling card without suffering many of the typical disadvantages and inconveniences of a calling card. Because the landline connection is remotely originated though a cellular mobile phone, the caller's identity can be automatically validated through the carriers home location register ("HLR") prior to completing the landline connection. This eliminates the need for the caller to input a calling card number and PIN with every call. The user can establish service with one or more carriers of their choice to obtain the rate structure and service plan best suited to their needs. The user's calls can be billed to the customer in a single statement, regardless of the point of connection.

[0019] A system and method to be described below by way of example in illustration of the present invention

is able to eliminate the need for the carrier to maintain a dedicated toll-free access network to offer "calling card" type services. The carrier can also select the most cost-effective location worldwide to originate telephone calls. As a result, carriers can pass their savings on to users in the form of lower rates, and/or can increase profit margins. In addition, an arrangement illustrative of the present invention allows cellular carriers to obtain revenue from landline calling.

[0020] In use, a user may take advantage of the illustrative method and apparatus by keeping his mobile telephone with him as he moves from place to place. When the user wants to place a call from his current location, he would find a convenient, nearby landline telephone and determine its telephone number. The user would then dial the destination telephone number and the nearby landline telephone number into the mobile telephone. The mobile telephone would then transmit this information in a message and ultimately the RTCO platform would call both the destination telephone number and the convenient, nearby landline telephone and connect the two calls together. In this way, the user could use a nearby landline telephone to complete a call, and have the charges routed to his own personal account, even though the landline telephone is not his telephone. For example, the landline telephone may be a public pay phone, a hotel phone, or another person's phone. In addition to allowing a user to move about and use whatever telephone is nearby and convenient, this method and apparatus allows multiple users to share a single landline telephone and each user to have his or her own account for charging or billing purposes. For example, migrant workers who are living temporarily in migrant housing could use an available "house" landline telephone and share the telephone, with each migrant worker having his or her own phone account. This would allow a large number of people to effectively share a telephone. Moreover, as the migrant worker would move from one job location to another, they would still have continuous, uninterrupted telephone service by virtue of the quasi-mobile service provided herein.

[0021] The present arrangement is also useful for receiving an incoming telephone call, whereby an incoming telephone call is re-routed from the user's mobile telephone to instead be directed to a nearby landline telephone. The cellular telephone is modified to be specially programmed to allow the phone to receive a data message (such as the standard ring command for cellular telephones) to indicate that there is an inbound call being attempted. The mobile telephone would then prompt the user to key in (input) the desired destination telephone number of a convenient, nearby landline phone. The mobile telephone would then put together a data message and communicate it (such as by using the short message service ("SMS") capabilities of the global system for mobile communications ("GSM") network) containing at least a destination telephone number of the nearby landline telephone that the user desires to receive the incoming telephone call with and identifying the called number. The data message is then routed to a platform that would receive the incoming call and the outbound call to the mobile telephone. The platform would be programmed to bridge these calls together to form a complete conversation.

[0022] While the present arrangement preferably uses a data network to relay messages from the mobile telephone to the RTCO platform, those skilled in the art will recognize that it is possible to have the mobile telephone communicate directly with the RTCO platform. Moreover, while a mobile telephone is preferred for initiating and rerouting calls (largely because of the widespread availability and low cost of such devices), those skilled in the art will also recognize that other devices could be employed to initiate and reroute calls. U.S. Patent No. 5,546,4 44 of Roach, et al, which is hereby incorporated herein by reference, discloses a way in which a control channel of a cellular mobile telephone can be used communicate data.

[0023] The following description and drawings disclose, by means of an example, the invention which is characterised in the appended claims, whose terms determine the extent of the protection conferred hereby.

[0024] In the drawings:-

Fig. 1 is a schematic illustration depicting a method and system for providing quasi-mobile telephone service according to a preferred form of the present invention, and specifically depicting the remote origination of telephone calls thereby,

Fig. 2 is a flow chart depicting the origination of telephone calls using the method and system described above,

Fig. 3 is a schematic illustration of a method and system for providing quasi- mobile telephone service according to a preferred form of the present invention, and specifically depicting termination of an incoming telephone call,

Fig. 4 is a flow chart depicting the termination of telephone calls using the method and system described above,

Fig. 5 is a schematic illustration of a method and system, according to a preferred form of the present invention, for establishing a telephone connection between a calling phone connected to a PBX or switchboard and a called phone, using a mobile phone to establish the connection, and

Fig. 6 is a schematic illustration of a method and system, according to another preferred form of the present invention, for providing calling card-like calling features when placing a call between a calling phone and a called phone using a mobile phone to establish the connection.

[0025] Referring now to the drawing figures, in which like reference numerals represent like parts throughout, the present arrangement includes a method

and system 10 for providing quasi-mobile telephone service, using an initiating device 12 to establish a connection between a local device 14 and a remote device 16. The system of the present arrangement preferably includes one or more computers and associated software for controlling the operation and switching according to the manner described herein. The associated software can be programmed into the memory of the computer or can be stored in a computer-readable medium according to known techniques. The method and system 10 preferably combine many of the advantages typical of one or the other of mobile or landline telephone service, while eliminating many of the disadvantages of each. Particular embodiments and applications of the method and system of the present invention are described in greater detail below. Although the present arrangement is described herein primarily with reference to examples directed to voice transmission applications conducted between telephones, it will be understood that the present arrangement is equally applicable to data transmission applications conducted between data transmission devices such as, for example, fax machines, computer modems, or the like.

[0026] In a preferred form of the present arrangement, described with particular reference to Figs. 1 and 2, a user (in this instance, the "calling party") utilizes a portable call initiating device 12 to establish a connection between a local (i.e., accessible for use by the caller) device 14 and a remote device 16. In preferred arrangements, the call initiating device 12 includes a mobile cellular telephone or another device capable of receiving and sending signals to and from a remote location, the local device 14 includes a local PSTN landline telephone in the vicinity of the calling party, and the remote device 16 includes a landline or mobile telephone available to a remote party (in this instance, the "called party"). To initiate an outgoing call using the method and system of the present arrangement, the calling party (or a third party initiating the call) preferably enters the telephone number or other unique identifier of the remote phone 16 on the mobile phone 12, as by using the mobile phone's keypad or a menu of phone numbers stored in the mobile phone's memory. The telephone number or other unique identifier of the local phone 14 is optionally entered by the calling party into the mobile phone 12, or can be stored in the memory of the mobile phone for automatic transmission upon initiation of a call. Alternatively, a default local phone number can be associated with the calling party on the calling party's home carrier network, the remote origination gateway, or elsewhere in the system. If a default local phone number is provided, the system can be configured to allow the calling party to override the default by inputting an override local phone number, or alternatively can require that all calls be conducted from the default local phone for security or other reasons. The mobile phone 12 formats a message including data identifying the remote number and optionally the local number, and transmits the message according to a standard electronic data communication protocol to an existing telecommunications network, such as a cellular telephone network. The message can be directly transmitted to the calling party's home cellular carrier network 20 or indirectly transmitted via a visited cellular carrier through one or more mobile switching centers ("MSC5") 22. The message preferably is transmitted over the network 20 using GSM SMS messaging. In a preferred form, the message is transmitted from the carrier network 20, preferably via an SMS gateway 24, to a remote origination gateway 26 including the RTCO platform. An SS7 message box is preferably provided, and the gateway is capable of originating voice and/or data telephone calls. The remote origination gateway 26 places a call to the local phone 14. A timer can be utilized to terminate the connection if the local phone 14 is not answered within a predetermined time interval, or if the local phone is busy. The calling party preferably answers the local phone 14, establishing a connection with the remote origination gateway 26. Upon completion of the connection with the local phone, the mobile phone can be disconnected automatically or manually by the calling party. The remote origination gateway 26 also places a call to the remote phone 16, simultaneously with or sequentially before or after the call is placed to the local phone 14. A timer can be utilized to terminate the connection if the remote phone 16 is not answered within a predetermined time interval. The called party preferably answers the remote phone 16, establishing a connection with the remote origination gateway 26. Upon connection with both the local phone 14 and the remote phone 16, the remote origination gateway 26 establishes a bridging connection between the local phone 14 and the remote phone 16, permitting voice or data transmission therebetween. The remote origination gateway 26 preferably monitors the call for disconnect at either the local phone 14 or the remote phone 16, and thereupon terminates the call. The system 10 can be configured for billing purposes to allocate all or a portion of the cost of the call to the account(s) of one or more of the initiating device 12, the local device 14, the remote device 16, and/or one or more third-party payers. According to optional and further preferred arrangements, the remote origination gateway 26 can be configured for conference calling. For example, users of one or more of the initiating device 12, the local device 14, and/or the remote device 16 can input the telephone number(s) or other unique identifiers of one or more additional parties to be conferenced in with the calling party and the called party.

[0027] Additionally or alternatively, one or more additional parties can call in to the remote origination gateway 26 to be conferenced in with the calling party and the called party.

[0028] Referring now with particular reference to Figs. 3 and 4, the method and system 10 of the present arrangement can be seen also to enable the connection

of an incoming call from a remote party at a remote phone or other remote device 16' (in this instance, the "calling party") to a user (in this instance, the "called party") at the local phone or other local device 14, via the user's mobile phone or other initiating device 12. An incoming call from the remote phone 16', directed to a telephone number or other unique identifier associated with the mobile phone 12 via an existing telecommunications network, is received at the mobile switching center (MSC) 22 of the user's home cellular carrier network 20. The MSC preferably forwards the incoming call to the remote origination gateway 26 on a "call forwarding-don't answer" ("CFDA") basis, connecting the remote phone 16 with the remote origination gateway 26. The remote origination gateway 26 preferably receives the incoming call and places the calling party on hold pending connection with the local phone 14. Live or recorded music or other entertainment, informational messages, advertising or other audible material can be broadcast to the parties while on hold. Simultaneously with or sequentially before or after forwarding the incoming call to the remote origination gateway 26, the MSC announces the call to the called party via the mobile phone 12, typically by means of a ring or other audible, tactile or visual signal, according to standard telecommunications protocol. Preferably, the mobile phone is configured to prevent the user from answering the call on the mobile phone, or is switchable to selectively permit or prevent answering calls on the mobile phone. A timer can be provided to terminate the call if the called party does not respond within a predetermined interval of time. Preferably, the called party acknowledges the incoming call signal and inputs the telephone number or other unique identifier of the local phone 14 to be used for receiving the incoming call, as by using the mobile phone's keypad or the menu of phone numbers stored in the mobile phone's memory. The mobile phone 12 transmits a message containing the local telephone number to be used for receiving the incoming call to the MSC, which signals the remote origination gateway 26 via the SMS gateway to place a call to the local phone 14. Alternatively, a default local phone number associated with the called party is transmitted to the MSC, which signals the remote origination gateway 26 to place a call to a default local phone 14. As discussed above, the default local phone number can be mandatory or subject to override. The called party then answers the local phone 14 to complete the connection between the local phone and the remote origination gateway 26. Upon connection between the local phone 14 and the remote origination gateway 26, the mobile phone 12 can be automatically or manually disconnected. The remote origination gateway 26 then establishes a bridging connection between the local phone 14 and the remote phone 16, permitting voice or data transmission therebetween. The remote origination gateway 26 preferably then monitors the call for disconnect at either the local phone 14 or the remote phone 16, and thereupon terminates the call. As described above, the system 10 optionally can be configured for conference calling with additional parties.

[0029] Figure 5 shows another arrangement illustrative of the present invention, wherein the local phone 14 is part of a PBX or other switchboard type of network 50. Preferably, the system, method and components of this arrangement are substantially as described above, with certain specific additions or modifications that will now be described. The user (in this instance, the "calling party") preferably initiates an outgoing call to a remote user (in this instance, the "called party") using the mobile cellular phone 12. A short message containing information regarding the telephone number of the remote phone 16 and the PBX switchboard 50 containing the user's local phone 14 is transmitted from the mobile phone 12 over a cellular communications network to a location server/messaging server 42. The location server/messaging server 42 communicates with the user's home carrier network 20 and the remote origination switch 26 substantially in the manner described above. The remote origination switch 26 places calls to the remote phone 16 and the PBX switchboard 50 substantially in the manner described above. In addition, the remote origination switch 26 places a temporary call to the mobile phone 12. A temporary bridging connection is established between the mobile phone 12 and the PBX switchboard 50, permitting the user to communicate with the PBX 50, via the mobile phone 12, to connect the call through the PBX to the local phone 14. This connection can be accomplished, for example, by keying in the PBX extension number of the local phone 14 on the keypad of the mobile phone 12 in the case of an automated switchboard; or alternatively, can be accomplished by voice in the case of an operator-answered switchboard. Upon connection of the local phone 14 to the remote origination switch 26, the temporary call from the remote origination switch to the mobile phone 12 is manually or automatically disconnected. The remote origination switch 26 then completes the bridging connection between the local phone 14 and the remote phone 16 substantially in the manner described above.

[0030] Figure 6 shows another preferred embodiment of the method and system of the present invention that is particularly adapted to provide telecommunication services having characteristics in the nature of an enhanced calling card. The user (in this instance, the "calling party") preferably initiates an outgoing call to a remote user (in this instance, the "called party") using the memory menu of the mobile cellular phone 12. A short message containing information regarding the telephone number of the remote phone 16 and the user's local phone 14 is transmitted from the mobile phone 12 over a cellular communications network, via a mobile switching center of a visited cellular carrier 40, to a location server/messaging server 42. In a preferred form, the location server/messaging server 42 includes an

SS7-IP gateway. The SS7-IP gateway converts an SS7 message to Internet protocol, and preferably carries out any necessary logic operations. Alternatively, logic operations can be completed on an SS7 box. The user's home carrier network 20 communicates with the location server/messaging server 42 to send routing information and user authorization, and to collect information for billing or charging the call to a prepaid service package. The home location register (HLR) of the home carrier network 20 validates the identity of the calling party according to standard cellular telecommunications fraud-prevention protocol, eliminating the need for the user to key in a calling card number and PIN for every call. In addition, because the call is set up using the existing cellular communications network, the need for a dedicated toll-free access network is eliminated. The location server/messaging server 42 communicates with the remote origination switch 26, which places calls to the local phone 14 and the remote phone 16, and completes the bridging connection between the local phone 14 and the remote phone 16 substantially in the manner described above.

[0031] A number of advantages and increased efficiencies are obtained by the arrangements described in illustration of the present invention. Billing information collected by the user's home carrier network 20 permits the user to be billed for all calls on a single statement, or permits all calls to be charged to a prepaid service plan, regardless of the locations of the one or more local phones 14 used to complete the calls, in much the same manner as is permitted with calling card systems. Because the connection between the local phone 14 and the remote phone 16 is maintained by the bridging connection provided by the remote origination switch 26, the system and method presently described permit a cellular carrier to obtain revenue from what would otherwise be a non-revenue generating, wholly landline connection. Consumers, however, can benefit from rates lower than standard calling card rates for landline connections, as the cellular carrier can route calls and manage billing more efficiently using the method and system described than is the case with standard landline connections using calling cards. In addition, consumers benefit from increased convenience, as the present arrangement enables landline calls to be initiated using calling information stored in the memory registers of a mobile phone, and obviates the need for remembering and dialing access numbers, calling card numbers and PINs. The system and method of the present arrangement also, advantageously, are not reliant on the touch tone quality of the local phone. Some hotels, for example, modify the touch tone signals of room phones to prevent users from using calling cards and thereby require them to pay the hotel's rates for phone connections. The present invention allows the call to be initiated using a mobile phone, bypassing any effect of altered touch tone quality of a local phone within a hotel's PBX network.

[0032] In optional and further arrangements, the system 10 includes voice mail messaging means, whereby an incoming call is directed to a recording device for recording a message from the calling party for later playback by the called party. The voice mail messaging means is preferably automatically activated in the event that the mobile phone 12 or the local phone 14 are in use at the time of the incoming call. The voice mail messaging means can preferably be selectively activated by the called party by signaling the MSC, via the mobile phone 12, to forward the call to voice mail upon receiving an incoming call signal. The system 10 optionally also includes caller ID means for identifying the calling party to the called party upon signaling an incoming call on the mobile phone 12, permitting the called party to screen incoming calls.

[0033] One unique application of the present arrangement is the enablement and implementation of a region-wide prepaid service providing significant advantages over existing calling-card systems or prepaid service plans. Since both incoming and outgoing calls are routed through the remote origination platform, a cellular carrier can provide a prepaid service (local, long distance and international long distance) on a region-wide or worldwide basis, This is a significant improvement over the standard prepaid service offered by cellular carriers in that it can be extended beyond the subscriber's local service coverage area. Moreover, with this arrangement a cellular carrier can prohibit or selectively restrict the use of the cellular voice channels. The carrier can restrict the usage on a time of day basis, originating network basis (restrict roaming capabilities or home zone only capabilities), the input of an access code, etc. The restriction of voice channel dapabilities can be remotely programmed using a data channel such as the short message service channel. In this arrangement, the mobile phone or other initiating device 12 functions solely as a control device for the system 10. This capability can be provided on a specially made device or on a standard cellular phone modified with special programming, such as a GSM phone using a subscriber identification module ("SIM") toolkit. The method and system of the present arrangement advantageously utilize the home location register (HLR) database, or other pre-existing user verification system of a cellular carrier to identify the mobile telephone or other initiating device from which the incoming call to the cellular network is being placed. By identifying the calling party upon receiving an incoming call to the network in this manner, the carrier can confirm that the calling party is an authorized user, collect information for billing and charging purposes, control the terms of connection, and conduct a variety of other operations. For example, the carrier can limit the duration of calls, specify authorized call destinations, limit the time periods during which calls can be placed, specify the types of calls (e.g., voice, data), etc.

[0034] The call set-up time for this quasi-mobile

service may be slightly longer than standard call set-up times using existing wireless networks. This extra time will most likely result from the necessity of requesting and receiving user input to complete the conversation. A cellular carrier may desire to offer voice announcements during a call set-up. These announcements can be provided either to the originating party or the terminating party during the call set-up.

[0035] Once the phone conversation is established through the remote origination gateway (RTCO) it is possible to provide other features through the cellular telephone. These features optionally include advanced call conferencing, call forwarding, special announcements, or any other telephony features. For mobile originated calls it is possible for the cellular carrier to populate the calling line ID field, from the remote gateway, with the telephone number of the users mobile telephone (i.e., the initiating device 12), the user's home telephone number, or another designated telephone number or identification field, regardless of the location and telephone number of the local phone 14 that is the actual destination of the telephone call used by the calling party to complete the call. This will allow the called party to receive the calling line ID of the calling party, and will allow the calling party to have the appearance of maintaining a consistent telephone number regardless of their location and regardless of the telephone number of the local phone actually used by the calling party. Optionally, the calling line ID of the calling party can be transmitted from the remote gateway to the calling party's local phone 14, as well as the remote phone 16, in order to identify the incoming call to the calling party for call screening purposes.

[0036] While the present invention has been described with reference to various preferred arrangements by way of example, it will be readily apparent to those of ordinary skill in the art that many additions, deletions and modifications can be made thereto, and other arrangements conceived without departing from the scope of the protection sought for the invention as defined in the claims which follow.

Claims

1. A method of providing a quasi-mobile telephone service using an RTCO platform, a data network, and a mobile telephone of the type capable of communicating with the data network, the method including the steps of:

   using the mobile telephone to dial a first telephone number and a second telephone number;
   capturing the first telephone number and a second telephone number;
   transmitting a data message to the data network, with the data message including the first and second telephone numbers;
   relaying the data message from the data network to the RTCO platform;
   placing a first call from the RTCO platform to the first telephone number; and
   placing a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

2. A method as claimed in claim 1 wherein the mobile telephone uses short messaging for communicating with the data network.

3. A method as claimed in claim 1 wherein the mobile telephone is used to reroute incoming calls to another telephone by detecting that an incoming call is being placed to the mobile telephone and sending a message to the RTCO platform to redirect the incoming call to the other telephone.

4. A method as claimed in claim 1 wherein the data network identifies the mobile telephone through a home location register.

5. A method as claimed in claim 1 wherein the data network transmits caller identification information to at least one of the first and second telephone numbers.

6. A method of providing a quasi-mobile telephone service using an RTCO platform and a mobile telephone, the method including the steps of:

   using the mobile telephone to dial a first telephone number and a second telephone number;
   capturing the first telephone number and a second telephone number;
   transmitting a data message to the RTCO platform, with the data message including the first and second telephone numbers;
   placing a first call from the RTCO platform to the first telephone number; and
   placing a second call from the RTCO platform to the second telephone number in a manner to connect the first and second calls to each other.

7. A method as claimed in claim 6 wherein the RTCO platform identifies the mobile telephone through a home location register.

8. A method as claimed in claim 6 wherein the RTCO platform transmits caller identification information to at least one of the first and second telephone numbers.

9. A system for providing communication between a

local device and a remote device, the system including:

an initiating device for receiving an input identifier of the remote device, and communicating a message containing the identifier of the remote device to a telecommunications network;
remote telephone call origination means for receiving the message containing the identifier of the remote device from a telecommunications network, and for effecting a bridging connection between the local device and the remote device.

10. A system as claimed in claim 9, wherein the initiating device includes a mobile telephone.

11. A system as claimed in claim 10, wherein the local device includes a landline telephone.

12. A system as claimed in claim 9, wherein the initiating device receives input identifiers of the local device and the remote device and communicates a message containing both identifiers to the telecommunications network, and wherein the remote telephone call origination means receives the message containing both identifiers and effects the bridging connection by calling the local device and the remote device.

13. A system as claimed in claim 12, wherein the telecommunications network identifies the initiating device through a home location register.

14. A system as claimed in claim 12 wherein the telecommunications network transmits caller identification information to at least one of the local and remote devices.

15. A system as claimed in claim 9, wherein the remote telephone call origination means effects connection of at least one additional device with the local device and the remote device for conference communications.

16. A system as claimed in claim 9, further including means for charging at least a portion of the cost of the communication to an account associated with the initiating device.

17. A system as claimed in claim 16, wherein the means for charging at least a portion of the cost of the communication to an account associated with the initiating device includes means for identifying the initiating device without the need for inputting identification information into the initiating device.

18. A system as claimed in claim 9, wherein the remote telephone call origination means includes a remote origination gateway.

19. A system as claimed in claim 9, wherein the initiating device further includes a signaling device for announcing an incoming call from a remote calling device, and means for communicating a message to the remote telephone call origination means containing an identifier of a local receiving device; and wherein the remote telephone call origination means includes means for effecting a bridging connection between the remote calling device and the local receiving device.

20. A system as claimed in claim 9, wherein the local device is one of a plurality of devices within a network, and wherein the initiating device communicates a message through the remote telephone call origination means to specify the local device and effect the bridging connection.

21. A system for providing communication between a remote device and a local device, the system including remote telephone call origination means for receiving an incoming call from the remote device over a telecommunications network and for communicating a message to announce the incoming call to an initiating device, wherein the initiating device includes means for inputting an identifier of the local device and communicating a message containing the identifier of the local device to the remote telephone call origination means, whereby the remote telephone call origination means receives the message containing the identifier of the local device and initiates a bridging connection between the local device and the remote device.

22. A system as claimed in claim 21, further including voice mail messaging means for recording a message from the remote device if the bridging connection is not completed.

23. A method of establishing communication between a local device and a remote device, the method including:

inputting an identifier of the remote device into an initiating device;
communicating a message containing the identifier of the remote device via a telecommunications network to a remote telephone call origination means; and
effecting a bridging connection between the local device and the remote device.

24. A method as claimed in claim 23, including inputting identifiers of the local device and the remote device into the initiating device, and communicating a mes-

sage containing both identifiers via the telecommunications network to the remote telephone call origination means.

25. A method as claimed in claim 23, further including connecting at least one additional device with the local device and the remote device, to establish a conference communication.

26. A method as claimed in claim 23, further including collecting billing information regarding the communication and charging at least a portion of the cost of the communication to an account associated with the initiating device.

27. A method as claimed in claim 26, wherein the step of charging at least a portion of the cost of the communication to an account associated with the initiating device includes identifying the initiating device without inputting identification information into the initiating device.

28. A method as claimed in claim 23, further including communicating a message from the initiating device to the remote telephone call origination means to specify the local device among a plurality of devices within a network.

29. A method as claimed in claim 23, further including identifying the initiating device through a home location register of the telecommunications network.

30. A method as claimed in claim 23, further including transmitting caller identification information to at least one of the local and remote devices.

31. A method for providing communication between a remote device and a local device, the method including:

receiving an incoming call from the remote device, via a telecommunications network, into a remote telephone call origination means;
communicating a message to announce the incoming call to an initiating device;
inputting into the initiating device an identifier of the local device; and
communicating a message containing the identifier of the local device to the remote telephone call origination means, whereby a bridging connection can be effected between the local device and the remote device.

32. A method as claimed in claim 31, further including recording a message from the remote device on a recording device if the bridging connection is not effected.

33. A method of charging for the cost of a telephone call including:

initiating a telephone call between a local device and a remote device using an initiating device;
communicating a message containing information identifying the initiating device to a communications network;
effecting a bridging connection between the local device and the remote device; and
collecting billing information regarding the telephone call and charging at least a portion of the cost of the communication to an account associated with the initiating device.

34. A method as claimed in claim 33, including identifying the initiating device via a home location register of the communications network.

Figure 1
Landline Remote Origination

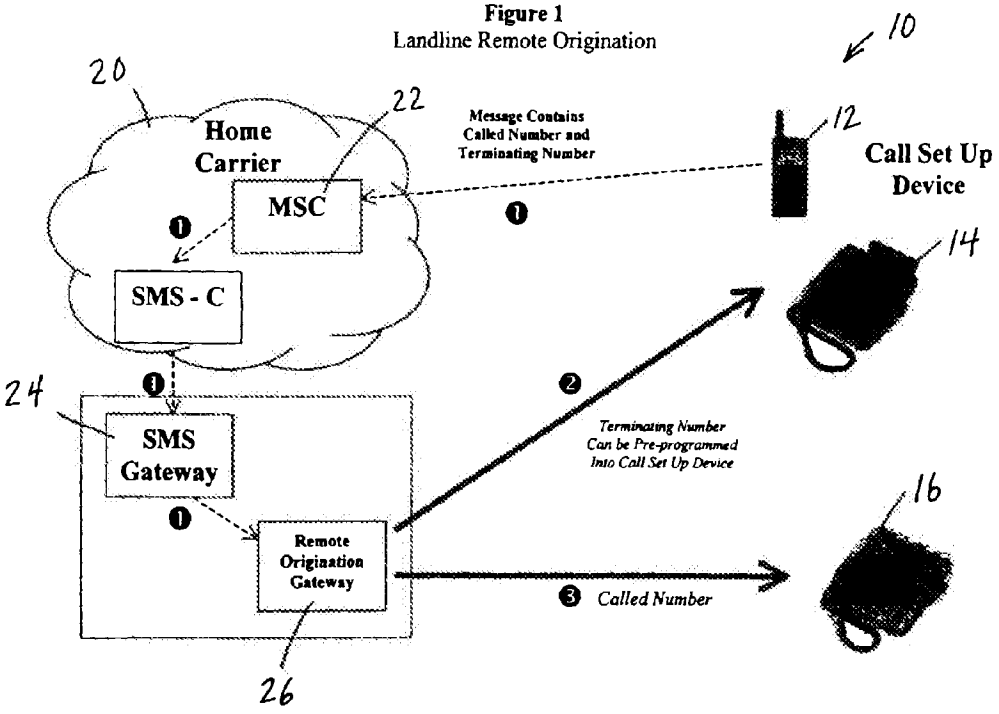


Figure 3
Landline Remote Termination

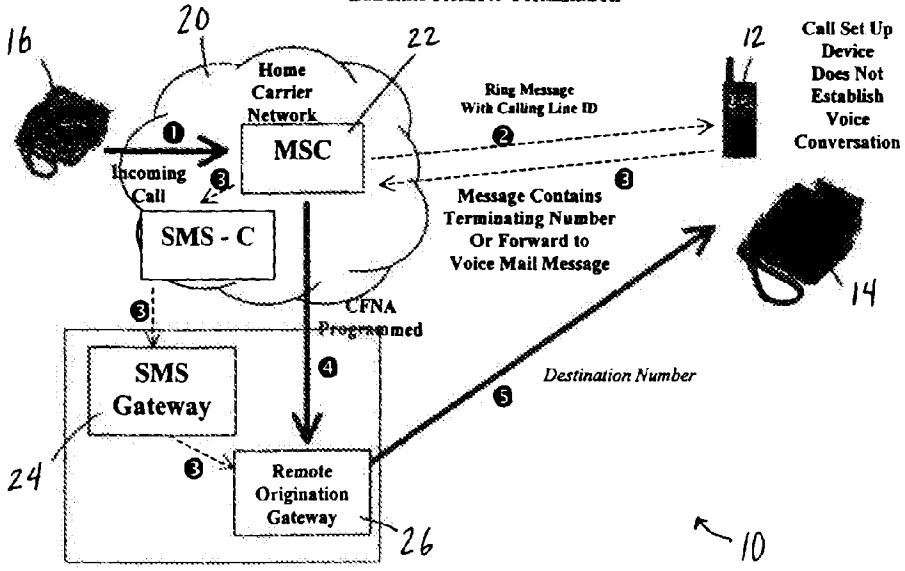


FIGURE 2

(Origination of telephone calls)

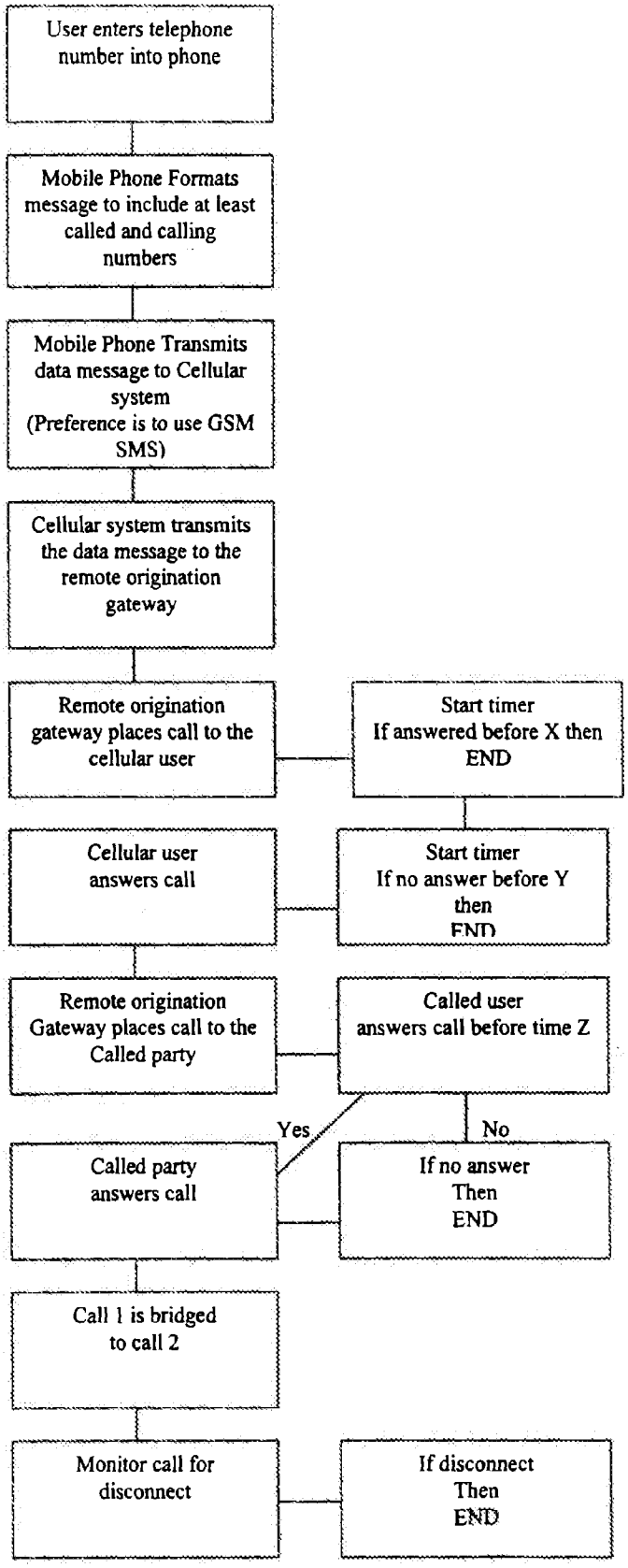


FIGURE 4
(Termination of telephone calls)

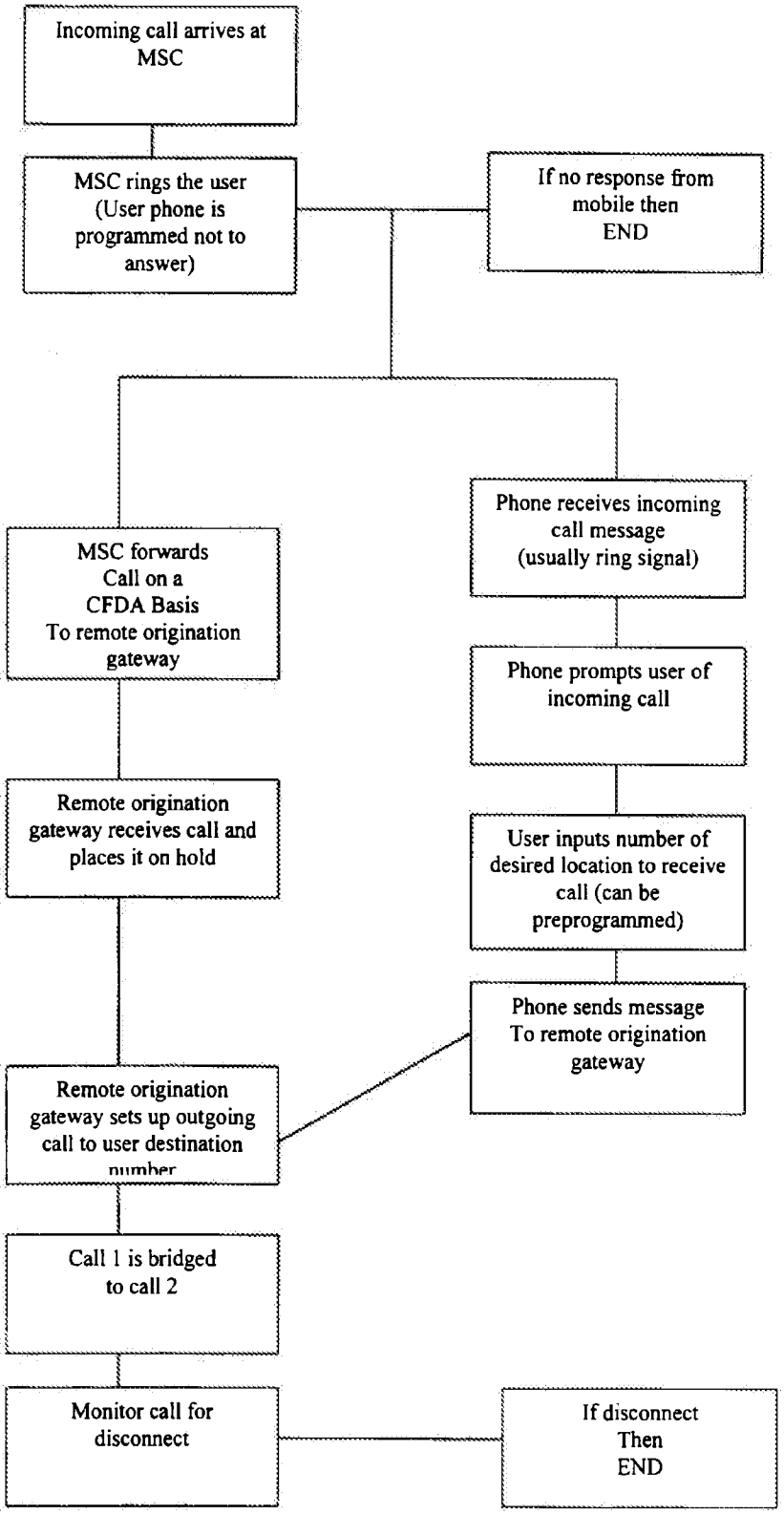


Figure 5

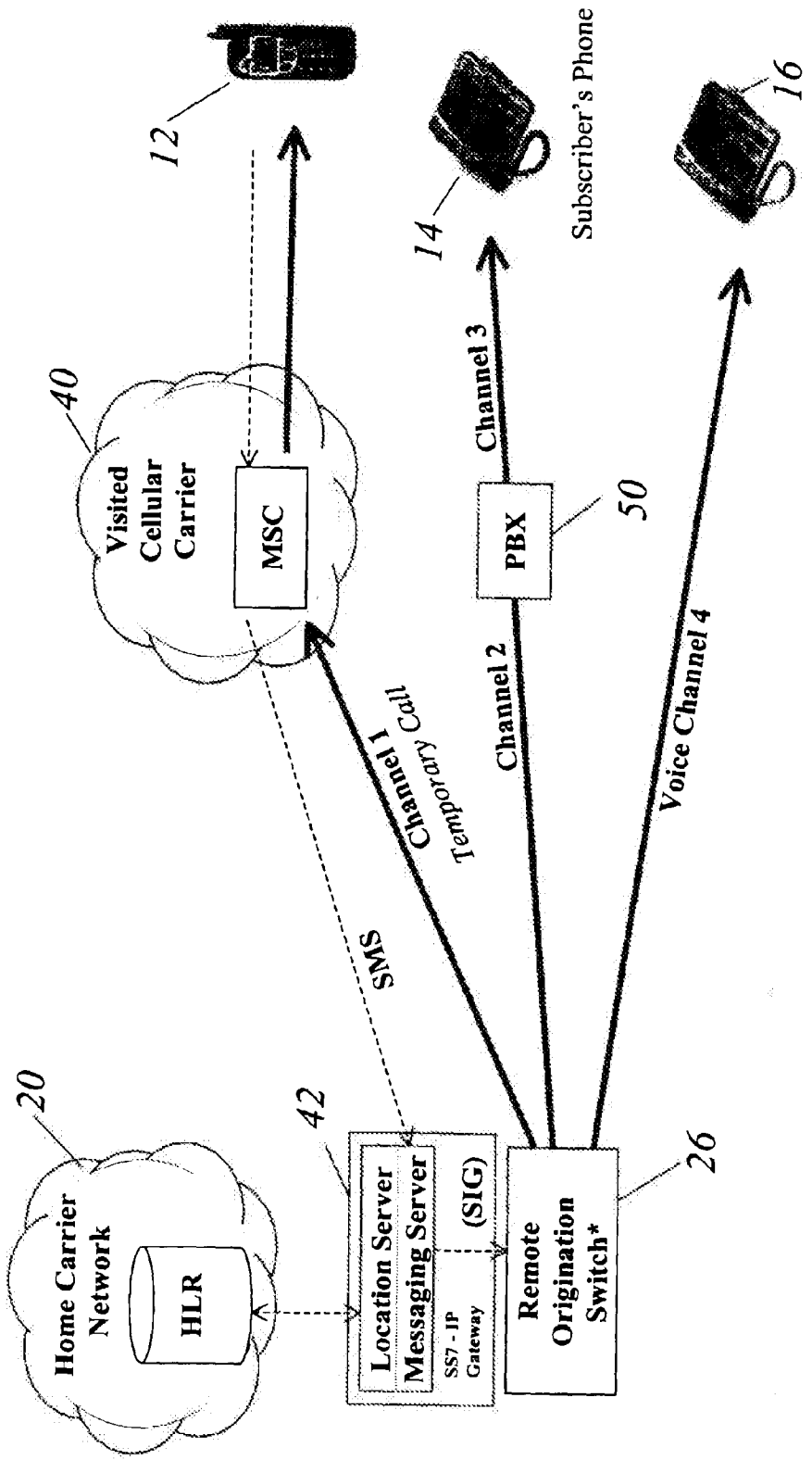
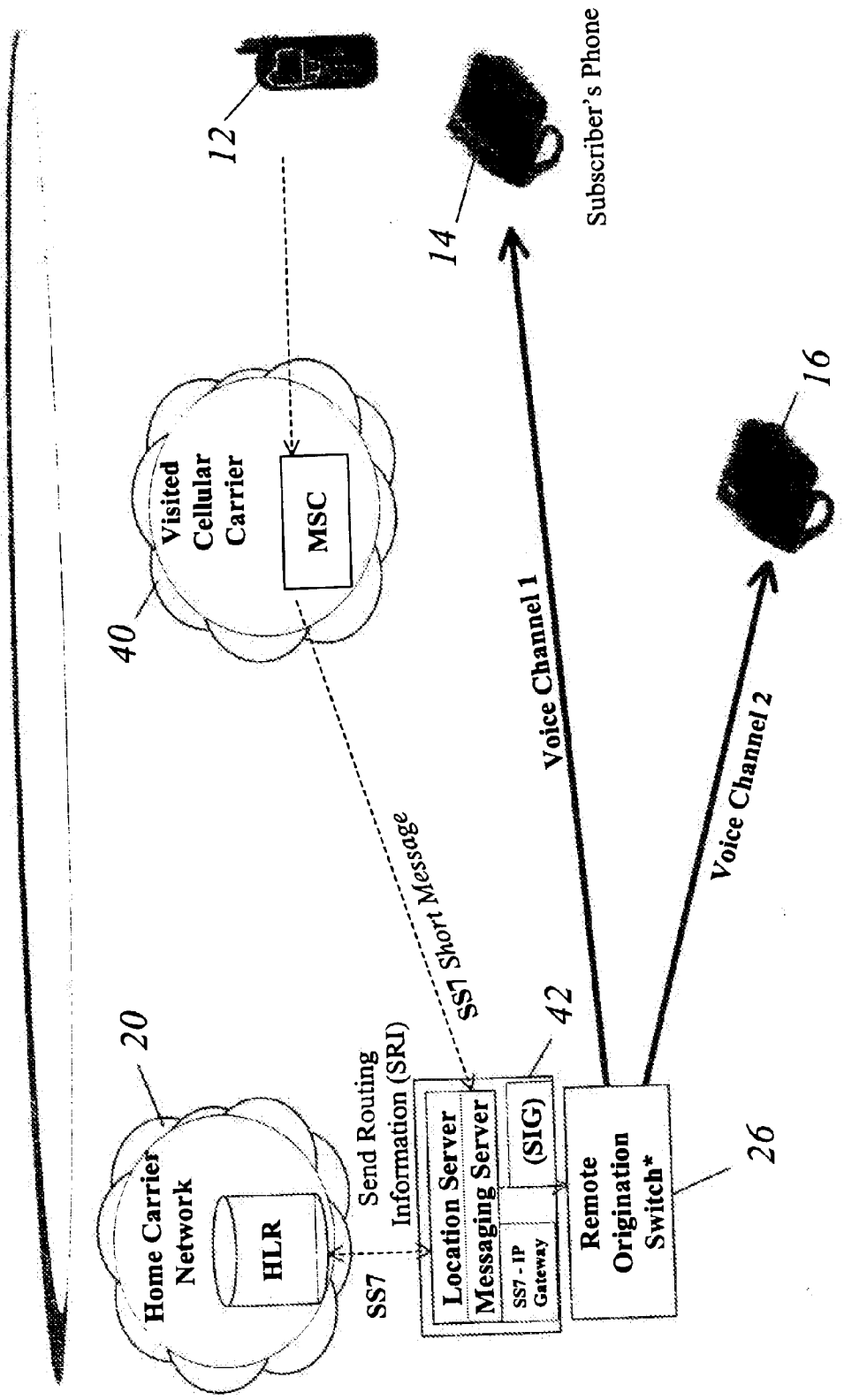


Figure 6



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 032 224 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
07.02.2001 Bulletin 2001/06

(43) Date of publication A2:
30.08.2000 Bulletin 2000/35

(21) Application number: **00301375.2**

(22) Date of filing: **22.02.2000**

(51) Int. Cl.[7]: **H04Q 7/24**, H04Q 7/38

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **22.02.1999 US 120925 P**

(71) Applicant:
Selex Communications LLC.
Atlanta, Georgia 30324 (US)

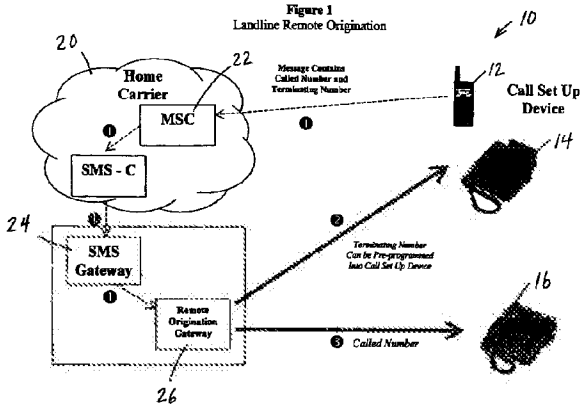
(72) Inventor: **Roach, Peter O., Jr.**
Atlanta, Georgia 30319 (US)

(74) Representative:
Orchard, Oliver John
JOHN ORCHARD & CO.
Staple Inn Buildings North
High Holborn
London WC1V 7PZ (GB)

(54) Method and apparatus for providing quasi mobile telephone service

(57) A telephone system and method allowing a user to set up landline calls using a mobile telephone. A user initiates outgoing calls by inputting into the mobile phone the phone numbers of a remote phone of a called party and a local landline phone convenient for use by the user. A message containing these phone numbers is sent by the mobile telephone to a remote telephone call origination platform, which establishes a bridging connection between the remote phone and the local phone. An incoming call is received by signaling the user of an incoming call on the mobile phone. The user inputs the number of a convenient landline phone into the mobile phone, which in turn signals the remote telephone call origination platform to forward the incoming call to the designated landline phone. The system and method are adaptable to PBX systems. Advantages of both mobile and landline phones are combined, and calling card-like billing/charging can be provided without the inconvenience of inputting calling card numbers and identification codes.

Figure 1
Landline Remote Origination



EP 1 032 224 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 1375

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 97 29609 A (HEIMANN JOSEF ;MANNESMANN AG (DE); SCHULZ WERNER (DE); HOESL ASTRI) 14 August 1997 (1997-08-14)	1,2,4,6, 7,9-13, 20,23, 24,28, 29,33,34	H04Q7/24 H04Q7/38
A	* page 5, line 4 - page 8, line 21 *	21,22, 31,32	
X	WO 92 01350 A (TELLER DAVID M) 23 January 1992 (1992-01-23)	1,4,6,7, 9-13,16, 17,20, 23,24, 26-29, 33,34	
A	* page 10, line 20 - page 15, line 27 *	21,22, 31,32	
X	US 5 839 067 A (JONSSON BJOERN ERIK) 17 November 1998 (1998-11-17) * column 8, line 58 - column 14, line 5 *	6,9-11	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q
H04M

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	18 December 2000	Weinmiller, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 1375

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

18-12-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9729609 A	14-08-1997	AU 2565297 A	28-08-1997
		DE 19780071 D	08-04-1999
		EP 0879543 A	25-11-1998
WO 9201350 A	23-01-1992	NONE	
US 5839067 A	17-11-1998	AU 707405 B	08-07-1999
		AU 4461196 A	31-07-1996
		CA 2197859 A	18-07-1996
		CN 1172571 A	04-02-1998
		EP 0803168 A	29-10-1997
		FI 971514 A	11-04-1997
		JP 10512123 T	17-11-1998
		NO 973140 A	28-08-1997
		SE 9500066 A	11-07-1996
		WO 9622000 A	18-07-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP1244250 (A1) — 2002-09-25

Method and telecommunication system for monitoring data streams in a data network

Inventor(s): KREUSCH NORBERT [DE]; PFAEHLER WOLFGANG [DE]; STIFTER HELMUT [DE] ± (KREUSCH, NORBERT, ; PFAEHLER, WOLFGANG, ; STIFTER, HELMUT)

Applicant(s): SIEMENS AG [DE] ± (SIEMENS AKTIENGESELLSCHAFT)

Classification: **- international:** ***H04L12/26; H04L29/06; H04L29/08; H04M3/22;*** (IPC1-7): H04L12/26; H04L29/06

- cooperative: **H04L12/2602**; **H04L29/06**; **H04L43/00**; **H04L63/00**; **H04L63/30**; **H04L65/103**; **H04L65/1046**; **H04L65/80**; **H04L67/2814**; **H04L67/306**; **H04M3/2281**; H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

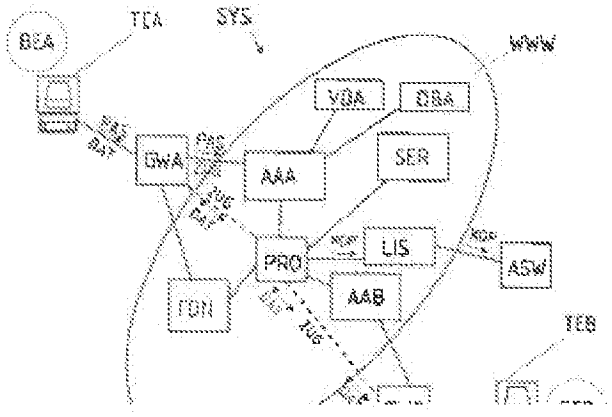
Application number: EP20010107063 20010321

Priority number(s): EP20010107063 20010321

Also published as: US2004181599 (A1) US7979529 (B2) RU2003130974 (A) RU2280331 (C2) EP1371173 (A1) EP1371173 (B1) WO02082728 (A1) CN1498482 (A) CN1274114 (C) BR0208272 (A) less

Abstract of EP1244250 (A1)

A data stream (DAT) is monitored in a data network (WWW) between two telecommunications terminals (TEA,TEB) connected to the data network via access servers (AAA,AAB), which operate during a monitoring situation to divert the data stream between the telecommunications terminals through a monitoring server (PRO) that produces a copy (KOP) of the data stream and transmits it to an



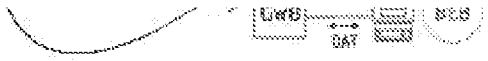


Fig. 1

analyzing unit (ASW). An independent claim is also included for a telecommunication system for monitoring a data stream in a data network between a telecommunications terminal linked to a data network via a gateway and to a further telecommunications device.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 244 250 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
25.09.2002 Patentblatt 2002/39

(51) Int Cl.7: **H04L 12/26**, H04L 29/06

(21) Anmeldenummer: **01107063.8**

(22) Anmeldetag: **21.03.2001**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

(72) Erfinder:
- **Kreusch, Norbert**
  82061 Neurled (DE)
- **Pfaehler, Wolfgang**
  85221 Dachau (DE)
- **Stifter, Helmut**
  81739 München (DE)

(54) Verfahren und Telekommunikationssystem zur Überwachung eines Datenstroms in einem Datennetz

(57) Ein Verfahren und ein Telekommunikationssystem (SYS) zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest zwei Telekommunikationsendgeräten (TEA, TEB), die über zumindest einen Zugangsserver (AAA, AAB) mit dem Datennetz verbunden sind, wobei von dem Zugangsserver (AAA, AAB) in einem Überwachungsfall der Datenstrom (DAT) zwischen den Telekommunikationsendgeräten (TEA, TEB) über einen Überwachungsserver (PRO) umgeleitet wird, der eine Kopie (KOP) des Datenstroms (DAT) erstellt und an eine Auswerteeinheit (ASW) übermittelt.

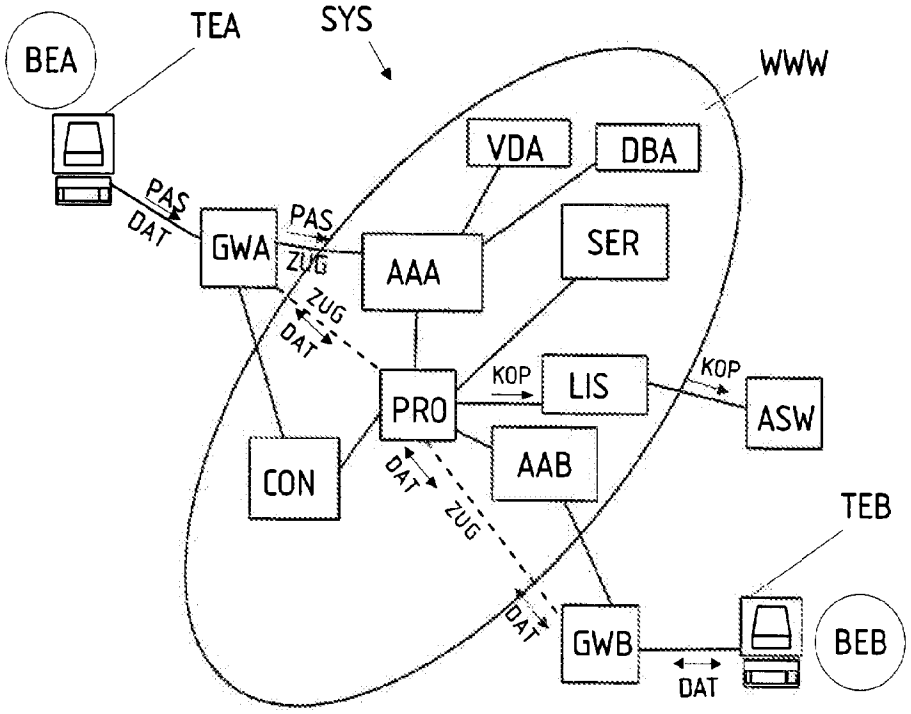


Fig. 1

EP 1 244 250 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

[0002] Weiters betrifft die Erfindung ein Telekommunikationssystem, welches zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung eingerichtet ist, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

[0003] Von Gesetzgebern wird in zunehmenden Maß verlangt, dass Betreiber von Datennetzen Funktionen zur Verfügung stellen, die es ermöglichen im Bedarfsfall den Datenaustausch einzelner Benutzer zu überwachen.

[0004] Das legale Abhören von Datenströmen die sogenannte "Lawful Interception" in Datennetzen, beispielsweise dem Internet, wird zur Zeit unterschiedlich gelöst.

[0005] Eine bekannte Methode besteht darin, externe Sniffer (Analysatoren) in einem LAN-Segment des zu Überwachenden anzuordnen, welche den gesamten Paket-Datenstrom analysieren und den Verkehr des Überwachten ausfiltern, vervielfältigen und dem Bedarfsträger zustellen. Nachteilig an dieser Methode ist vor allem, dass ein zeitlich befristeter, physikalischer Eingriff in das Netz erforderlich ist. Bei erhöhter Mobilität des zu Überwachenden ist diese Methode praktisch nicht verwendbar.

[0006] Eine andere Methode, die vor allem zum Abhören/Überwachen des e-Mailverkehrs dient, sieht vor, dass an einem oder mehreren e-Mailservern eine automatische Weiterleitungsfunktion implementiert ist, die sowohl ankommende als auch abgehende e-Mails dem Bedarfsträger, beispielsweise eine Behörde, zustellt. Ähnliches gilt für Voice-Mail etc. Bei dieser Methode ist es erforderlich, dass alle e-Mailserver dazu eingerichtet sein müssen, einen Abhör/Überwachungsfall zu erkennen und an die zuständige Behörde weiterzuleiten, was mit einem hohen administrativen Aufwand verbunden sein kann.

[0007] Aus der WO 0042742 sind eine Überwachungsmethode und ein Überwachungssystem zur Durchführen eines gesetzlichen Abhorchens in einem paketorientierten Netz, wie dem GPRS- oder dem UMTS-Netz beschrieben. Hierzu ist ein erst Netzelement mit Überwachungsfunktionalität für Datenpakete vorgesehen, welches durch ein zweites Netzelement gesteuert wird. Die abgefangenen (überwachten) Daten werden über ein Gateway, welches eine Schnittstelle zu einer zum Abhören berechtigten Behörde darstellt. Nachteilig an dieser Methode ist vor allem, dass auch Datenströme von Benutzern, die nicht abgehört werden sollen durch das Netzelement geführt werden, wodurch sich der technische und administrative Aufwand dieser Methode wesentlich erhöht.

[0008] Zur "Lawful Interception" im Internet siehe beispielsweise ETSI TR 101 750 V1.1.1.

[0009] Nicht außer Acht zu lassen sind die sehr hohen Kosten, die üblicherweise für einen Netzbetreiber bei zur Verfügungstellung der oben erwähnten Abhör/Überwachungsfunktionalität anfallen, die vor allem durch einen hohen administrativen Aufwand verursacht werden.

[0010] Es ist daher eine Aufgabe der Erfindung einen Weg zu schaffen, der es auf einfache und kostengünstige Weise ermöglicht, eine Abhör/Überwachungsfunktion in einem Datennetz zu implementieren und anzubieten.

[0011] Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art dadurch gelöst, dass von dem zumindest einem Authentifikationsserver überprüft wird, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei in einem Überwachungsfall eine Kopie des Datenstroms erstellt wird, welcher eine Identifikationskennzeichnung beigefügt wird, und die Kopie samt Identifikationskennzeichnung hierauf an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit übermittelt wird.

[0012] Es ist ein Verdienst der Erfindung, eine Abhörfunktionalität von seiten des Netzes zur Verfügung zu stellen, wodurch ein Eingriff mittels externer Abhörgeräte in das Netz vermieden werden kann. Weiters ist ein Zugriff auf einen Datenstrom eines zu Überwachenden auch dann möglich, wenn er mobil ist und seinen Standort ändert, da er sich über den Authentifizierungsserver eines Providers, der die Maßnahmen zur Überwachung setzt, einwählen muss.

[0013] In einer Variante der Erfindung wird die Kopie von dem Gateway erstellt.

[0014] Eine andere Variante der Erfindung sieht vor, dass die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver erstellt wird.

[0015] Vorteilhafterweise stellt der LI-Server anhand einer Identifikationskennzeichnung fest, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll(en).

[0016] Günstigerweise erstellt der LI-Server die zumindest eine Sekundärkopie, d.h. der LI-Server vervielfältigt die Kopie entsprechend der Anzahl der berechtigten Stellen.

[0017] Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server eine Schnittstellenanpassung zu der Auswerteeinheit durchführt.

[0018] Der Authentifizierungsserver kann anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwachungskennzeichnung feststellen, ob ein Überwachungsfall vorliegt.

[0019] Die verborgene Datenbank steht mit einer Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet wird.

[0020] Im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank werden auch die zugeordneten Überwachungskennzeichnungen in der verborgenen Datenbank gelöscht.

[0021] In einer weiteren Variante der Erfindung wird der Datenstrom als Voice over IP-Datenstrom übertragen, wobei ein Call-Controller den Datenstrom über den Überwachungsserver, der die Kopie erstellt, umleitet.

[0022] Eine andere Möglichkeit besteht darin, dass der Authentifizierunsserver in einem Überwachungsfall den Datenstrom über den Überwachungsserver umleitet.

[0023] Eine Variante des Umleitens besteht darin, dass der Datenzugang von dem Gateway zu dem Überwachungsserver durchgetunnelt wird.

[0024] Um einen Datenverlust zu vermeiden, falls die Kopie nicht sofort an einen Bedarfsträger zugestellt werden kann, kann die Kopie des Datenstroms auf dem Überwachungsserver und/oder auf dem LI-Server zwischengespeichert werden.

[0025] In einer bevorzugten Ausführungsform der Erfindung steuert der Controller sowohl das Gateway als auch den Überwachungsserver.

[0026] Eine weitere sehr vorteilhafte Ausführungsform der Erfindung sieht vor, dass der zumindest eine Authentifizierungsserver den Überwachungsserver steuert.

[0027] Zur Durchführung des erfindungsgemäßen Verfahrens eignet sich insbesondere ein Telekommunikationssystem der eingangs genannten Art, bei welchem der Authentifikationsserver dazu eingerichtet ist, zu überprüfen, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei das Telekommunikationssystem dazu eingerichtet ist, in einem Überwachungsfall eine Kopie des Datenstroms zu erstellen und der Kopie eine Identifikationskennzeichnung hinzuzufügen und die Kopie samt Identifikationskennzeichnung an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit zu übermitteln.

[0028] In einer ersten Variante der Erfindung ist das Gateway dazu eingerichtet, die Kopie des Datenstroms zu erstellen.

[0029] Bei einer zweiten Variante der Erfindung ist ein Überwachungsserver vorgesehen. der dazu eingerichtet ist, die Kopie zu erstellen.

[0030] Weiters ist der LI-Server dazu eingerichtet, anhand der Identifikationskennzeichnung festzustellen, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll(en).

[0031] Günstiger Weise ist der LI-Server dazu eingerichtet, die zumindest eine Sekundärkopie zu erstellen.

[0032] Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit durchzuführen.

[0033] Der Authentifizierungsserver kann dazu eingerichtet sein, anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwachungskennzeichnung festzustellen, ob ein Überwachungsfall vorliegt.

[0034] Die verborgene Datenbank und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten sind dazu eingerichtet, Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet ist.

[0035] Das Telekommunikationssystem kann dazu eingerichtet sein, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank zugeordnete Überwachungskennzeichnungen in der verborgenen Datenbank zu löschen.

[0036] In einer vorteilhaften Variante der Erfindung, ist der Datenstrom ein Voice over IP-Datenstrom, wobei ein Call-Controller vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

[0037] Eine andere günstige Variante sieht vor, dass der Authentifizierungsserver dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

[0038] Weitere Vorteile lassen sich dadurch schaffen, dass das Telekommunikationssystem dazu eingerichtet ist, den Datenzugang von dem Gateway zu dem Überwachungsserver durchzutunneln.

[0039] Um einem Datenverlust vorzubeugen können der Überwachungsserver und/oder der LI-Server dazu eingerichtet sein, die Kopie des Datenstroms zwischenzuspeichern.

[0040] Weiters kann der Call-Controller dazu eingerichtet sein, sowohl das Gateway als auch den Überwachungsserver zu steuern.

[0041] In einer anderen Variante ist der Authentifizierungsserver dazu eingerichtet, den Überwachungsserver zu steuern. Günstigerweise weist der Überwachungsserver die Funktionalität eines Proxy-Servers auf.

[0042] Die Erfindung samt weiterer Vorteile ist im folgenden anhand einiger nicht einschränkender Ausführungsbeispiele, die in der Zeichnung veranschaulicht sind dargestellt, in dieser zeigen schematisch:

Fig. 1 ein erfindungsgemäßes Telekommunikationssystem,

Fig. 2a eine Kopie eines Datenstroms mit einer Identifikationskennzeichnung,

Fig. 2b die Identifikationskennzeichnung aus Fig. 2a im näheren Detail und

Fig. 3 einen beispielsweisen Ablauf des erfindungsgemäßen Verfahrens.

[0043] Gemäß Fig. 1 muss sich jeder Benutzer BEA, BEB, eines erfindungsgemäßen Telekommunikationssystems SYS der über sein Telekommunikationsendgerät TEA bzw. Telekommunikationseinrichtung TEB Zugang zu einem Datennetz WWW, beispielsweise dem Internet, haben will, über ein Gateway GWA, GWB einwählen bzw. sich bei einem Zugangsserver AAA anmelden. Unter einer Telekommunikationsvorrichtung wird in diesem Dokument jede Art von Telekommunikationsendgerät, wie beispielsweise ein mit dem Datennetz verbundener PC, bzw. auch Server, die in dem Datennetz WWW stehen können, verstanden.

[0044] Der Zugangsserver AAA, AAB kann als AAA-Server oder als Remote Authentication Dial-In User Service Server kurz RADIUS-Server ausgebildet sein. Um einen Datenzugang ZUG dem Datennetz WWW zu erlangen, ist es für einen Benutzer erforderlich sich zu authentifizieren.

[0045] Die Authentifikation eines Benutzers BEA, BEB kann dabei über Eingabe eines Passwortes PAS bzw. einer Benutzeridentifikation, beispielsweise des Namens des Benutzers, erfolgen.

[0046] Anhand des Identifikationsergebnisses entscheidet der Zugangsserver AAA, AAB, ob einen Datenzugang ZUG zu dem Datennetz WWW gewährt oder verweigert wird.

[0047] Die Authentifikation des Benutzers BEA, BEB kann von seiten des Zugangsservers AAA mittels Abfrage einer Verwaltungsdatenbank VDA, in der die Benutzerdaten verwaltet werden erfolgen.

[0048] Liegt ein positives Authentifizierungsergebnis vor, so wird eine verborgene Datenbank abgefragt, in der jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung UWD zugeordnet ist. Besagt die Überwachungskennzeichnung UWD, dass ein Datenstroms DAT zwischen dem Telekommunikationsendgerät TEA des Benutzer BEA und einem weiteren Telekommunikationsendgerät durchgeführt werden soll, so wird eine Kopie KOP des Datenstromes DAT angefertigt.

[0049] Die Kopie KOP des originalen Datenstromes DAT kann beispielsweise von dem Gateway GWA, welches dem Telekommunikationsendgerät TEA zugeordnet ist, oder von einem eigens hierfür vorgesehenen Überwachungsserver PRO erstellt werden. Für den Fall, dass der Überwachungsserver PRO die Kopie des originalen Datenstromes DAT erstellt, wird der Datenstrom DAT zwischen über den Überwachungsserver PRO umgeleitet. Bevorzugter Weise weist dieser Server Proxyfunktionalität auf. Der Überwachungsserver PRO unterscheidet sich von einem Proxy-Server lediglich dadurch, dass der Überwachungsserver PRO dazu eingerichtet ist, die Kopie KOP eines über ihn laufenden (umgeleiteten) Datenstroms DAT zu erstellen und diese Kopie mit einer mitgelieferten Identifikationskennzeichnung IDK (Fig. 2), beispielsweise der IP-Adresse oder einer verschlüsselten Kennzeichnung des abzuhörenden Benutzers, zu versehen und an einen "Lawful Interception"-Server oder kurz LI-Server LIS zu übermitteln, wobei der originale Datenstrom an die durch den Benutzer bestimmte Zieladresse weitergeroutet wird.

[0050] Erstellt das Gateway GWA die Kopie KOP, so ist die soeben beschriebene Funktionalität des Kopierens und Weiterleitens der Kopie KOP an den LI-Server bzw. des Routens des originalen Datenstromes DAT gemäß der benutzerbestimmten Zieladresse in dem Gateway GWA realisiert.

[0051] Ein Datenzugang ZUG zu dem Datennetz WWW kann im Überwachungsfall für den zu überwachenden Benutzer BEA direkt über das Gateway und den Überwachungsserver PRO erfolgen.

[0052] Die Umleitung des Datenstromes DAT an den Überwachungsserver PRO kann mittels Tunneling, beispielsweise gemäß dem in der RFC 2661 spezifizierten L2T-Protokolls erfolgen.

[0053] Eine andere Möglichkeit den Datenstrom DAT über den Überwachungsserver PRO umzuleiten besteht darin, dass dem Überwachungsserver PRO eine Adresse in dem Datennetz zugeordnet wird, im Fall des Internet eine IP-Adresse. Diese Adresse kann in einer Speichereinheit des Zugangsservers AAA, AAB abgelegt sein, wobei im Überwachungsfall der Datenstrom DAT, beispielsweise gemäß dem TCP/IP-Protokolls, an die Adresse des Überwachungsservers PRO weitergeleitet wird. Der Überwachungsserver PRO erstellt sodann, wie bereits oben erwähnt, eine Kopie KOP des über ihn umgeleiteten Datenstroms DAT und übermittelt diese Kopie KOP an einen LI-Server, der anhand der Identifikationskennzeichnung IDK, welche der Kopie beigefügt ist, entscheidet was mit der Kopie KOP zu geschehen hat, beispielsweise ob weitere Kopien d.h. Sekundärkopien WKO der Kopie erstellt werden sollen bzw. an welche Auswerteeinheit(en) die Kopie(n) zu übermitteln ist (sind).

[0054] Die weitere Verarbeitung und Auswertung der Kopie KOP erfolgt dann in der Auswerteeinheit ASW, beispielsweise einem dazu eingerichteten PC einer Behörde.

[0055] Der LI-Server LIS ist üblicherweise eine Anordnung mehrerer Workstations. Seine Aufgabe ist es, wie bereits oben erwähnt, die Kopie KOP des Datenstromes DAT zu empfangen, die der Kopie KOP von dem Überwachungsserver beigefügte Identifikationskennzeichnung IDK auszuwerten, gegebenenfalls wei-

tere Kopien WKO der Kopie KOP herzustellen und an die Bedarfsträger zuzustellen.

[0056] Auch ist der LI-Server dazu eingerichtet, eine Schnittstellenanpassung zu unterschiedlichen Auswerteeinheiten ASW der Bedarfsträger durchzuführen. So kann es beispielsweise notwendig sein für eine Überwachung zwei H.323 Verbindungen zu einem bekannten Time Division Multiplex oder kurz TDM-Übergabe-Interface der überwachenden Behörde herzustellen. Eine andere Möglichkeit besteht darin, die Kopie über ein IP-Übergabe Interface an die überwachende Behörde zuzustellen.

[0057] Die Informationen, die der LI-Server LIS benötigt, um die Kopie an den Bedarfsträger bzw. die Auswerteeinheit ASW weiterzuleiten, können von Seiten der Bedarfsträger in einer Datenbank LID abgelegt werden.

[0058] Eine weitere Möglichkeit besteht darin, dass die Kopie KOP samt der Identifikationskennzeichnung IDK von dem Überwachungsserver PRO bzw. Gateway GWA direkt an die Auswerteeinheit ASW zugestellt wird.

[0059] Nach dem Erstellen der Kopie KOP des Datenstroms DAT, wird der originale Datenstrom DAT von dem Überwachungsserver PRO auf die herkömmliche Weise, beispielsweise gemäß dem TCP/IP-Protokoll, an den zweiten Benutzer BEB bzw. die Telekommunikationseinrichtung TEB, SER weitergeroutet.

[0060] Nach Fig. 2a wird der Kopie KOP des Datenstromes DAT eine Identifikationskennzeichnung IDK als Header vorangestellt. Die Identifikationskennzeichnung kann zumindest einen IP-Header IPH aufweisen, beispielsweise die IP-Adresse des überwachten Benutzers BEA. Weiters kann ein spezieller LI-Header LIH vorgesehen sein (Fig. 2b), der Informationen betreffend die weitere Datenübermittlung für den LI-Server enthält. So kann beispielsweise die erste Zeile die Art TYP der Nachricht enthalten, ob es zum Beispiel um eine Sprachnachricht oder eine "abgehörte" e-Mail handelt. Eine nächste Zeile kann die Länge LEN des Headers enthalten, während in einer dritten Zeile eine Operator-ID OID gemäß dem Standard ETSI ES 201671 enthalten kann. Eine Rufidentifizierungsnummer CIN kann zur Identifizierung eines "abgehörten" Benutzers BEA dienen, während eine Behördenidentifizierung LID dazu dient den Bedarfsträger, an den die Kopie KOP zugestellt werden soll, zu identifizieren. Weitere Informationen SUP können an die soeben genannten im Bedarfsfall angehängt werden.

[0061] Gemäß Fig. 3 wird im Fall einer Sprachübertragung gemäß dem Voice over IP-Protokoll eine entsprechende Applikation APP auf dem Telekommunikationsendgerät TEA des Anrufers BEA gestartet, welches daraufhin eine Verbindung über ein erstes Gateway GWA zu einem ersten Zugangsserver AAA aufbaut. Dieser Zugangsserver AAA überprüft, welcher Teilnehmer den Dienst zur Sprachübertragung in Anspruch nehmen will, und ob dieser zur Inanspruchnahme dieses Dienstes berechtigt ist. Zu diesem Zweck findet eine H.323 oder RADIUS-Kommunikation zwischen dem Gateway GWA und dem Zugangsserver AAA statt.

[0062] Ist der anrufende Benutzer BEA zur Benutzung des Sprachdienstes berechtigt, so überprüft der Zugangsserver AAA anhand der Authentifizierung dieses Benutzers BEA, ob der Datenaustausch zwischen dem Anrufer und einem Angerufenen überprüft werden soll.

[0063] Nach erfolgreicher Zugangsprüfung ermittelt der Call-Controller CON durch Kommunikation mit einem zweiten Zugangsserver AAB die IP-Adresse des angerufenen Telekommunikationsendgerätes TEB und veranlasst den Signalisierungsverkehr über ein weiteres Gateway GWB zu diesem Telekommunikationsendgerät TEB.

[0064] Ist nun der Anrufer zu überwachen, dann baut der Controller CON die Verbindung vom Gateway GWA nicht direkt zu dem angerufenen Telekommunikationsendgerät TEB auf, wie es üblicherweise der Fall ist, sondern schleift den Überwachungsserver PRO ein. D. h. die Verbindung von dem ersten Telekommunikationsendgerät TEA zu dem zweiten Telekommunikationsendgerät TEB wird in zwei Strecken zerlegt, nämlich in die Strecke von dem ersten Telekommunikationsendgerät TEA zum Überwachungsserver PRO und in die Strecke von dem Überwachungsserver PRO zu dem zweiten Telekommunikationsendgerät TEB.

[0065] Der Controller CON steuert im Normalfall das erste Gateway GWA. Da aber nun wegen der Überwachung der Zugang zum Datennetz WWW bis zu dem Überwachungsserver PRO verlängert wird und dort eigentlich erst das normale Routing für den Datenstrom DAT des Benutzers BEA anfängt, ist der Controller CON dazu eingerichtet, einen "Handover" vom Gateway zu dem Überwachungsserver durchführen. D. h. der Controller CON wird durch den ersten Zugangsserver AAA informiert, dass ein Überwachungsfall vorliegt und der Datenzugang ZUG des zu überwachenden Telekommunikationsendgerätes TEA zu einem Überwachungsserver PRO durchzutunneln ist. Der Controller betrachtet den Überwachungsserver PRO von nun an als "neues" erstes Gateway GWA und steuert diesen Server als ob es das Gateway GWA wäre. Im Überwachungsfall verhält sich der Call-Controller CON also so, als ob der Überwachungsserver PRO das Gateway GWA wäre, dies gilt sowohl für die rufende als auch die gerufene Seite.

[0066] Der Überwachungsserver PRO erstellt dann, wie bereits oben erwähnt, eine Kopie KOP des Datenstromes DAT zwischen den beiden Telekommunikationsendgeräten TEA, TEB. Zur Erstellung der Kopie KOP wird der ursprüngliche Datenstrom DAT in dem Überwachungsserver PRO verdoppelt. Der ursprüngliche Datenstrom DAT wird nach der Verdoppelung von dem Überwachungsserver PRO an das zweite Telekommunikationsendgerät TEB weitergeroutet, während die Kopie KOP des Datenstromes DAT, wie bereits oben erwähnt, an einen LI-Server oder eine Auswerteeinheit

ASW übermittelt wird.

[0067] Der Überwachungsserver PRO als auch der LI-Server LIS können dazu eingerichtet sein, die Kopie KOP zwischenzuspeichern, um für den Fall, dass eine unmittelbare Zustellung an die Auswerteeinheit ASW nicht möglich ist, einen Datenverlust zu vermeiden.

[0068] Um ein Abhören ohne merkliche Beeinträchtigung der Qualität und der Geschwindigkeit des ursprünglichen Datenstroms DAT zu verwirklichen, sollte die Strecke zwischen dem Überwachungsserver PRO und dem Gateway GWA gering sein, weshalb es vorteilhaft ist, wenn eine große Anzahl von Überwachungsservern PRO in dem Datennetz WWW angeordnet sind.

[0069] Soll der angerufene Benutzer BEB überwacht werden erfolgt das Verfahren im wesentlichen so wie oben beschrieben, wobei der zweite Zugangsserver AAB anhand der IP-Adresse des gerufenen Teilnehmers BEB die Authentifizierung durchführen kann und den Datenstrom DAT über den Überwachungsserver PRO umleitet.

[0070] Zu Zweck der Authentifizierung des gerufenen Teilnehmers BEB anhand seiner IP-Adresse kann der zweite Zugangsserver AAB eine Datenbank DAB aufweisen, welche die IP-Adresse des gerufenen Teilnehmers und einen Eintrag ob dieser abgehört werden soll enthält.

[0071] Der Befehl zur Überwachung des Benutzers BEA von einer zur Überwachung berechtigten Behörde gegeben und in der versteckten Datenbank DBA eingetragen.

[0072] Wenn der überwachte Benutzer BEA eine Applikation zur Datenübertragung in dem Datennetz WWW auf seinem Telekommunikationsendgerät startet, erfolgt die Authentifizierung des Benutzers und die Feststellung ob ein Überwachungsfall vorliegt, wie bereits oben erwähnt.

[0073] Der A-Seite wird in einem Überwachungsfall anstelle der Adresse des gerufenen Benutzers BEB bzw. einer Telekommunikationseinrichtung TEB SER, wie beispielsweise einem Server, auf dem eine Homepage oder andere Daten abgelegt sind, die Adresse des Überwachungsservers PRO übermittelt. Das B-seitige Gateway GWB erhält von dem Authentifizierungsserver AAA oder Call-Controller CON anstelle der Netzwerkadresse des rufenden Benutzers BEA die Netzwerkadresse des Überwachungsservers PRO.

[0074] Der Überwachungsserver PRO wird von dem Authentifizierungsserver AAA oder Call Controler CON informiert, dass eine Überwachung stattfinden soll. Alle zur Überwachung und Verbindung notwendigen Informationen, z. B. "Verbinde die A-Seite mit der B-Seite" und ähnliche Informationen, können mittels H.248 Übertragung von dem Authentifizierungsserver AAA bzw. Call-Controler CON an den Überwachungsserver PRO übertragen werden.

[0075] In dem Überwachungsserver wird, wie bereits oben erwähnt,der Datenstrom DAT zwischen dem A-seitigen und B-seitigen Benutzer bzw. Server verdoppelt, wobei die verdoppelten Daten mit einer Identifikationskennzeichnung IDK versehen werden. Die so erstellte Kopie KOP wird in weiterer Folge an den LI-Server übermittelt.

[0076] Für den originalen Datenstrom funktioniert der Überwachungsserver wie ein Proxyserver und verbindet lediglich die A-Seite mit der B-Seite.

[0077] Eine andere Variante der Erfindung sieht vor, dass die A-Seite von dem Authentifizierungsserver AAA oder Call-Controler CON die Netzwerkadresse der B-Seite erhält, wobei das A-seitige Gateway mittels H. 248-Übertragung dazu aufgefordert wird, den gesamten Datenverkehr, der von dem Benutzer BEA stammt, zu dem Überwachungsserver zu tunneln. Hierbei wird der B-Seite, deren Netzwerkadresse bekannt ist anstelle der Netzwerkadresse der A-Seite von dem Call-Controler die Adresse des Überwachungsservers PRO übermittelt.

[0078] Der Überwachungsserver PRO erhält von dem Call-Controler die entsprechenden Informationen für das Tunnneln und verbindet die A-Seite mit der B-Seite.

[0079] Die Vorteile des Tunnelns bestehen darin, dass für den überwachten Benutzer BEA die für das Umleiten des Datenstroms über den Überwachungsserver PRO notwendigen Adressänderungen nicht sichtbar sind.

[0080] Wenn der Überwachungsserver PRO von dem Authentifizierungsserver AAA, AAB oder dem Call-Controler über eine H.248 Kommunikation informiert wird, dass ein Datenstrom DAT umgeleitet wird, so kann er eine Startnachricht an den LI-Server übermitteln, sodass dieser die notwendigen Daten aus der LI-Datenbank LID abfragt und diese bei eintreffen der Kopie KOP schon zur Verfügung stehen.

[0081] Wenn der zu überwachende Datenaustausch beendet wird, dann informiert der Call-Controler CON den Überwachungsserver PRO, dass er die Kommunikation bezüglich der konkreten Überwachung mit dem LI-Server abbrechen soll. Nach Erhalt einer von dem Überwachungsserver PRO stammenden Beendigungsnachricht kann der LI-Server die aus LI-Datenbank stammenden Daten wieder löschen und die Kommunikation mit den Bedarfsträgern einstellen.

Patentansprüche

1. Verfahren zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB), wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
dadurch gekennzeichnet, dass von dem zumin-

dest einem Authentifikationsserver (AAA, AAB) überprüft wird, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) erstellt wird, welcher eine Identifikationskennzeichnung (IDK) beigefügt wird, und die Kopie samt Identifikationskennzeichnung (IDK) hierauf an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) übermittelt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kopie (KOP) von dem Gateway (GWA, GWB) erstellt wird.

3. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver (PRO) erstellt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** der LI-Server anhand der Identifikationskennzeichnung (IDK) feststellt, ob zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll(en).

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet, dass** der LI-Server (LIS) die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt.

6. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** der LI-Server (LIS) eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchführt.

7. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** der Authentifizierungsserver (AAA, AAB) anhand einer dem zumindest einem Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB)zugeordneten Überwachungskennzeichnung (UWD) feststellt, ob ein Überwachungsfall vorliegt.

8. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die verborgene Datenbank (DBA, DBB) mit einer Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung steht und jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenem Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet wird.

9. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwachungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) gelöscht werden.

10. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** der Datenstrom (DAT) als Voice over IP-Datenstrom übertragen wird.

11. Verfahren nach Anspruch 9, **dadurch gekennzeichnet, dass** ein Call-Controller (CON) den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet, der die Kopie (KOP) erstellt.

12. Verfahren nach Anspruch 3 bis 10, **dadurch gekennzeichnet, dass** der Authentifizierunsserver (AAA, AAB) in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet.

13. Verfahren nach einem der Ansprüche 3 bis 11, **dadurch gekennzeichnet, dass** der Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchgetunnelt wird.

14. Verfahren nach einem der Ansprüche 3 bis 12, **dadurch gekennzeichnet, dass** die Kopie (KOP) des Datenstroms (DAT) auf dem Überwachungsserver (PRO) zwischengespeichert werden.

15. Verfahren nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** die Kopie des Datenstroms (DAT) auf dem LI-Server zwischengespeichert wird.

16. Verfahren nach einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet, dass** der Controller (CON) sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) steuert.

17. Verfahren nach einem der Ansprüche 11 bis 14, **dadurch gekennzeichnet, dass** der zumindest eine Authentifizierungsserver (AAA, AAB) den Überwachungsserver steuert.

18. Telekommunikationssystem, welches zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB) eingerichtet ist, wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu

eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
dadurch gekennzeichnet, dass der Authentifikationsserver (AAA, AAB) dazu eingerichtet ist, zu überprüfen, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei das Telekommunikationssystem (SYS) dazu eingerichtet ist, in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) zu erstellen und der Kopie (KOP) eine Identifikationskennzeichnung (IDK) hinzuzufügen und die Kopie (KOP) samt Identifikationskennzeichnung (IDK) an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) zu übermitteln.

19. Telekommunikationssystem nach Anspruch 17,
dadurch gekennzeichnet, dass das Gateway (GWA, GWB) dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zu erstellen.

20. Telekommunikationssystem nach Anspruch 17,
dadurch gekennzeichnet, dass ein Überwachungsserver (PRO) vorgesehen ist, der dazu eingerichtet ist die Kopie (KOP) zu erstellen.

21. Telekommunikationssystem nach einem der Ansprüche 17 bis 19,
dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, anhand der Identifikationskennzeichnung (IDK) festzustellen, ob zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll(en).

22. Telekommunikationssystem nach Anspruch 21,
dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) zu erstellen.

23. Telekommunikationssystem nach einem der Ansprüche 17 bis 22,
dadurch gekennzeichnet, dass der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchzuführen.

24. Telekommunikationssystem nach einem der Ansprüche 17 bis 23,
dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, anhand einer dem zumindest einen Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB)zugeordneten Überwachungskennzeichnung (UWD) festzustellen, ob ein Überwachungsfall vorliegt.

25. Telekommunikationssystem nach Anspruch 24,
dadurch gekennzeichnet, dass die verborgene Datenbank (DBA, DBB) und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten dazu eingerichtet sind Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenen Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet ist.

26. Telekommunikationssystem nach Anspruch 25,
dadurch gekennzeichnet, dass es dazu eingerichtet ist, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwachungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) zu löschen.

27. Telekommunikationssystem nach einem der Ansprüche 17 bis 26,
dadurch gekennzeichnet, dass der Datenstrom (DAT) ein Voice over IP-Datenstrom ist.

28. Telekommunikationssystem nach Anspruch 27,
dadurch gekennzeichnet, dass ein Call-Controller (CON) vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

29. Telekommunikationssystem nach einem der Ansprüche 20 bis 28,
dadurch gekennzeichnet, dass der Authentifizierunsserver (AAA, AAB) dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

30. Telekommunikationssystem nach einem der Ansprüche 20 bis 29,
dadurch gekennzeichnet, dass es dazu eingerichtet ist, den Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchzutunneln.

31. Telekommunikationssystem nach einem der Ansprüche 20 bis 30,
dadurch gekennzeichnet, dass der Überwachungsserver dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

32. Telekommunikationssystem nach einem der Ansprüche 17 bis 31,
dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

33. Telekommunikationssystem nach einem der Ansprüche 28 bis 32,
dadurch gekennzeichnet, dass der Call-Controller (CON) dazu eingerichtet ist, sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) zu steuern.

34. Telekommunikationssystem nach einem der Ansprüche 29 bis 32,
dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, den Überwachungsserver zu steuern.

35. Telekommunikationssystem nach einem der Ansprüche 20 bis 34,
dadurch gekennzeichnet, dass der Überwachungsserver (PRO) die Funktionalität eines Proxy-Servers aufweist.

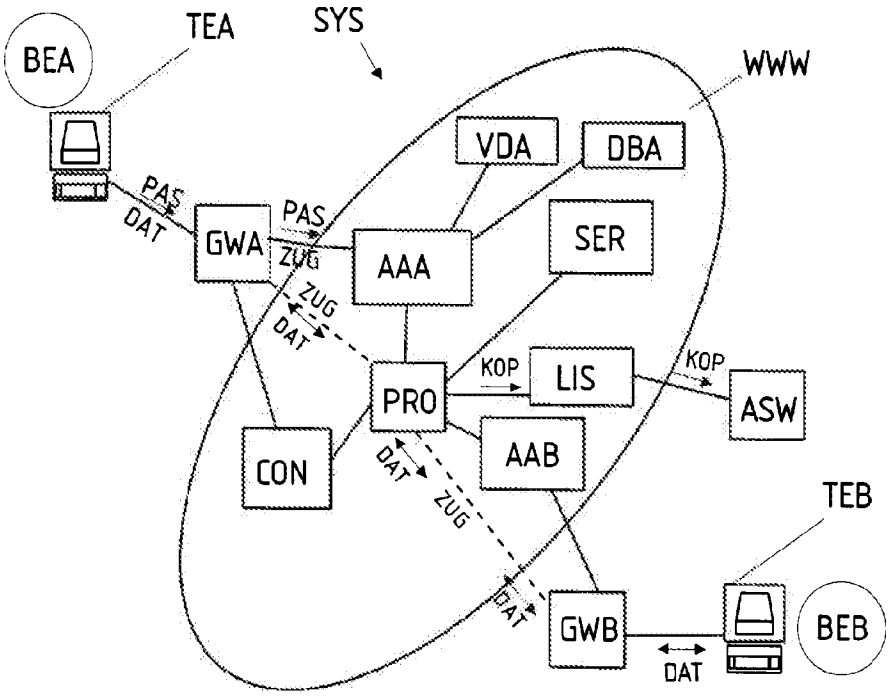


Fig. 1

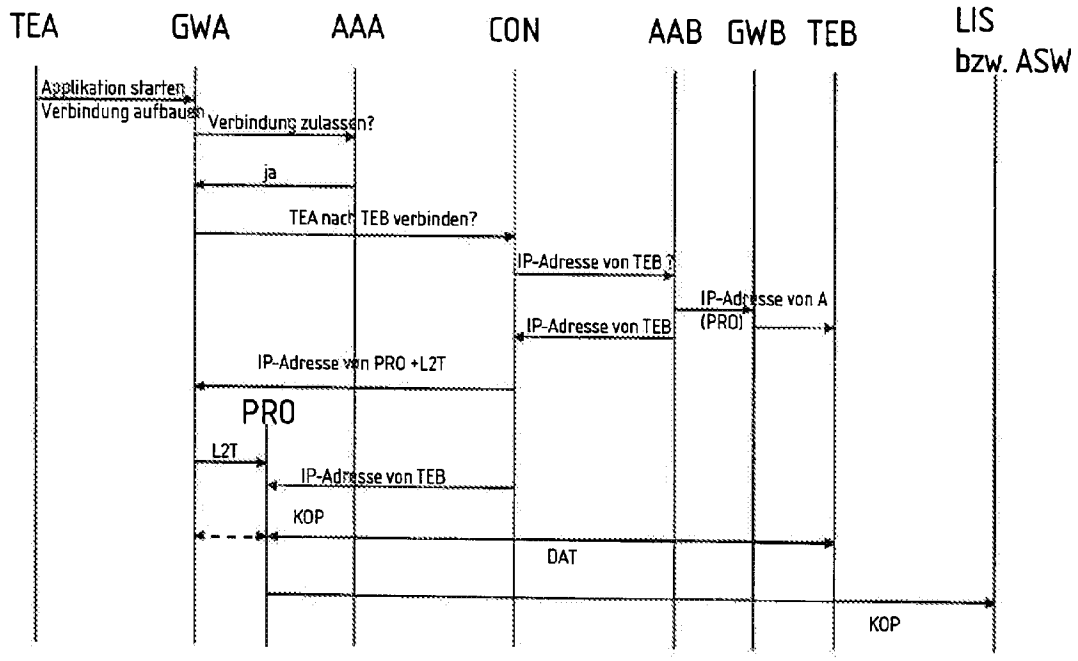


Fig. 3

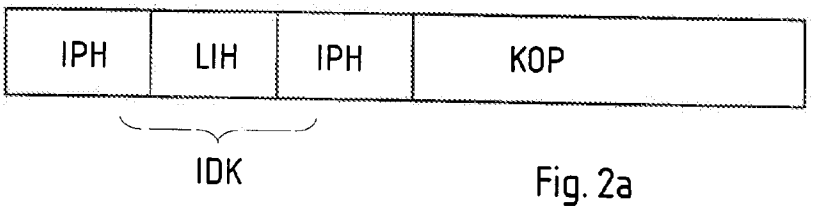


Fig. 2a

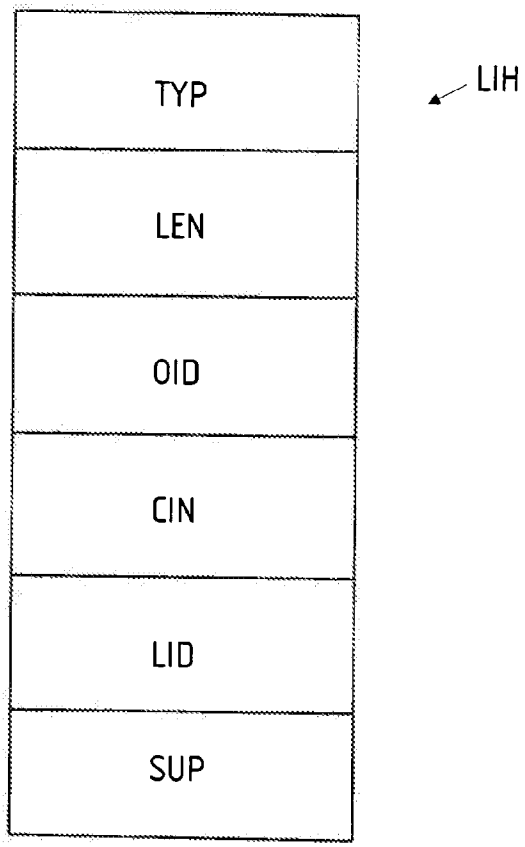


Fig. 2b

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 01 10 7063

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
A	WO 00 56019 A (NOKIA NETWORKS OY ;ELORANTA JAANA (FI)) 21. September 2000 (2000-09-21) * Seite 1, Zeile 5 - Seite 1, Zeile 19 * * Seite 7, Zeile 27 - Seite 10, Zeile 16 * * Abbildungen 1,2,4 *	1-3,7-9, 11-16, 18-20, 24-26, 28,30-33	H04L12/26 H04L29/06
A	WO 00 42742 A (NOKIA NETWORKS OY ;HIPPELAEINEN LASSI (FI)) 20. Juli 2000 (2000-07-20) * Seite 2, Zeile 18 - Seite 3, Zeile 6 * * Seite 4, Zeile 7 - Seite 4, Zeile 32 * * Seite 6, Zeile 4 - Seite 8, Zeile 21 * * Seite 10, Zeile 28 - Seite 11, Zeile 14 * * Abbildungen 1-4 *	1-3,6-9, 11-16, 18-20, 23-26, 28,30-33	
A	WO 99 55062 A (GTE GOVERNMENT SYST) 28. Oktober 1999 (1999-10-28) * Seite 3, Zeile 3 - Seite 3, Zeile 6 *	10,27	RECHERCHIERTE SACHGEBIETE (Int.Cl.7) H04L
A	METZ CHRISTOPHER: "AAA Protocols: Authentication, Authorization, and Accounting for the Internet" IEEE INTERNET COMPUTING, 1999, Seiten 75-79, XP002176948 * das ganze Dokument *	1,7,8, 12,17, 18,24, 25,29,34	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
MÜNCHEN	7. September 2001	Körbler, G

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P01C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.

EP 01 10 7063

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

07-09-2001

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0056019 A	21-09-2000	AU 3035399 A	04-10-2000
WO 0042742 A	20-07-2000	AU 2617399 A	01-08-2000
WO 9955062 A	28-10-1999	AU 3865599 A	08-11-1999

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

Espacenet

Bibliographic data: EP1266516 (A2) — 2002-12-18

Establishing real-time interactive audio calls by a computer on behalf of a packet -switched data network telephone

Inventor(s): SOLLEE PATRICK N [US]; CREECH DAVID R [US]; OSTERHOUT GREGORY T [US]; JESSEN CHRISTOPHER L [US] + (SOLLEE, PATRICK, N, ; CREECH, DAVID, R, ; OSTERHOUT, GREGORY, T, ; JESSEN, CHRISTOPHER, L)

Applicant(s): NORTEL NETWORKS LTD [CA] + (NORTEL NETWORKS LIMITED, ; GENBAND US LLC)

Classification: **- international:*H04M1/253;*** *H04M7/00;* (IPC1-7): H04M1/253; H04M3/42; H04M7/00
- cooperative: H04M1/2535; H04M7/0006

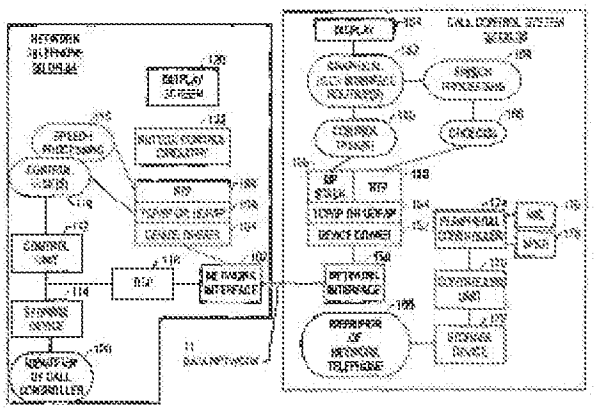
Application number: EP20010918523 20010312

Priority number(s): WO2001US07686 20010312 ; US20000524342 20000313

Also published as: EP1266516 (B1) WO0169899 (A2) WO0169899 (A3) US6934279 (B1) US2006007940 (A1) US7995589 (B2) AU4559001 (A) less

Abstract not available for EP1266516 (A2)
Abstract of corresponding document: WO0169899 (A2)

A method and apparatus of communicating over a data network (11) includes providing a user interface (200) in a control system (32, 36) for call control and to display information relating to a call session. The control system (32, 36) communicates one or more control messages (e.g., Session Initiation Protocol or SIP messages) over the data network (11) to establish a call session with a remote device in response to receipt of a request through the user interface. One or more commands are transmitted to a voice device (30, 34) associated with the control system (32, 36) to establish the



call session between the voice device (30, 34) and the remote device over the data network (11). A Real-Time Protocol (RTP) link may be established between the voice device (30, 34) and the remote device.;Recently, network telephones have been developed that are capable of being connected directly to a data network, such as an IP network. These network telephones are capable of placing telephony calls over a data network. The voice quality offered by such telephones are typically superior to those that can be offered by computer systems, since such network telephones typically include dedicated digital signal processors (DSPs) that perform the data intensive calculations involved in speech processing. However, the existing network telephones do not provide desired multimedia presentation capabilities such as those offered by displays of computer systems. Thus, while networks telephones offer superior speech capabilities, it does have the desired multimedia capabilities.; On the other hand, computer systems have superior multimedia capabilities, but they suffer from relatively poor speech processing performance. A need thus exists for an improved method and apparatus for controlling voice communications over data networks. A method and apparatus of communicating over a data network (11) includes providing a user interface (200) in a control system (32, 36) for call control and to display information relating to a call session. The control system (32, 36) communicates one or more control messages (e.g., Session Initiation Protocol or SIP messages) over the data network (11) to establish a call session with a remote device in response to receipt of a request through the user interface.; One or more commands are transmitted to a voice device (30, 34) associated with the control system (32, 36) to establish the call session between the voice device (30, 34) and the remote device over the data network (11). A Real-Time Protocol (RTP) link may be established between the voice device (30, 34) and the remote device.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 266 516 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 01/069899 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 01/069899 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 01/069899 (art. 158 de la CBE).

Espacenet

Bibliographic data: EP1362456 (A2) — 2003-11-19

SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS

Inventor(s): PYKE CRAIK R [CA]; HERN WILLIAM [GB]; THOMPSON ROGER L [US]; CARON SERGE S [CA]; MOUNJI HALIMA H [CA]; EWOTI CHARLES B [DE]; GOERENS MICHAEL [DE]; STRENG PETE J [CA]; GOERTZEN CHRISTOPHER J [CA]; KITTLITZ CHRISTIAN [CA]; TAYLOR RICHARD C [CA]; WELHAM MICHAEL [DE] + (PYKE, CRAIK, R, ; HERN, WILLIAM, ; THOMPSON, ROGER, L, ; CARON, SERGE, S, ; MOUNJI, HALIMA, H, ; EWOTI, CHARLES, B, ; GOERENS, MICHAEL, ; STRENG, PETE, J, ; GOERTZEN, CHRISTOPHER, J, ; KITTLITZ, CHRISTIAN, ; TAYLOR, RICHARD, C, ; WELHAM, MICHAEL)

Applicant(s): NORTEL NETWORKS LTD [CA] + (NORTEL NETWORKS LIMITED)

Classification: **- international:** ***H04L12/26; H04L29/06; H04M3/22; H04M7/00;*** (IPC1-7): H04L12/56

- cooperative: **H04L29/06**; **H04L63/30**; **H04L69/22**; **H04M3/2281**; **H04M7/006**; H04Q2213/13034; H04Q2213/13196; H04Q2213/13372; H04Q2213/13389

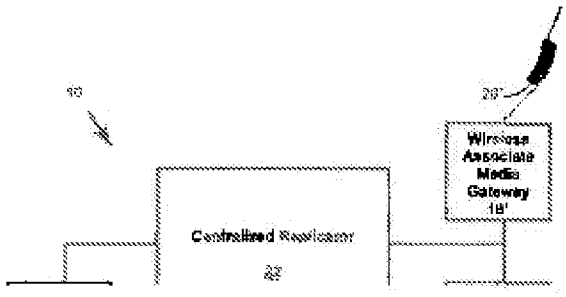
Application number: EP20010273516 20011009

Priority number(s): WO2001US31548 20011009 ; US20000239048P 20001010

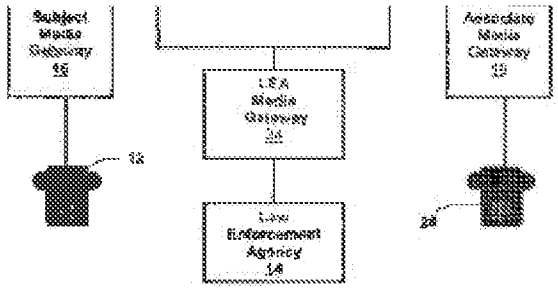
Also published as: EP1362456 (A4) EP1362456 (B1) WO02082782 (A2) WO02082782 (A3) US2003179747 (A1) DE60133316 (T2) CA2437275 (A1) AU2001297701 (A1) less

Abstract not available for EP1362456 (A2)
Abstract of corresponding document: WO02082782 (A2)

A system and method for intercepting a telecommunication signal are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload and



PETITIONER APPLE INC. EX. 1004-661



adding a second header to replicated payload and directing the replicated payload to the address associated with the second.;A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 362 456 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 02/082782 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 02/082782 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 02/082782 (art. 158 de la CBE).

Espacenet

Bibliographic data: EP1371173 (A1) — 2003-12-17

METHOD AND TELECOMMUNICATIONS SYSTEM FOR MONITORING A DATA FLOW IN A DATA NETWORK

Inventor(s): STIFTER HELMUT [DE]; PFAEHLER WOLFGANG [DE]; KREUSCH NORBERT [DE] ± (STIFTER, HELMUT, ; PFAEHLER, WOLFGANG, ; KREUSCH, NORBERT)

Applicant(s): SIEMENS AG [DE] ± (SIEMENS AKTIENGESELLSCHAFT)

Classification: **- international:** ***H04L12/26; H04L29/06; H04L29/08; H04M3/22;*** (IPC1-7): H04L12/26; H04L29/06
- cooperative: **H04L12/2602; H04L29/06; H04L43/00; H04L63/00; H04L63/30; H04L65/103; H04L65/1046; H04L65/80; H04L67/2814; H04L67/306; H04M3/2281;** H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

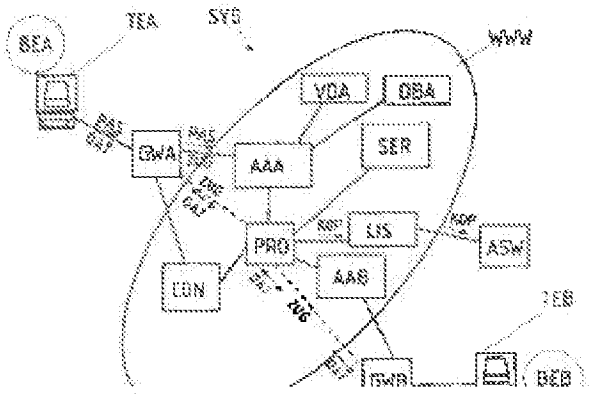
Application number: EP20020759770 20020307

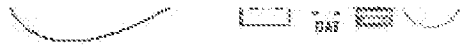
Priority number(s): EP20020759770 20020307 ; WO2002EP02524 20020307 ; EP20010107063 20010321

Also published as: EP1371173 (B1) EP1244250 (A1) US2004181599 (A1) US7979529 (B2) RU2003130974 (A) RU2280331 (C2) WO02082728 (A1) CN1498482 (A) CN1274114 (C) BR0208272 (A) less

Abstract not available for EP1371173 (A1)
Abstract of corresponding document: EP1244250 (A1)

A data stream (DAT) is monitored in a data network (WWW) between two telecommunications terminals (TEA,TEB) connected to the data network via access servers (AAA,AAB), which operate during a monitoring situation to divert the data stream between the telecommunications terminals through a monitoring server (PRO) that produces a copy (KOP) of the data stream and transmits it to an





analyzing unit (ASW). An independent claim is also included for a telecommunication system for monitoring a data stream in a data network between a telecommunications terminal linked to a data network via a gateway and to a further telecommunications device.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 371 173 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 02/082728 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 02/082728 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 02/082728 (art. 158 de la CBE).

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 411 743 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.04.2004 Bulletin 2004/17

(51) Int Cl.[7]: **H04Q 7/38**, H04M 11/04

(21) Application number: **03256372.8**

(22) Date of filing: **09.10.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **16.10.2002 US 270629**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

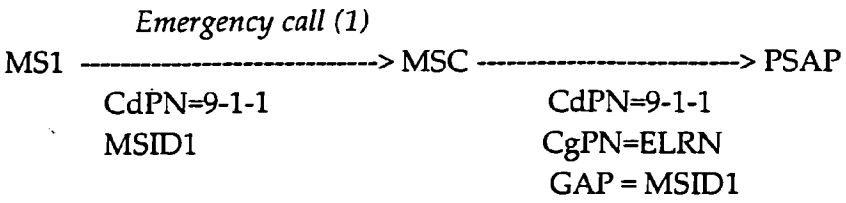
(72) Inventors:
- **Chin, Mary**
  Westmont, Illinois 60559 (US)
- **Rollender, Douglas**
  Bridgewater, New Jersey 08807 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies NS UK Limited,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) An emergency call back method

(57) An emergency routing number is assigned to each switch in a wireless network. When a switch of the wireless network routes an emergency call to a Public Service Answering Point (PSAP), the switch sends the emergency routing number as the calling party number and provides the PSAP with the identifier of the mobile station. If the emergency call drops, the PSAP performs a call back using the emergency routing number as the called party number. The switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. When a switch receives its emergency routing number as the called party number, the switch recognizes an emergency call back situation and pages the mobile station identified by the mobile station identifier received in association with the emergency routing number. The mobile station is then reconnected with the PSAP.

Fig. 1



EP 1 411 743 A1

Description

BACKGROUND OF THE INVENTION

[0001] Emergency service calls in North America are originated by dialing "9-1-1." Other parts of the world may use some other abbreviated string of dialable digits such as "6-1-1" in Mexico; all share the intent to provide the caller with an easy way to call for help with an easy to remember number. These calls are routed to a local Public Service Answering Point (PSAP) where an emergency response may be initiated (police, fire department, road repair, ambulance, etc.) while the caller is kept on the phone. If the call is somehow disconnected or dropped before the emergency is completely reported or the responder arrives, the PSAP may call back the originator using a call back number provided through its databases.

[0002] For example, the call record for a 911 call originated through a wired network may include Automatic Line Identification (ANI) or the telephone number of the access line from which the call originated. However, the mobile directory number (MDN) or telephone number of a wireless subscriber is not associated with a physical line or mobile station. Instead, calls to a wireless subscriber are routed to the mobile station by way of the mobile station identification (MSID), not the MDN. Accordingly, performing an emergency call back to a mobile station poses hurdles not encountered with, e.g., land line devices.

[0003] Typically, the MSID is either a 10-digit mobile identification number (MIN) or a 15-digit International Mobile Subscriber Identifier (IMSI) programmed into a mobile station by the service provider with whom the mobile station user has entered into a service agreement. Accordingly, the MSID is not necessarily a dialable number.

[0004] The MDN of a mobile station is a dialable number. The MDN is dialed by a caller and used to route a call through the network to the wireless subscriber's home system. At the subscriber's home system, the home location register (HLR) contains the MSID associated with the subscriber's MDN. The MSID, not the MDN, is then used to route the call through the network to the serving wireless system and page the subscriber. The subscriber's MDN is provided by the home system to the serving system in a separate data file called the subscriber profile.

[0005] The use of a separate number for MDN and MSID is new to some systems. Historically, in TIA/EIA-41 systems before the implementation of wireless number portability (WNP) or thousands block number pooling (TBNP) based on the Local Routing Number (LRN) method and international roaming (IR), the mobile identification number (MIN) of a mobile station was the same as the MDN. However, with WNP and TBNP, the MDN became "portable" or "poolable" from one service provider to another service provider. Since MSID is not portable or poolable, the recipient service provider assigns a new MSID for a subscriber with a ported-in or pooled MDN.

[0006] International roaming also forced the separation of MSID and MDN. While the MIN is a 10-digit number modeled after the North American Numbering Plan's 10-digit MDN, other nation's carriers using a different directory numbering plan may not allow their MDN to be equivalent to the internationally recognized MIN format. Another standard MSID is the IMSI. It is used in both TIA/EIA-41 and GSM systems around the world. IMSI is a 15-digit number, and therefore, can not serve as a 10-digit MDN.

[0007] Historically, when the MDN was the same as the MIN, the MIN would be delivered to a PSAP and would be used for a call back number. With the separation of MIN and MDN as described above, it became necessary to deliver the MDN as a separate call back number to the PSAP as well as the caller's MSID. There are certain problems associated with implementing this solution. The primary problem is that the serving system may not have the caller's MDN, only the MSID, to present to the PSAP with the call. Some of the reasons for this relate to the way MSID-MDN separation has been implemented according to standards.

[0008] An old serving TIA/EIA-41 system may not support WNP, TBNP or IR. This means that the older serving system may be expecting the MIN and the MDN to be the same. The older system would not even know to look for a separate MDN in the subscriber's service profile (keyed on MIN, not MDN). With this limitation, these subscribers may not be allowed to use basic services, but they must be allowed to call for emergency services. As a result, a roamer who dials "9-1-1" while on an old system will have his or her call delivered to the PSAP with an MSID but no MDN. Accordingly, no call back is possible.

[0009] A newer serving system that is WNP and IR capable may not be able to deliver MDN to the PSAP. This could happen if the calling mobile station is not registered with any service provider (e.g., there are mobile phones used for emergency calls only). It is also possible for a subscriber to place an emergency call before the HLR has responded to the serving system with the subscriber's service profile containing the MDN.

[0010] The call back MDN for an international roamer would require the PSAP to place an international call to reach a subscriber in their local Emergency Service Zone (ESZ). This is not a practical, timely or sufficiently reliable solution for a PSAP that normally does not place international calls and may require immediate call back information in order to save someone's life. In addition, the entire international MDN (up to 15 digits including a country code) may not be presented to the PSAP for callback.

[0011] One proposed solution to these problems calls for delivering 9-1-1+the last 7 digits of the electronic serial number (ESN) of the calling mobile station to the

PSAP as the call back number when the MDN is not available. While this may serve to identify the caller to the PSAP and the serving system, this "9-1-1+ESN7" can not be routed through the network and can not be used to place a call back.

SUMMARY OF THE INVENTION

[0012] The call back method according to the present invention assigns an emergency local routing number (ELRN) to each switch in a wireless network. When a switch of the wireless network routes an emergency call to a Public Service Answering Point (PSAP), the switch sends the emergency local routing number as the calling party number (CgPN) and provides the PSAP with the identifier of the mobile station (MSID). If the emergency call drops, the PSAP performs a call back using the emergency routing number as the called party number (CdPN). As a result the switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. This MSID is used to page the correct mobile station. In an embodiment of the present invention, the PSAP signals the mobile station identifier to the switch in a generic address parameter.

[0013] When a switch receives its emergency local routing number as the called party number, the switches recognizes an emergency call back situation and pages the mobile station identified by the mobile station identifier received in association with the emergency routing number. In an embodiment of the present invention, the switch gives higher priority to handling the call back than other tasks when an ELRN is the CdPN. In this manner, the PSAP is reconnected with the mobile station.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The present invention will become more fully understood from the detailed description given herein below and the accompanying drawings which are given by way of illustration only, wherein like reference numerals designate corresponding parts in the various drawings, and wherein:

[0015] Figs. 1-6 are communication flow diagrams illustrating the operation of the call back method according to the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0016] The call back method according to the present invention assigns a unique routable call back number to each switch (e.g., a mobile switching center (MSC)) in a wireless communication system. This number will be referred to as an "Emergency Local Routing Number" or ELRN hereafter. The ELRN can be thought of as similar to the local routing number (LRN) assigned to each local switch to implement wireless number portability (WNP) or thousands block number pooling (TBNP). However, an ELRN can only be routed to the switch that owns the number, and the ELRN for each switch is unique and is not portable.

[0017] As is known, when a mobile station makes an emergency call, the mobile station identifier (MSID) is supplied in association with the emergency call. For example, the MSID is the mobile identification number (MIN), a ten digit International Roaming Mobile Identification Number (IRM) for those 10 digit numbers outside the range of the North American Numbering Plan, or the International Mobile Subscriber Identifier (IMSI). When a switch of the wireless system receives an emergency call (e.g., a 9-1-1 call) from a mobile station, particularly, a mobile station with no MDN, the switch sends the ELRN of the switch to the Public Service Answering Point (PSAP) serving the switch. The switch supplies ELRN as the calling party number (CgPN), and also provides the PSAP with the MSID of the mobile station. For example, the MSID is signaled such as in the ISUP generic address parameter (GAP).

[0018] If the emergency call drops, the PSAP performs a call back using the ERLN as the called party number (CdPN). As a result, the switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. For example, the MSID is signaled with the call back such as in the ISUP generic address parameter (GAP).

[0019] When a switch receives its emergency routing number as the called party number, the switch recognizes an emergency call back situation and pages the mobile station identified by the MSID received in association with the ERLN and establishes the emergency call back. This ERLN technique may also be provisioned with priority queuing in the switches; wherein the switch handles the call back number at a higher priority than tasks involving other calls. This should improve the emergency call back completion rate even during peak traffic periods at the switch. Furthermore, while described as performed for all emergency calls, use of the method could be limited to just emergency calls made by mobile stations with no or unavailable MDNs.

[0020] Figs. 1-6 are communication flow diagrams illustrating the operation of the call back method according to the present invention. As shown in Fig. 1, a first mobile station MS1 places an emergency call, a 9-1-1 call in this example, that is received by a MSC. Accordingly, the called party number is 9-1-1, and the MSID1 of the first mobile station MS1 is supplied to the MSC as well. The MSC then routes the emergency call to the serving PSAP. In so doing, the called party number remains 9-1-1, but the MSC supplies its ERLN as the calling party number. The MSC also supplies the MSID1 of the first mobile station MS1 in the generic address parameter (GAP).

[0021] If the emergency call is dropped, the PSAP performs a call back using the ERLN as the called party number because the ERLN was supplied to the PSAP

as the calling party number. The result is that the call back is routed to the MSC as shown in Fig. 2. As further shown in Fig. 2, the MSID 1 of the first mobile station is signaled with the call back in the ISUP GAP. As shown in Fig. 3, the MSC uses the MSID1 of the first mobile station MS1 to page the first mobile station MS 1 and complete the call back.

[0022] Assume that while the call back to the first mobile station MS1 is in progress, a second mobile station MS2 places a 9-1-1 emergency call as shown in Fig. 4. As with the emergency call from the first mobile station MS1, the second mobile station MS2 supplies its mobile station identifier MSID2 along with the emergency call (e.g., called party number is 9-1-1). Then, the MSC then routes the emergency call to the PSAP. In so doing, the called party number remains 9-1-1, but the MSC supplies its ERLN as the calling party number. The MSC also supplies the MSID2 of the second mobile station MS2 to the PSAP. Accordingly, Fig. 4 demonstrates that the MSC supplies the same calling party number (i.e., the ERLN) to the PSAP for both of the emergency calls.

[0023] If the second emergency call is dropped, the PSAP performs a call back using the ERLN as the called party number because the ERLN was supplied to the PSAP as the calling party number. The result is that a second call back is routed to the MSC as shown in Fig. 5. As further shown in Fig. 5, the MSID2 of the second mobile station is signaled with the second call back in the ISUP GAP. As shown in Fig. 6, the MSC uses the MSID2 of the second mobile station MS2 to page the second mobile station MS2 and complete the call back.

[0024] The emergency call back method of the present invention ensures a routable call back number is provided to a PSAP with every emergency call from a mobile station. Specifically, the ELRN is one number used to route one or many emergency service call backs to the originating switch (e.g., MSC). The ELRN of the originating switch is signaled to the PSAP as the calling party number (CgPN), particularly when there is no local MDN available to accompany an emergency call.

[0025] In the North American Numbering Plan, the ELRN is a 10-digit number (NPA-NXX-XXXX) where the leading 6-digits (NPA-NXX) are uniquely assigned to each local switch in North America for call routing purposes. The subsequent four digits are assigned by the switch operator. However, the emergency call back method is applicable in a public switched network anywhere in the world. Namely, the ELRN contains those digits assigned from any national numbering plan to route calls to a particular switch. Also, the emergency call back method may be applied with any mobile service or wireless access technology.

[0026] The emergency call back method is independent of number portability and number pooling. These network capabilities depend upon the Local Routing Number (LRN) Method to route a call to a serving switch based on the LRN associated with a ported or pooled dialed number. In comparison, the ELRN is not associated with a dialed number, instead it is associated with a switch.

[0027] In some ways, the ELRN functions in the public network like the Local Routing Number (LRN) required for local number portability; for instance, both function as a single number to route many calls to a particular switch. However, no database query is required to identify the ELRN required to route a call to a serving MSC. As a result, when used as the called party number (CdPN) to route a callback from a PSAP to the serving MSC, the ELRN may be accompanied with the ISUP Forward Call Indicator (FCI) set to indicate no number portability database query is required.

[0028] As discussed above, an ELRN is not associated with any particular MDN and is used to route a call back directly to the serving switch, not the home system. The ELRN eliminates the need for the PSAP to use a MDN to place an emergency call back. There is no need to request an MDN or an LRN to route a callback through a home system as per existing mobile application part (MAP) standards. Also, there is no need to place an international call through a foreign home system to call back an international roamer in the local area. This reduces signaling, saves time and improves service reliability. Further, there is no need for a Temporary Long Distance Number (TLDN), as in TIA/EIA-41 networks, or a Mobile Station Routing Number (MSRN), as in GSM networks, to route a call back from the home system to the serving system. This reduces signaling, saves time and places no demand on the supply of TLDNs or MSRNs.

[0029] The invention being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the invention, and all such modifications are intended to be included within the scope of the following claims.

Claims

1. An emergency call back method, comprising:

   assigning an emergency routing number to each switch in a wireless network for use as the calling party number of emergency wireless calls routed to a Public Service Answering Point (PSAP) by each switch.

2. The method of claim 1, wherein each assigned emergency routing number is not portable.

3. An emergency call back method, comprising:

   sending an emergency routing number of a switch in a wireless network handling communication needs of a mobile station initiating an emergency call and an identifier of the mobile

station to a Public Service Answering Point (PSAP).

4. An emergency call back method, comprising:

receiving an emergency routing number of a switch in a wireless network handling communication needs of a mobile station initiating an emergency call and an identifier of the mobile station at a Public Service Answering Point (PSAP); and
initiating a call back to the mobile station at the PSAP by calling the emergency routing number when the emergency call made by the mobile station drops.

5. The method of claim 1, further comprising:

signaling the identifier of the mobile station to the switch when initiating the call back.

6. The method of claim 5, wherein the signaling step sends the identifier of the mobile station in a generic address parameter.

7. An emergency call back method, comprising:

receiving, at a switch of a wireless communication system, a called party number and a mobile station identifier; and
paging a mobile station identified by the mobile station identifier when the called party number matches an emergency routing number assigned to the switch.

8. The method of claim 7, wherein the receiving step receives the identifier of the mobile station in a generic address parameter.

9. The method of claim 7, wherein the paging step is performed with priority over other tasks at the switch.

10. The method of claim 7, wherein the switch is a mobile switching center.

Fig. 1

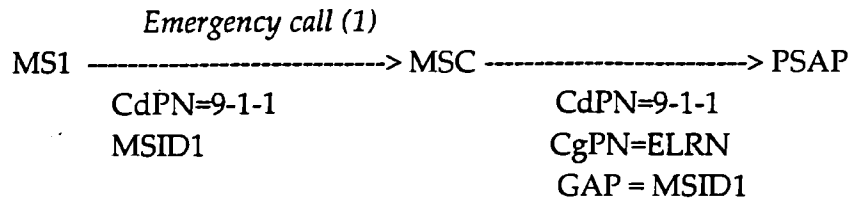


Fig. 2

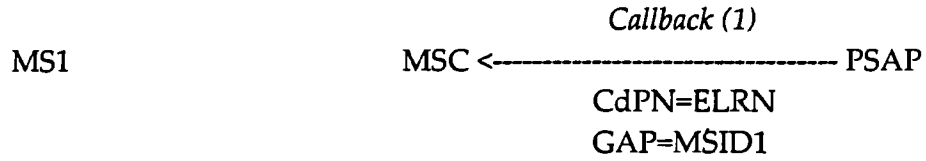


Fig. 3

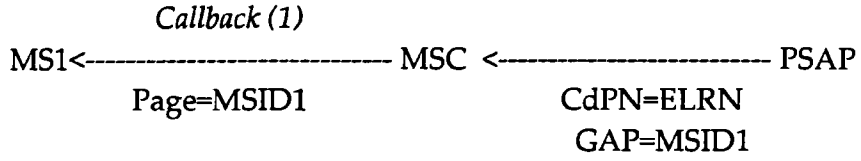


Fig. 4

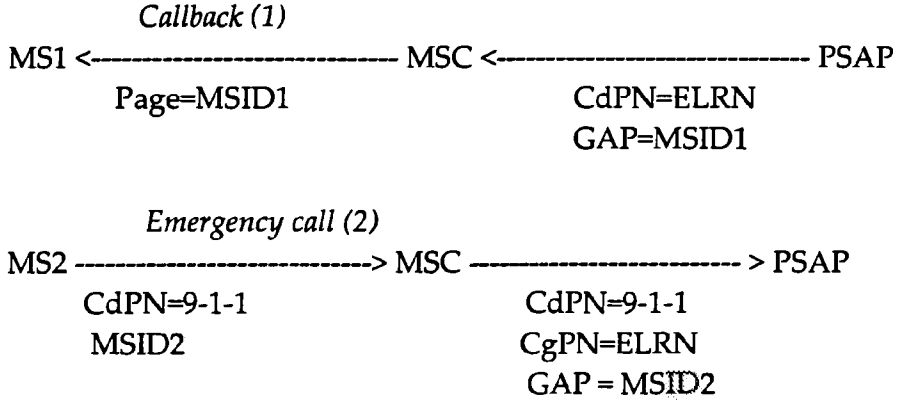


Fig. 5

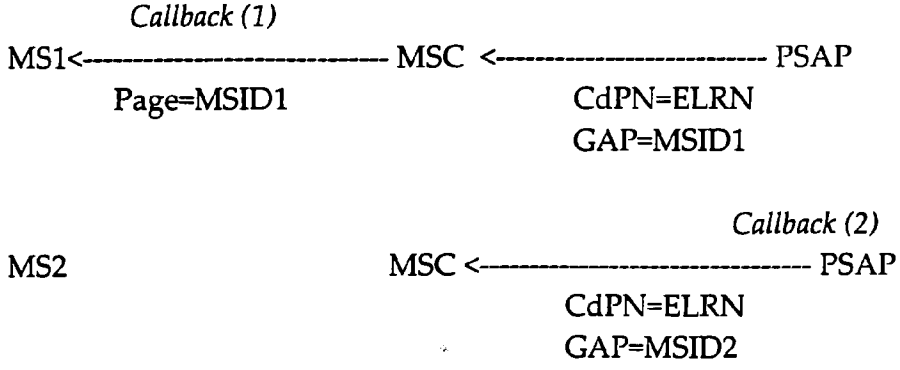
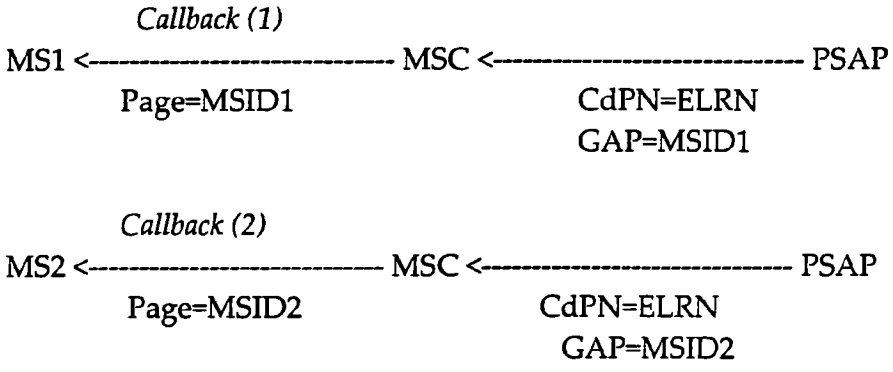

Callback (1)
MS1
MSC
PSAP
Page=MSID1
CdPN=ELRN
GAP=MSID1
Callback (2)
MS2
MSC
PSAP
CdPN=ELRN
GAP=MSID2

Fig. 6


Callback (1)
MS1
MSC
PSAP
Page=MSID1
CdPN=ELRN
GAP=MSID1
Callback (2)
MS2
MSC
PSAP
Page=MSID2
CdPN=ELRN
GAP=MSID2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 25 6372

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 689 548 A (ALPEROVICH VLADIMIR ET AL) 18 November 1997 (1997-11-18) * abstract; claims 1-9; figures 3,4 * * column 2, line 38 - line 67 * * column 5, line 42 - column 6, line 57 *	1-10	H04Q7/38 H04M11/04
A	WO 00 11879 A (QUALCOMM INC) 2 March 2000 (2000-03-02) * page 4, line 12 - line 26 *	9	
T	RICARDO GOMEZ: "Global title translation (GTT) routing " IFAST, vol. 2, no. 1, March 2003 (2003-03), pages 2-3, XP002270040	1-10	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q
H04M

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	12 February 2004	Ohanovici, Z-C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 25 6372

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-02-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5689548 A	18-11-1997	AU 715981 B2	10-02-2000
		AU 3227797 A	09-12-1997
		CN 1226364 A ,B	18-08-1999
		EP 0900511 A2	10-03-1999
		WO 9744971 A2	27-11-1997
WO 0011879 A	02-03-2000	AU 5492099 A	14-03-2000
		BR 9913127 A	06-11-2001
		CA 2341199 A1	02-03-2000
		CN 1323502 T	21-11-2001
		EP 1106028 A1	13-06-2001
		FI 20010322 A	20-02-2001
		ID 29056 A	26-07-2001
		JP 2002523989 T	30-07-2002
		NO 20010829 A	29-03-2001
		NZ 510022 A	28-08-2002
		TW 546978 B	11-08-2003
		WO 0011879 A1	02-03-2000
		US 2002065082 A1	30-05-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 526 697 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.04.2005 Bulletin 2005/17

(51) Int Cl.7: **H04L 29/06**

(21) Application number: **04256443.5**

(22) Date of filing: **20.10.2004**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **21.10.2003 US 690074**

(71) Applicant: **3COM Corporation**
Marlborough, MA 01752-3064 (US)

(72) Inventors:
- **Grabelsky, David**
  Skokie, IL 60076 (US)
- **Homeier, Michael**
  Lake Forest, IL 60045 (US)
- **Tripathi, Anoop**
  Lake Zurich, IL 60047 (US)
- **Joseph, Boby**
  Philadelphia, PA 19131 (US)

(74) Representative: **Finnie, Peter John**
Gill Jennings & Every,
Broadgate House,
7 Eldon Street
London EC2M 7LH (GB)

(54) IP-based enhanced emergency services using intelligent client devices

(57) Providing enhanced emergency services (E-911) to an IP Telephony-based PBX or similar system, by utilizing aspects of the intelligence of end-user SIP client devices to address challenges and difficulties associated with E-911-like services in LAN-based telephony environments.

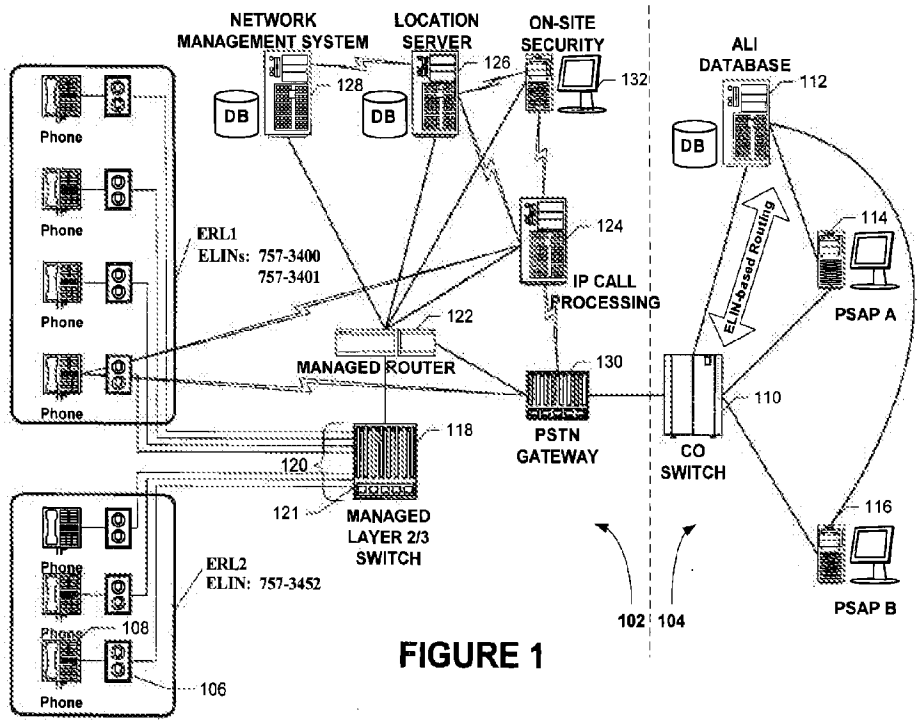


FIGURE 1

EP 1 526 697 A2

Description

Field of Invention

[0001] The present invention is related to voice over IP communication systems, and more particularly, to a method and system of providing IP-based enhanced emergency services using intelligent client devices.

Background to the Invention

[0002] Enhanced emergency services for telephony systems tie the caller's physical location to the call signaling and follow-on messaging. The goal is to increase the effectiveness of the emergency response personnel. By helping pin-point the caller's location, as well as adding reliability to the telephony link between the caller and the emergency responder, precious time may be saved in responding to an emergency. In the United States, the service is referred to as E-911.

[0003] While government and industry groups have worked together to provide consistent requirements of the E-911 system, many aspects of practical implementations have not yet achieved standardization. The variety of systems currently deployed may share common elements in their respective designs, but optimal solutions are still lacking for many of the technical challenges posed by the requirements. This is particularly true for an IP telephony system in an enterprise or campus environment.

[0004] The successful delivery of E-911 service requires that two general areas of operation be satisfied: 1) the ability to route 911 calls to an appropriate emergency response center, based upon the location of the caller (calling station); and 2) the ability of the emergency response center to both locate, and automatically call back to, the calling station, following the receipt of a 911 call from that station (call-back being required, e.g., in the event that the original call gets disconnected). Both of these are related to each other by virtue of their dependency on the location of the calling station. Therefore, accurate and verifiable location of the caller is fundamental to proper implementation of E-911 service.

1. Emergency E911 Terminology

[0005] The definitions below reproduce E-911 terminology listed at the Association of Public-Safety Communication Officials (APCO) website. The list may be accessed at the following Internet website at www.apco911.org/about/pbx/index.html:

9-1-1: A three digit telephone number to facilitate the reporting of an emergency requiring response by a public safety agency.

9-1-1 Service Area: The geographic area that has been granted authority by a state or local governmental body to provide 9-1-1 service.

9-1-1 Service Provider: An entity providing one or more of the following 9-1-1 elements: network, CPE, or database service.

9-1-1 Tandem: (See E9-1-1 Control Office)

Access Line: The connection between a customer premises network interface and the Local Exchange Carrier that provides access to the Public Switched Telephone Network (PSTN).

Automatic Location Identification (ALI): The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone and supplementary emergency services information.

Automatic Location Identification (ALI) Database: The set of ALI records residing on a computer system.

Automatic Number Identification (ANI): Telephone number associated with the access line from which a call originates.

Central Office (CO): The Local Exchange Carrier facility where access lines are connected to switching equipment for connection to the Public Switched Telephone Network.

Centralized Automated Message Accounting (CAMA): An MF signaling protocol originally designed for billing purposes, capable of transmitting a single telephone number.

Data Base Management System Provider: Entity providing Selective Routing (SR) and/or Automatic Location Identification (ALI) data services.

Data Provider: An entity which provides, on a routinely maintained static database, names, addresses and telephone number to be inserted and updated in the E911 MSAG. Data providers are defined as local exchange carriers, alternate exchange carriers, wireless carriers or an entity authorized to act on behalf of any of the aforementioned entities.

Default Routing: The capability to route a 9-1-1 call to a designated (default) PSAP when the incoming 9-1-1 call cannot be selectively routed due to an ANI failure or other cause.

Enhanced 9-1-1 (E9-1-1) Control Office: The Central Office that provides the tandem switching of 9-1-1calls. It controls delivery of the voice call with ANI to the PSAP and provides Selective Routing, Speed Calling, Selective Transfer, Fixed Transfer, and certain maintenance functions for each PSAP. Also known as 9-1-1 Selective Routing Tandem or Selective Router.

Emergency Location Identification Number (ELIN): A valid North American Numbering Plan format telephone number assigned to the MLTS Operator by the appropriate authority that is used to route the call to a PSAP and is used to retrieve the ALI for the PSAP. The ELIN may be the same number as the ANI. The North American Numbering Plan number may in some cases not be a dialable number.

Emergency Response Location (ERL): A location to which a 9-1-1 emergency response team may be

dispatched. The location should be specific enough to provide a reasonable opportunity for the emergency response team to quickly locate a caller anywhere within it.

Emergency Service Number (ESN): A number assigned to specific geographic area within which all E911 calls are routed to one specific PSAP and the residents of the area are served by the same police, fire, and emergency medical agencies.

Emergency Service Zone (ESZ): The geographic area within which all E911 calls are routed to one specific PSAP and the residents of the area are served by the same police, fire, and emergency medical agencies.

Fast Busy: (see Reorder Tone)

Grade of Service: The probability (P), expressed as a decimal fraction, of a telephone call being blocked. P.01 is the grade of service reflecting the probability that one call out of one hundred during the average busy hour will be blocked. P.01 is the minimum recommended Grade of Service for 9-1-1 trunk groups.

Master Street Address Guide (MSAG): A data base of street names and house number ranges within their associated communities defining Emergency Service Zones (ESZs) and their associated Emergency Service Numbers (ESNs) to enable proper routing of 9-1-1 calls.

No Record Found (NRF): A condition where no ALI information is available for display at the PSAP.

P.01 Grade of Service: (See Grade of Service.)

PBX: (See Private Switch)

Primary Public Safety Answering Point (PSAP): A PSAP to which 9-1-1 calls are routed directly from the 9-1 -1 Control Office. (See PSAP)

Primary Rate Interface (PRI): Primary Rate Interface (PRI) is trunking technology which enables the networking of multiple locations. A single PRI trunk can carry various types of traffic. PRI provides such features as Calling Number Delivery, Called Number delivery, Network Redirection and Reason, Network Name, Network Ring Again, Network Automatic Call Distribution, Equal Access, Special number Services, Integrated Service Access (ISA), Network Message service, and Release Link Trunk (RLT). Each PRI trunk group requires one D-Channel and can support multiple DS-1 s up to a maximum of 479 B-channels distributed over 20 DS-1 links. PRI call processing supports Q.931 messages for call setup, call progress, and feature activation.

Private Switch ALI (PS/ALI): A service option which provides Enhanced 9-1-1 features for telephone stations behind private switches. e.g. PBXs

Public Safety Answering Point (PSAP): A facility equipped and staffed to receive 9-1-1 calls. A Primary PSAP receives the calls directly. If the call is relayed or transferred, the next receiving PSAP is designated a Secondary PSAP.

Public Switched Telephone Network (PSTN): The network of equipment, lines, and controls assembled to establish communication paths between calling and called parties in North America.

Reorder Tone: An audible tone of 120 interrupts per minute (ipm) returned to the calling party to indicate the call cannot be processed through the network. Sometimes referred to as fast busy.

SCC: The Qwest 9-1-1 database management service provider.

Selective Routing (SR): The routing of a 9-1-1 call to the proper PSAP based upon the location of the caller. Selective routing is controlled by the ESN which is derived from the customer location.

System Integrator: Coordination and oversight responsibilities as undertaken by the Company relating to the quality of 911 serviced provided by the Company, alternate exchange carriers and data providers.

2. E-911 Service Requirements

[0006] The primary elements of E-911 service are: 1) association of locations with 911 calls; and 2) routing 911 calls to emergency response centers most suited to answering and responding (including dispatching emergency personnel) to specific calls. The emergency response center is referred to as the Public Safety Answering Point, or PSAP. The mechanisms of E-911 service include transport of vital and relevant information in the call signaling, using this information to route the call to the optimal PSAP, and presenting this information to the PSAP personnel to help determine the location of the caller.

[0007] When a 911 call is placed, the location of the caller is used to route the call to an appropriate end-office switch. The calling station location is referred to as the Emergency Response Location, or ERL. The routing can be static, e.g., as in the case of a residential connection to a specific end-office; or dynamic, e.g., as in the case of a lookup by a PBX system based upon the calling station extension. Included in the call signaling is a phone number called the Emergency Location Identification Number, or ELIN, that identifies the ERL from which the call was placed. The ELIN is included in the call signaling of a 911 call as the ANI. In the PSTN, the ELIN is used to route the call to an appropriate PSAP. The routing is done by accessing a location information database called the called Automatic Location Identification (ALI) Database. The ELIN may also be used by the responding PSAP to access the ALI for detailed location information. The PSAP may also use the ELIN to call back the calling station in the event that the call gets disconnected.

[0008] In addition to the procedures used to set up a 911 call and determine the location of the caller, the system must insure that emergency calls cannot be disrupt-

ed by signaling events which might be allowable for non-emergency calls. For example, if the caller has call-waiting service, it must be disabled during an emergency call from that caller's phone. Similarly, only the PSAP, or its representative, may release a 911 call; if the caller hangs up the phone during a 911 call, the call should not be released. Other potentially interrupting service features must similarly be disabled. The PSTN typically provides these capabilities.

[0009] Typically in a PBX system, an on-site emergency facility will be notified when a 911 call is placed. This may be a simple logging system, or a security system that is monitored by security/safety personnel. The information available to such a system may include more detail than that passed to the PSTN, or maintained in the ALI database. For example, the location information available to the on-site system may be precise enough to identify an office or cubicle, while the ERL available to the PSAP may only identify a building floor or wing. Reliance on an on-site component to a PBX emergency response system is one approach to mitigating some of the difficulties in designing such a system.

[0010] Deployment of E-911 behind a PBX introduces further considerations such as location precision, mapping ELIN to calling station, and the information in the ALI database. As noted, the specification of the location of a 911 calling station is defined as the Emergency Response Location, or ERL. The precision with which the ERL actually locates a calling station may vary. For example, for residential service, an ERL may be the address of a house, or a unit within an apartment complex. For an enterprise PBX, an ERL could be a building address, a floor in building, a wing on a floor, or even an office or cubical.

[0011] When an ERL corresponds to an extended area, such as building floor or wing, it may contain multiple calling stations. Note that the information used both to route a 911 call to a PSAP, as well as to provide the PSAP with the location of the calling station, is only as precise as the ERL from which the call is placed. Considerations in specifying an ERL can include state and local regulations governing required precision of the location, and, in the case of multi-station ERLs, the maximum number of calling stations that a single ERL may contain. Recall that the identity of an ERL is associated with the ELIN, which acts as a phone number. Note that one ERL may possess more than one ELIN, but one ELIN may identify one and only one ERL.

[0012] Within the PSTN, location information is maintained in a database called the Automatic Location Identification (ALI) Database. Typically, there are multiple ALI databases, each associated with, e.g., a different calling area, or different local exchange carrier (LEC). The ALI database essentially correlates ELINs with ERLs, as well as with routing rules for directing 911 calls to appropriate PSAPs. Thus the ALI database is queried using the ELIN when a 911 call is made to determine which one of possibly multiple PSAPs should receive the call. Once the call is received by the PSAP, the ELIN may again be used to query the ALI, this time to provide ERL information. The ELIN can also be used by the PSAP as a direct call back number to the calling station, e.g., in the event that the original call is disconnected. That is, as far as the PSAP is concerned, the ELIN functions as a Direct Inward Dial (DID) number to the calling station. Note that in the case of multi-station ERLs, a single ELIN may be shared among all calling stations in an ERL. Therefore, in order for the PSAP to be able to use the ELIN as a DID number to refer to a specific calling station, some form of mapping from ELIN to calling station must be implemented by the PBX.

[0013] When a 911 call is placed from behind a PBX, the ERL of the calling station is the factor that determines the ELIN that will be passed to the end-office switch; i.e., into the PSTN signaling space. Before the call is actually passed to the PSTN, the PBX, or some associated on-site emergency service system, must first select an appropriate end-office switch. If there is only one choice (i.e., the PBX is connected to only one switch), then the decision is pre-determined. If there is more than one, then the on-site system must be configured to route 911 calls to end-office switches based upon ELIN (or ERL). When the switch receives the call, it (or an agent of the switch) consults the ALI database to determine the proper PSAP to which the call should be routed.

[0014] Once the PSAP receives the call, the location and callback information it gets is only as specific as is contained in the ELIN and the ALI database. That is, any site-specific mapping or location information that is not contained in the ERL definition in the ALI database is not passed in the call. Typically, calls outbound from a PBX do not pass internal extension information. This means that if an ERL contains several calling stations, the ALI will only locate the ERL, not individual calling stations. Also, even if each calling station has its own DID number, the PSAP will only receive the ELIN of the ERL; the on-site emergency system must incorporate intelligence to recognize that a 911 call has been made, and, if multi-station ERLs are used, to establish and maintain a mapping of ELIN to DID of the calling station (to support the event of call disconnection to the PSAP). Depending upon the level to which internal location information is passed in outbound 911 calls, a PBX may actually have to multiplex call-back numbers across internal location areas, rather than provide location-unique information to emergency response centers. To complicate matters further, the allowable size and definition of such internal areas may be subject to different regulatory rules in different states or localities.

[0015] Unless each calling station is its own ERL, then sharing of ELINs among calling stations leads to the possibility of more than one concurrent 911 call using a single ELIN. While the ERL information in such a case would be correct, the callback information would be ambiguous, since the PSAP would have no way of uniquely

identifying the calling station beyond ELIN, and thus the PBX would not be able to de-multiplex a callback from the PSAP based upon ELIN alone. Note that while the ALI database must be regularly updated to reflect configuration changes in the PBX system, such updates are not intended to provide dynamic mapping on a call-by-call basis.

[0016] One way to deal with the case of multiple calls per ERL is to assign multiple ELINs to multi-station ERLs. Such a technique is used in the Emergency Response E-911 system by Cisco, for example. The number of ELINs per ERL can be determined according to the statistical probability of concurrent 911 calls in an ERL of a given size. As long as the number of ELINs assigned to an ERL is always greater than or equal to the number of concurrent 911 calls from that ERL, then there can always be a unique mapping of ELIN to calling station. One limitation is that "always" can not be guaranteed except for the case of single-station ERLs. Given multi-station ERLs, the issue of the number of ELINs provisioned for each ERL is primarily one of cost: the PSTN service provider charges for each ELIN assigned. Thus for multi-station ERLs, there is a tradeoff between a "safe" ratio of calling stations to ELINs, and the cost of ELINs. The importance or relevance of this tradeoff is partially dependent upon the size and type of PBX.

[0017] For example, in a traditional (TDM) PBX system that provides each calling station with a DID number, single-station ERLs are not necessarily an excessive allocation of circuit resources. Since the service provider charges for each DID number, the PBX can, in principle, use each DID as an individual ELIN, thereby providing each calling station with its own ERL (and ELIN). This can work because, in a circuit-based PBX, even though each DID is typically associated with a person (e.g., employees at an enterprise), each is also assigned to a specific calling station. Because a 911 call is tied to the ERL of the calling station, the DID number identifies the ERL.

[0018] The situation is different in an IP-based PBX that uses, e.g., SIP. In this case, even if each person served by the PBX has an individual DID number, that number is not necessarily tied to a specific calling station (i.e., SIP phone). Rather, each DID number is associated with a person, and any person could register at any SIP phone behind the PBX. As a result, no predictable association exists between personal DID numbers and ERLs. It is still possible to tie each calling station to an ERL by virtue of some hardware attribute and assign an ELIN to the ERL. However, in order to support single-station ERLs in this environment, a complete second set of hardware-identifying DID numbers would be required to assign one each to every calling station. While this would free personal DIDs to travel with each user, it could be expensive, and requires a burdensome level of provisioning of circuit resources.

[0019] In addition to the problems associated with the ELIN-DID mapping in multi-station ERLs in IP-based PBXs, LAN system and equipment configurations tend to be more fluid, in general, than circuit-based PBX systems. Layer 2/3 switches can be moved or reconfigured, IP subnets can be modified, and SIP phones can be relocated. Within the context of E-911 service, this characteristic has the potential of translating into problems or difficulties in maintaining accurate location information, even for calling stations. Some solutions, such as the Cisco Emergency Responder, utilize a centralized device (e.g., the Emergency Responder node) to query a network device (e.g., the CallManager) to obtain a list of registered phones. The central device then queries individual switches to determine which physical ports are associated with those phones. Because a user's location may change at any moment, the central device must repeat this process continuously. If the time between queries is short, the amount of network traffic can become large, and if the time interval is too long, the risk of improperly reporting the ERL increases.

[0020] A LAN-based or VoIP-based PBX can introduce additional problems because internal extension numbers, which are usually associated with a person, may not be accurate indicators of location. For example, in the case of a SIP-based system, a given end user with a "fixed" phone number may actually register at arbitrary locations within network. If such a user makes a 911 call, then the fixed phone number associated with that user may provide inaccurate, or worse, dangerously erroneous, location information. To address this problem, a 911 caller's phone number must be mapped to a physical attribute of the phone, such as MAC address, which in turn may be associated with a current network location.

[0021] While conceptually straightforward, this solution brings with it added complexities, such as a new layer of indirection in the mapping, possible delay issues, and the need for a method for reliable location tracking of "portable" phones, among others.

[0022] In addition, reliance on network-based call control elements in setup of 911 calls can introduce a failure point. While redundant elements may be added, this increases the expense and configuration of the E911 system. It also requires call control elements to reside on the same site as the phones in order to avoid WAN-based communications to complete a 911 call. In turn, this may add further expense for small sites that could otherwise use WAN-based communications for non-emergency calls. Consequently, a system that overcomes these limitations is desirable.

Summary of the Invention

[0023] Described herein is a method of providing enhanced emergency services (E-911) to an IP Telephony-based PBX or similar system, by utilizing aspects of the intelligence of end-user SIP client devices to address challenges and difficulties associated with E-911-like services in LAN-based telephony environments.

[0024] The system and methods limit, or preferably eliminate, direct reliance on the IP Call Processing network element (e.g., SIP Proxy) during actual emergency calls. The system and method preferably incorporates processing capabilities of intelligent IP phones. In one embodiment, information necessary for initiating 911 calls is stored in the phone. The information may include an ERL identifier, or one or more ELINs for identifying the source of the 911 call to the PSAP.

[0025] Thus, one aspect of the preferred embodiments is to provide ERL information to an intelligent phone, thereby enabling it to place emergency calls directly to a PSTN gateway, without involvement or aid of any other call signaling components. This also enables network configurations in which the call signaling component may be resident at a site remote from the intelligent phones, without the danger of a failed inter-site link causing an inability in placing an emergency call.

[0026] In one preferred embodiment, the IP phone communicates directly to a PSTN gateway, bypassing any signaling agents typically used to set up a call. In an alternative embodiment, the call is initiated by communicating with call signaling elements, such as a SIP Proxy device. In either embodiment, the method preferably includes providing the phone with ERL information (in the form of one or more ELINs) to provide to the gateway or call signaling element. Further aspects of preferred embodiments include providing the phone with a default gateway identifier, thereby allowing the phone to identify a default PSTN gateway to use for 911 calls when bypassing the normal signaling elements. The ERL, ELIN and/or default gateway identifier information may be provided during the phone's boot-up procedure, or using subsequent signaling messages.

[0027] A location server preferably stores the ERL and associated ELINs, as well as default gateway identifier information. In addition, the location server preferably stores location information associated with the IP phone. A further aspect of preferred method is the use of an intelligent PSTN gateway that is capable of receiving and acting upon IP-based call setup signaling directly from IP phones, as well as implementing some ancillary functions associated with 911 calls.

[0028] There are numerous network management tools and systems that can auto-detect network topology and operational state. An element of E-911 service in an IP-based PBX, then, is interfacing to, or integration of, the appropriate network management functions that ensure accurate and reliable location information.

[0029] An additional feature of certain preferred embodiments includes automatic discovery of intelligent phone location when the phone registers with the system. This may involve the merger of the network management system with the signaling system to be able to find device. The preferred embodiments include a Location Server as the architectural element of the network that bridges the call signaling components and the network management components. The location server, based on the MAC address of a calling device or an IP address assigned to a calling device, is able to determine a physical port associated with the device. The determination may be made through a network management system.

[0030] In another aspect of certain preferred embodiments, the intelligent phone enters into a state of emergency readiness before presenting dial tone, and without the need for a specific user to register in the network via the phone. This may support, e.g., public phones, at which no user is registered, but from which calls, in particular emergency calls, may be placed.

[0031] Still further aspects include certain actions by the intelligent phone for ensuring that emergency calls cannot be disrupted by otherwise normal call signaling events to the phone. These include sending a notification to the network signaling agent (e.g., SIP Proxy) informing it that an emergency call has been placed; or deregistering the user from the phone (via SIP signaling to the Proxy), so that the IP network will not even try to place calls to the phone.

[0032] Additional aspects include actions by the intelligent phone for ensuring that emergency calls cannot be released by the caller once the call has been connected to the PSAP. These include declining to generate and/or send the appropriate IP-based signaling message(s) that would initiate the call release sequence. In addition or instead, the phone could automatically activate its speaker and/or microphone if and when the caller attempts to release a connected emergency call. This feature may be easily extended to systems utilizing video phone features or capabilities to provide a monitoring function.

[0033] Yet another feature of the system is a PSTN gateway that is configured to accept direct signaling from intelligent phones in the case of emergency calls. That is, the preferred gateway includes a SIP stack to accept an invite from something other than a SIP proxy. In certain embodiments, the gateway stores ERL and associated lists of ELINs for use in initiating an outgoing 911 call. The preferred PSTN gateway is also configurable to provide priority handling to emergency calls. In addition, the gateway preferably maintains a record of in-use ELINs, performs ELIN management, generates CDRs associated with emergency calls, sends a notification to the safety/security station when the call is placed, and provides backup storage of intelligent phones' ERL information.

Brief Description of the Drawings

[0034] Examples of the present invention will now be described in detail with reference to the accompanying drawings, in which:

FIG. 1 is a block diagram illustrating one embodiment of a high-level reference architecture;

FIG. 2 illustrates the functional elements of E-911

service in one preferred embodiment;

FIG. 3 illustrates a preferred embodiment of a location server and database;

FIG. 4 illustrates a preferred method of configuring a phone for emergency state readiness;

FIG. 5 illustrates an alternative preferred method of configuring a phone for emergency state readiness;

FIG. 6 is a call signaling flowchart for phone initiation; and

FIG. 7 is a call signaling flowchart for establishing a 911 emergency call.

Detailed Description

A. Reference Architecture

[0035] The basic components of IP-based E-911 service are illustrated in Figure 1, which depicts a high-level reference architecture of a preferred embodiment. The elements are shown to reside either behind the IP PBX (Enterprise Premise area 102) or in the PSTN space (Service Provider & PSAPs area 104). Multi-station emergency response locations ERL1 and ERL2 reside in the enterprise area 102. ERL1 may be associated with a description of the Emergency Response Location, for example, of 3200 Main Street, 3rd floor, and ERL2 may be associated with a description of 3200 Main Street, 2nd floor, cubes 5 through 7. Note that ERL1 has two ELINs, while ERL2 has just one.

[0036] The physical connection points to the network are preferably provided by some form of jack (e.g., an RJ45) which are identified with physical locations. An example physical location is jack 106, indicated for the bottom-most connection point in Figure 1, which might be an RJ-45 jack located on the second floor, cubicle 7. Other types of connection hardware and networking may be used, such as token ring, optical fiber, and wireless ports (e.g., 802.11, Bluetooth, etc.). In Figure 1, an IP phone (e.g., phone 108) is connected to each managed physical connection point 106, which is connected to a single managed port 121. The phones may use the Session Initiation Protocol (SIP), for example, but other types of IP-based phones may also be used. The phones may be dedicated programmable hardware, or soft-clients running on, e.g., desktop computers.

[0037] The PSTN side 104 includes a Central Office (CO) switch 110, an ALI database 112, and two PSAPs 114, 116. There may be more or fewer of each of these components. Note that the enterprise side 102 may actually be distributed over multiple sites or campuses. In such an embodiment, it is assumed that some form of secure managed links is maintained between individual sites. As examples, VPN connections over IPsec, or private leased lines may be used.

[0038] Managed Layer 2/3 switch 118 is the managed switch that provides the first point of connectivity to the network for the IP phones (and other IP client devices). As illustrated, ports 120 on the switch 118 are connected directly to the managed physical connection points, such as port 106. The switch 118 is typically resident at the same site as the phones (and other devices), which use it to connect to the local IP network. Note that there may be other switches at topologically higher levels in the network.

[0039] The managed router 122 represents the managed network infrastructure above the managed switch 118. That is, there may be a multiplicity of routers and related devices (e.g., DHCP servers, AAA servers, etc.). From the point of view of determining the location of IP phones, only the managed switch 118 is relevant. Thus, only a single representative router 122 is shown in Figure 1. In embodiments having multiples sites, each site may have one or more routers.

[0040] An IP Call Processing network element 124 is responsible for IP-based signaling and call control. For example, in a SIP-base system, this may be a SIP Proxy server. The Call Processing element 124 may be located at the same site as the phones that it services, or may be located remotely at a different (possibly central) site. If remotely located, the relevant signal messaging will traverse the inter-site connections (e.g., secure VPNs).

[0041] The Location Server 126 is a network element that keeps track of where phones are located, maintaining the information in a database. This element may be located at the same site as the phones, or remotely, at a different (possibly central) site. If remote, the relevant communications with other network elements may traverse the inter-site connections (e.g., secure VPNs).

[0042] Network management system (NMS) 128 is a combination of hardware and software that monitors and manages the network. In the context of E-911 services, the NMS 128 should be capable of discovering the location of any IP phone, as specified by the managed switch 118 and switch port 120 to which the phone connects. The NMS 128 may be located at the same site as the phones, or remotely, at a different (possibly central) site. If remote, the relevant communications with other network elements may traverse the inter-site connections (e.g., secure VPNs).

[0043] The PSTN gateway 130 provides an interface to the CO switch 110 (e.g., via PRI lines) on the PSTN side, and IP connectivity (e.g., via RTP) on the IP network side. The gateway 130 may interact with the IP Call Processing element 124 in order to manage calls, but may also be able to communicate directly with intelligent IP phones for this purpose. The gateway element 130 is typically on the same site as the phones that it services, since it is preferably connected to the local PSTN. However, it could be at a remote site, but preferably is able to place PSTN calls to the appropriate PSAP for the phones that it services. In addition, it is desirable for the gateway 130 to be able to establish and maintain reliable IP connectivity to those phones across the inter-site IP links.

[0044] The On-site Security Station 132 is a monitor-

ing station at which security/safety personnel may obtain real-time status and information on emergency calls placed to a PSAP. It must be on the same site as the phones that it services. That is, it is intended to support on-site personnel in responding to local (same site) emergency calls.

[0045] In Figure 1, all of the above elements are shown to have physical connections (solid lines) to the network (represented by the Managed Router 122). Logical links, shown as zig-zag lines, indicate which elements communicate with each other in the implementation of E-911 services. Only a single, representative phone 108 is shown to have such links; it should be understood that all phones may have similar logical links. Note that not all possible communications links are shown, and that others are possible. Finally, there may be other elements of a local data and IP telephony network which are not shown in Figure 1. These may include other application servers, multimedia servers, etc. It should be understood that their omission from Figure 1 does not exclude their possible presence in a network that supports E-911 services.

B. Exemplary Method for Emergency Telephony Services

[0046] In the following descriptions of preferred embodiments, the IP telephony network is assumed to be based upon SIP, and SIP messaging is used to illustrate the system and method. However, other protocols that support direct signaling and call control messaging between the IP phones and the PSTN gateway are also possible (e.g., H.323). First the functional architecture is presented, followed by a description of system initialization, and finally actual call processing. In addition, some configuration and provisioning considerations are discussed.

1. Functional Architecture

[0047] Figure 2 illustrates the functional elements of E-911 service in a preferred system, as well as the architectural relationships among them. The elements include a SIP phone 202, Managed Access Switch Port 204, 911 Location Server and Database 206, PSTN Gateway 208, DHCP Server 210, Software Image Download Server 212, NMS 214, SIP Proxy Server 216, Local Security Station 218, Accounting Server 220, ALI Liaison Server 222, and Provisioning Server 224.

[0048] SIP phone 202 is the calling station from which 911 calls may be placed. It includes processing intelligence; i.e., a SIP user agent for support of the SIP protocol, plus additional application capabilities for features, functions and services, including speaker mode. Phone 202 uses DHCP to obtain an IP address, and may also obtain other custom options via DHCP. Custom options may be used, for example, to identify the Software Image Download server, or a default SIP Proxy server. The SIP phone does not necessarily support SNMP. However, phone 202 does support the 911-specific functionality associated with this system and method.

[0049] The Managed Access Switch Port 204 typically identifies the first layer 2/3 switch and switch port within the managed network infrastructure to which the SIP phone connects for access to the local IP network. This typically does not include any layer 2 devices that may possibly be deployed between the phone and the first managed switch; e.g., a desktop switch which is not part of the managed infrastructure. The managed switch preferably supports SNMP, or an alternative network management protocol.

[0050] The 911 Location Server Database 206 is a centralized server that preferably maintains two databases: an ERL database 302, and a Phone Location database 304, as shown in Figure 3. The ERL database typically stores one record 305 for each ERL in the campus or site served by the emergency system. Each ERL record 305 preferably contains the following information: ERL identification 308; Assigned managed switch and switch ports 310; Assigned managed physical connection points 312; Assigned ELINs 314; Assigned PSTN gateways 316; and Location Description 318. Alternative ERL records may contain a subset of these parameters, and may also include others not listed here.

[0051] The composite information in an ERL record 305 defines the ERL. ERL definitions are created first "on paper" as part of a site management process that may or may not lend itself to automation. That is, the assignments of switch ports, ELINs, etc., to an ERL may depend upon the physical layout of the site, and hence require human decision making. The ERL records in the database may be populated as part of a provisioning/configuration process.

[0052] The Phone Location database 304 stores one record 319 for each registered phone in the system. Each phone location record 319 preferably contains the following information: IP address 320 of the phone; Assigned ERL 322 (ERL identification); Assigned managed switch and switch port 324; Assigned managed physical connection point 326 (only if port-to-connection point is one-to-one); Assigned ELINs 328; Assigned PSTN gateways 330; MAC address 332 of the phone; and Serial Number 334 of the phone. Additional information may also be contained in the phone location record.

[0053] Note that an ERL record 305 may contain multiple switch ports 310 and multiple physical connection points 312, while a phone location record 319 contains only a single switch port 324 and single physical connection point 326. That is, an ERL serves one or more possible switch ports 120, while a phone 202, 108 is served by one of each of these entities (i.e., one physical connection point, and one switch port). In contrast, each phone may be served by all of the ELINs and PSTN gateways assigned to its ERL. Note also that, if a single

switch port is connected to multiple managed connection points (e.g., several cubes sharing access to a switch port), then it is not possible to determine the connection point from a phone's IP address. In such cases, its physical connection point may be omitted from the Phone Location record. However, typical LAN configurations do use one-to-one assignments of switch ports to physical connection points. In these cases, the switch port is equivalent to the physical connection point, provided the mapping information is maintained.

[0054] The process for populating the Phone Location database is dynamic, executing in response to a request to the 911 Location server from the SIP Proxy server 216. Given an initial request from SIP Proxy server 216 with the IP address or MAC address of a SIP phone, the 911 Location Server 206 discovers the Managed Access Switch port 204 for the phone, and uses the switch port identification 324 to index the associated ERL record. A new Phone Location record 319 is then created, and the associated information loaded. Subsequent requests from the SIP Proxy Server 216 using the same IP address or MAC address may cause the Phone Location record 319 to be retrieved, or a new location discovery process to be launched. A new discovery process may result in updated location information, which may be used to update the Phone Location record 319.

[0055] It should be understood that the descriptions of these databases are illustrative, and they may be implemented in multiple ways. The description herein is one of many ways. For example, alternative embodiments may use less information and fewer data fields, or there may be additional information in additional data fields included in these databases. In addition, the 911 Location Server databases 302, 304 may serve phones that are co-resident at the same site, or resident at a site remote from the server.

[0056] The PSTN gateway 208 provides PSTN connectivity to the packet-based phone system. For a given SIP phone, this is the specific media gateway, or set of media gateways, from among a possible plurality of media gateways available to the phone, that provides access to the PSTN for 911 calls. The Gateway 208 terminates SIP calls from, and originates SIP calls to, the SIP phones that it serves. It also supports additional SIP functionality for communication with the Local Security Server 218. If multiple PSTN gateways are available, each SIP phone may be assigned a prioritized list for backup/reliability purposes. In addition, the PSTN gateway 208 supports some ancillary tasks associate with 911 calls, including maintaining a record of ELINs that are in use, and maintaining minimal call-state information specific to active 911 calls.

[0057] The DHCP Server 210 provides IP client devices such as SIP phone 108 with IP addresses and other parameters when they first start up, and upon subsequent request. DHCP server 210 responds to the SIP phone's initial DHCP request for IP access in the local network. In addition to an IP address, the DHCP response message may include custom options, such as identification of a Software Image Download Server 212.

[0058] The Software Image Download Server 212 provides each SIP phone with its software image when it initializes, or boots up, through the use of a download request message and a download response. Note that other methods of supplying the SIP phone with its software image are possible, such as non-volatile ROM or RAM storage in the phone. Such alternative methods may eliminate the need for the Software Image Download server 212.

[0059] The Network Management System (NMS) 214 is a combination of hardware and software that monitors and manages the network. It may reside in a remote or central site, but can still perform basic network management functions, such as device discovery, and topology mapping in the local network. In particular, the Network Management System 214 may discover the Managed Access Switch port 204, given the IP address or MAC address of a connected SIP phone. It may also be used to discover if any unmanaged switches are in the path between the SIP phone and the Managed Access Switch port. In a preferred embodiment it uses the SNMP protocol to communicate with the various network components.

[0060] The SIP Proxy Server 216 is the IP Call Processing network element 124 in a SIP-based system. SIP Proxy Server 216 may reside in a remote or central site.

[0061] The Local Security Station Sever 218 is the monitoring station in an on-site system that may be monitored by security/safety personnel. This station provides alerts when 911 calls are placed, and supplies additional location information that may not be available in the ERL definition in the ALI database. For example, the switch port to which the SIP phone is connected may be used to identify a specific location, such as an office or cubicle. It may also provide web-based user interface.

[0062] The Accounting Server 220 is a repository of records related to calls that have been made in the system. Accounting Server 220 is a sever suitable for maintaining call detail records, as well as associated management functions, such as reading, writing, and updating records. In particular, it maintains call detail records associated with emergency calls.

[0063] The ALI Liaison Server 222 is an application that converts the system's ERL information, in particular Location Description 318, into a format compatible with the ALI database maintained by the LEC or service provider. The ALI liaison is configurable to adapt to multiple ALI database formats used by LECs and service providers.

[0064] The Provisioning Server 224 is a server that allows network managers and operations personnel to create/update provisioned data and parameters of the system such as user accounts and authorizations. In the context of E-911 service, it can be used to manually pop-

ulate the ERL database in the 911 Location server.

[0065] Note that some of these elements, such as the SIP Proxy Server 216, the PSTN Gateway 208, and the Accounting Server 220, may be common to other functions of an IP telephony system, besides E-911 service. In addition, some elements used in the operation of an IP telephony system, but not specifically in E-911 service, may be omitted from the figure for clarity. Interfaces between elements are represented by specific protocols, identified in the double arrows connecting the elements. The interface identified simply as "IP" supports standard IP communications, without reference to specific high-layer protocols. Similarly, the arrow labeled "L2/L3" represents the basic, low-layer support of all upper-layer protocols. Note that "3Q" is a 3Com protocol which is similar to RADIUS. Thus, RADIUS or other suitable protocols (e.g., DIAMETER) may be used in alternative embodiments. The arrows 230, 232, 234, 236, represent information flow through an API or interactive user interface. All of the protocols in this illustration are exemplary, and alternative suitable protocols may be used.

[0066] In Figure 2, the dotted circle 238 surrounding the SIP phone 202 identifies all the protocol interfaces that are supported by the phone's physical connection to the Managed Access Switch port 204. The switch port 204 itself is included explicitly because it provides the most precise physical location for the phone 202 that is known to the overall system, and therefore performs a functional role in enabling E-911 service. Note that the management of the switch port 204 by the Network Management System 214 is also explicitly shown (via SNMP in this illustration). For all the other indicated protocol interfaces, the switch port 204 provides the usual network access, and thus is omitted from the communication paths depicted in Figure 2 for clarity.

2. System Configuration

[0067] When an IP telephony system is deployed at an enterprise or campus, each ERL is preferably defined in terms of the Managed Access Switch ports and physical connection points that will be included. The process of mapping the topology of these switch ports may be an automated feature of the Network Management System, but the task of assigning individual switch ports and connection points to specific ERLs requires human decision making. The task of assigning an ELIN or ELINs to each ERL is similarly discretionary.

[0068] Assignment of the PSTN gateway or gateways may be determined in part by requirements of the LEC, but may also include some discretion on the part of the site management. The considerations that go into making the assignments may include state and/or local regulation, as well as preferences of the site management personnel.

[0069] Once the configuration is defined, it is provisioned in the 911 Location Server database 206. Each Managed Access Switch port 204 is included in an ERL record 305, which preferably contains the information shown in Figure 3, and discussed above. Again, other information may be added to the ERL record 305. For example, when a SIP phone 108 registers, it becomes associated with an ERL, by virtue of the phone's physical connection point 106 and switch port 121. The ERL record may be dynamically extended to include the IP and/or MAC addresses of all associated and/or registered SIP phones. Other ancillary information may also be included in the record, such as, phone extension numbers, cube numbers, names of employees assigned to the locations (areas, offices, cubes, etc.), text or image-based descriptions of the location, and any other relevant information (including file names or URL or other links to additional information) that may be useful in assisting emergency response teams.

[0070] Any time the network configuration is modified, the provisioning information associated with the ERL records is preferably updated. Modifications include, but are not limited to, adding/removing switch ports to/from an existing ERL, adding/removing ERLs, and modifying network switch interconnections or topologies. As described below, the system also includes periodic self-consistency checks in order to detect any such modifications for which the provisioning updates were not made, or were made incorrectly.

3. SIP Phone Initialization and Default Registration

[0071] The method 400 of SIP phone initialization and default registration shown in Figure 4 illustrates how a SIP phone first achieves a state of emergency services readiness (that is, a state in which any arbitrary end user may use the phone to place a 911 call). This may be an appropriate state for a public phone; no actual user registration would be required. The steps outlined below describe a preferred embodiment of the system and method, and it should be understood that altemative implementations may be used to achieve the desired results. Some of the possible alternatives are noted as well, but these are not intended to represent the full range of implementation approaches.

[0072] In a preferred method 400, the phone first registers (step 402) with the system using a configuration associated with a default profile. The system then determines (step 404) the ERL information associated with the phone based on the phone's location, and at least a subset of the ERL information is then provided (step 406) to the phone. The ERL information provided to the phone preferably includes one or more ELINs that may be used when the phone initiates an emergency 911 call.

[0073] In an alternative embodiment shown in Figure 5, a preferred method 500 operates as follows: when a SIP phone (e.g., phone 202) is first connected to the Managed Access Switch port 204 and powered on, it is initialized, as shown at step 502. Initialization involves

booting the phone 202 with its operational software and generally registering on the network, by, e.g., obtaining an IP address. Preferably, the phone will issue a DHCP request to initially obtain its IP address. Assuming the phone 202 acquires its software image from a download server 212, the DHCP response may also contain the address of this server in an option data field of the message. Similarly, the address of the SIP Proxy server 216 may be included in a DHCP option field. If a download server 212 is not used, then the associated option may be omitted; the address of the SIP Proxy 216 may be determined in another manner, such as pre-configuring the information in the phone 202.

[0074] In one preferred embodiment of step 502, the phone 202 will next request its software image from the download server 212. After download, the phone will boot the image and again contact the DHCP server 210 to renew/reinitialize its lease, and possibly request a new IP address on a specific subnet. This second DHCP request may be omitted from step 502 if the phone's software resides locally on the phone 202 in RAM or ROM memory.

[0075] At step 504, the phone 202 performs default registration. Typically the phone 202 will issue a SIP REGISTER message to its SIP Proxy server 216 in order to obtain a default registration; this message may also contain information about the phone hardware if it is relevant to the SIP Proxy's actions. Note that this request is not associated with any specific end user, but with the phone itself. Upon receipt of the SIP registration request, the SIP Proxy server 216 will access a default profile for the phone, either from a local cache, or an external profile server. The profile may contain such information as keypad mapping, allowed functions, etc., for default operation of the phone.

[0076] At step 506, the relevant ERL information is obtained. Preferably, SIP Proxy 216 will issue a request to the 911 Location Server 206 for the ERL information for the SIP phone 202, passing the phone's IP and/or MAC address as its identifier. In some embodiments, the location server does not populate or dynamically update its database of phone identification records 319 until a query is received. In such embodiments, the initial request for this phone may result in the absence of a record 319 for this IP and/or MAC address. Thus, at step 508, the 911 Location Server will use the phone's IP and/or MAC address in a request to the Network Management system for the identity of the Managed Access Switch port to which the phone is connected. Step 508 may be omitted in embodiments where the phone location record is updated via other means, typically associated with the phone registration (for example, in response to a DHCP request or DHCP response, or software image download, etc.). In further alternative embodiments, the database information may be co-located or merged with the SIP proxy function.

[0077] The Network Management system 214 may also be able to determine if there are any intervening, unmanaged switches between the phone and the managed switch port. The Network Management system 214 will provide the switch port identification in its response (or in its dynamic update) to the 911 Location server 206, along with the identity of any intervening, unmanaged switches. If there are any unmanaged switches in the path between the phone and the managed switch port, then the 911 Location server 206 may choose to deny admission of the phone into the system. Such an action would prevent potentially bogus location information from being entered into the database. The action may also be accompanied by an alert to the NMS 214, or similar monitoring function, allowing for corrective action to be taken. If the phone 202 is connected directly to the managed switch port 204, then the 911 Location server 206 uses the switch port identification to lookup the associated ERL record in step 510, and at least a subset of the information in the record is returned to the SIP Proxy. Preferably, the ERL information provided to the SIP Proxy includes a list of ELINS for the ERL. Alternative embodiments may include other information such as text description of the location, cube or office number, occupant(s), etc. A Phone Location record 319 is also created (or updated) for the phone, and entered into the Phone Location database.

[0078] When the SIP Proxy receives the ERL information, it sends at least a subset of it to the SIP phone at step 512. The subset includes one or more ELINs for use in a subsequent emergency 911 call. The ERL information is preferably sent in the OK message, along with the phone's default profile, to complete the registration transaction. The SIP phone activates its default profile, and internally stores its ERL information for use in the event that a 911 call is placed. Once the default registration is successful the SIP phone may receive dial-tone, indicating that it has achieved the state of emergency services readiness. Note that any subsequent, user-specific registrations will not invalidate the ERL information received by the phone during default registration. For example, a specific user may register with a personal profile at the phone without affecting the default registration state or default profile of the phone.

[0079] Figure 6 is a call flow showing the initialization procedure. In this example, the SIP phone sends a DHCP request (step 601) to obtain an initial IP address (step 601A). Then phone 108 sends a download request for a boot image (step 602). The phone receives a software image (step 602A), and a VLAN tag, and issues a second DHCP request using the VLAN tag (step 603). The phone may then register with the network (step 604), which in this case uses SIP signaling and a SIP proxy. The SIP proxy queries the location server (step 605), and upon receiving the response, sends the SIP OK message containing the ERL record along with the default profile (step 606), preferably as a textual description in the body of the SIP OK message.

[0080] Figure 6 thus illustrates how voice traffic may be kept on a specific VLAN within a local IP network. In

addition, an optional action (step 607) is shown in which the PSTN gateway provides local backup storage of the phones ERL information. It should be understood that the exact steps, as well as their sequence, are illustrative, and alternative call flows may be used.

4. 911 Call Processing

[0081] With reference to Figure 7, when a 911 call is placed from a registered SIP phone 108 (default or user-specific registration), the SIP phone 108 user agent application will retrieve the stored ERL information and formulate a SIP INVITE message 701 containing the ERL information for transmission to the PSTN gateway 208. The ERL information may be included in an associated SDP, but other methods of inclusion of the ERL data in the INVITE message 701 are possible. In one embodiment, the INVITE message 701 is sent directly to the PSTN gateway 208; i.e., it is not directed to the SIP Proxy 216. The phone 108 then sends a SIP NOTIFY directly to the Local Security station 218.

[0082] Upon receiving the SIP INVITE message 701, the PSTN gateway 208 places an outbound call 701A on the appropriate PSTN interface. The PSTN signaling in this example is based on SS7/ISUP, but other signaling could be used, for example PRI. Note that PSTN signaling elements for handling SS7/ISUP are not shown in Figure 7. The call may be to the local CO switch, which will direct the call to a 911 tandem switch for processing. Alternatively, the PSTN gateway 208 may have a specific interface for 911 calls. Either way, the gateway 208 will examine the Service Description Protocol (SDP) message (or other appropriate message elements) in the INVITE message 701 in order to determine the ERL. The SDP preferably includes the ERL record 305, or may include only an associated ERL ID 308, or one or more assigned ELINs from the list of ELINs 314. It will then examine the list of (possibly multiple) ELINs, and select one that does *not* match any that may already be included in its list of in-use ELINs. The selected ELIN is used to set the ANI in the outbound call 701A. The ELIN will then be recorded (possibly along with other ELINs), effectively marking it as in-use for any subsequent 911 calls from the same ERL. Along with the ELIN, the list may also contain additional identifying information about the location of the calling station; for example, the phone's IP address and the ERL identifier.

[0083] Once the call is placed to the PSTN, the gateway 208 will send a SIP NOTIFY message 704 to the Local Security station 218 with the status of the call. The gateway 208 will also generate CDRs (Call Detail Records) at various stages of each 911 call episode, and send them (706) to the Accounting Server 220; for example, when the call is placed to the PSTN, when the call terminates, etc.

[0084] For the duration of the call, the PSTN gateway 208 must be able to map any inbound call from the PSAP to the assigned ELIN to the original calling station. However, the gateway 208 must block any other calls inbound to the assigned ELIN.

[0085] The Local Security station 218 preferably includes an application that correlates SIP NOTIFYs 702 for 911 calls from SIP phones with SIP NOTIFYs 704 from the PSTN gateway 208. This will help insure reliability of the system, since the security station can be made to expect a notification from the gateway 208 that the call has been placed. If such notification is not received, the security station can be alerted, and the monitoring personnel can take appropriate backup action. In a duplicate action with the gateway 208, the Local Security station will also generate CDRs 705 at various stages of each 911 call episode, and send them to the Accounting Server 220.

[0086] The Accounting Server 220 will correlate and merge CDRs on each 911 call. They will be available for viewing and analysis at a later time, as well as documenting the call.

[0087] Once the call has been handled and terminated normally (i.e., the emergency situation is known to have been handled and cleared by the PSAP), call teardown proceeds as usual. When complete, the call status is cleared from all the relevant database elements, and the list of in-use ELINs at the PSTN gateway 208 is cleared of the associated call entry. If a particular call is terminated, but there is no clear indication that the emergency situation has been resolved, then the in-use status of the associated ELIN is maintained, as is the list at the gateway 208. After a configurable time limit, if no further information is received regarding the call, it is assumed to be resolved, and the ELIN is freed up and the list is cleared of that entry. All call status changes during the call, including termination, will cause the gateway to issue SIP NOTIFY messages to the Local Security station. In addition, some or all of the same status changes will cause the gateway 208 to generate related CDRs to the Accounting Server 220.

[0088] While a 911 call is active, the assigned ELIN is marked as in-use, by virtue of its presence in the PSTN gateway's 208 list. Any subsequent 911 calls from the same ERL while the ELIN is in use should be assigned a different ELIN for that ERL. For example, the gateway 208 may compare the list of ELINs in a SIP INVITE with the list of ELINs in its list to make this determination. However, depending upon the number or ELINs per ERL, there could arise a circumstance in which a 911 call is made from an ERL when all ELINs for that ERL are active (in-use). In this case, the PSTN gateway 208 preferably employs an algorithm to select which of the in-use ELINs for the particular ERL should be re-assigned to the new 911 call. For example, the ELIN which has been in-use for the longest time could be assigned to the new call. Note that this will invalidate the previous mapping of the ELIN to the original calling station 108. However, the relevant call information, even if it includes a multiply-assigned ELIN, can be maintained at the gateway 208 and/or the security stations for the duration

of the calls.

[0089] Note that once a call is established from a calling station 108 to a PSAP, it must not be disrupted by otherwise normal call signaling events. For example, the calling station 108 should not receive any call-waiting messages, or other advanced calling feature signals. This can be achieved with the SIP phone 108 simply by having the phone 108 use only its default profile once a 911 call is placed from it, and signaling the SIP Proxy 216 to block any inbound signaling to the phone 108. Alternatively, if there is an active personal registration (and personal profile) at a SIP phone 108 when a 911 call is placed, the phone 108 may automatically de-register that user from the phone 108. This has the effect of blocking any signaling to the user at that specific phone 108, since the SIP Proxy 216 would no longer see the user as reachable at the phone 108. Note that calls to that user could still be placed to any other SIP user agents at which he/she is registered. Again, there may be other ways to accomplish the non-disruption feature.

[0090] The phone's user agent application may also ensure that, once connected to the PSAP, the call cannot be released by the caller. For example, once a 911 call is active, the user agent application can simply decline to send a SIP BYE message if the user hangs up the phone 108. In addition or instead, the phone 108 may automatically activate its speaker and/or microphone if the user hangs up. This way, the PSAP could maintain a monitor at the phone's location, even if the user does not participate further in the call. Such a mode of operation could be advantageous, for example, in an intrusion situation.

Location Verification Management

[0091] Location verification management includes the methods, processes, and triggers used to discover location information for each calling station and ERL; populate the information elements of the location server database; and periodically check and verify the validity of database information, perform any required updates, and generate any alarms or alerts.

These are covered in following subsections.

1. Network Topology Considerations

[0092] One challenge in devising a location management strategy is that network topologies can differ from LAN to LAN, and enterprise to enterprise. In the context of location determination of a specific IP client device (with one physical interface) in a wireline network, an important piece of information is the location of the first managed switch that provides the (layer 2/3) entry point into the network. Here, the term "first" refers to the phone's perspective, looking toward the network. The term "managed" refers to a switch that is maintained as part of the managed infrastructure of a local network, e.g., by an enterprise's IT department. It is used to distinguish from an unmanaged switch, such as a desktop switch that may be connected to the network, but deployed outside the boundary of the managed infrastructure. Note that an unmanaged switch may still be discoverable by the network management system of the managed infrastructure, but critical attributes such as location might not be available or reliable.

[0093] The switch port on the first managed switch provides the most specific location information available, with respect to the managed infrastructure. The infrastructure may be configured to provide a unique switch port to individual locations, such as offices or cubicles. In this case, the identity of the managed switch port also specifies the location of the managed physical connection point. Alternatively, the configuration could be set up to provide area-wide, shared access to all or some of the managed switch ports, for example, by locating managed hubs between the shared switch ports and available connection points distributed across several offices or cubicles. In this case, the identity of the managed switch port specifies only the area served, but cannot distinguish between individual connection points. The precision of the location in the former case would likely be greater than that in the latter case (though not necessarily).

[0094] If the first managed switch port is also the first port to which a client device is connected (i.e., there are no unmanaged switches in between), then it provides the most specific location information for that client, with respect to the managed infrastructure, and with a precision corresponding to the sharing configuration of the port. For example, if a managed switch port serves a single office, then a client device connected to that port would be known to be connected in the corresponding office. Note that this does not preclude the possibility of using a very long Ethernet cable for the connection, thereby effectively decreasing the precision of the location information. If instead, a managed switch port serves a cluster of cubicles, then a client device connected to that switch port would be known to be connected in one of cubicles in the cluster. Again, non-switched extensions (e.g., hubs) could decrease the effective precision of the location information.

[0095] If a client device is connected to the first managed switch port via an unmanaged switch (e.g., an intervening desktop switch), then the precision of the location of the client with respect to the managed infrastructure is effectively decreased, in a similar manner to a non-switched extension. However, there are two potential differences: 1) the network management system 214 may be able to detect the presence of the unmanaged switch; and 2) such a switch could provide unmanaged bridging of multiple subnets, which could be problematic from the point of view of client location determination (particularly if the client device has more than one physical interface). As is discussed in the next subsection, management of switch ports may include the ability

to discover unmanaged switches, and detect if they introduce any problematic topologies.

2. Switch Port Management

[0096] Switch port management refers to establishing and maintaining identifying information about the managed switch ports that are configured for first-port access for client devices. This information should be sufficient to specify the location of a connected client, at least to the precision supported by the port-sharing configuration.

[0097] When a network is set up, a new switch installed, or an existing switch relocated, this information must be updated. Assuming that the network management system 214 can discover the network topology, any updates to the location information must be validated against the port-to-port and/or switch-to-switch connections determined by the topology. This is discussed in the previous section under "System Configuration."

[0098] Switch port management also includes discovery of unmanaged switches, if possible. While location information for such devices may not be reliable, their presence in the path between client devices and managed switches may be detectable. Further, any unmanaged switch that provides bridging between managed switch ports or between IP subnets must be flagged, if the bridging topology can be discovered. If such an unmanaged switch is determined to be the first switch port connection for an IP calling station (SIP phone), then an alert can be generated to the network management system 214, allowing appropriate action to be taken according to local policy.

[0099] The identifying information in a switch configured to provide first switch port access could include: the IP address of the switch; the Port number on the switch; the Switch location; the most precise location associated with port number (e.g., office, cubicle, cluster, floor, etc.); managed physical connection points assigned to the switch port.

3. Automatic Discovery

[0100] Automatic discovery encompasses three processes:

1. Discovery of network topology, including managed and unmanaged switches (if possible);
2. Discovery of calling stations (SIP phones); and
3. Generation and population of the Location Server database.

The first process is generally a capability provided by the network management system 214. Suitable network management tools and features are available on platforms such as HP Openview, available from Hewlett Packard. Alternatively, new software layers (e.g., middleware) may be used to provide this service to the Location server via an API, or similar programmable interface. The software preferably utilizes the SNMP protocol to obtain routing tables from routers and bridging tables from switches to identify an IP address with a known port and physical location.

Processes (2) and (3) preferably run on the Location server. They access the interface to the network management system 214 as needed. For each calling station, the second process combines the switch port identification information with any location information that may be supplied by the calling station, in order to determine the most accurate location of the calling station, as well as its ERL. It is possible for the result this process to indicate an inconsistency in the one or more of the reported configurations. For example, if the physical mapping of switch ports to physical connections is modified, but the change is not properly updated in the provisioning system, then the NMS discovery could disagree with the recorded mappings. If the change is made while registered SIP phones are connected to the switch, then the phones' internally stored location information will disagree with that reported from an NMS discovery procedure.

The respective weightings given to the phone location information and the switch port location information depends upon the trigger that invokes the discovery process. For example, if a SIP registration is the trigger, then the switch port information is taken as correct. However, if periodic verification check is the trigger, and the phone has maintained continuous registration, then the phone location may be selected over that of the switch port (assuming disagreement).

The third process uses input from the second process to generate the Location Server database records.

4. Triggers and Actions

[0101] Triggers are the events that cause the automatic discovery processes to run. Actions are additional tasks and/or functions that are associated with processes. The trigger for process (1) is a request for information from either of the other two processes. That is, when either process of (2) or (3) executes, they invoke process (1) in order to get the required input. It is up to process (1) to decide how to carry out the request. For example, whether restricted or full topology discovery is required to fulfill the request; or whether current topology information is applicable to a request, without actually running any discovery steps.

[0102] The triggers for process (2) are: SIP phone registration; Periodic, automatic verification check.

[0103] The triggers for process (3) are: System turn-up; SIP phone registration; Periodic, automatic verification check.

Claims

1. A method of configuring a packet based phone for initiating an emergency call in a packet based network, comprising:

   receiving an ERL record at a packet based phone, said ERL record being associated with the phone's emergency response location; and transmitting from the packet-based phone at least a portion of the ERL record as part of an emergency call setup process.

2. The method of claim 1, wherein the packet based network is an Internet Protocol network.

3. The method of claim 1, wherein the ERL record includes one or more ELINs, and wherein the phone transmits at least one of the ELINs.

4. The method of claim 1, wherein the ERL record includes one or more ELINs, and wherein the phone transmits at least one of the ELINs using the Session Initiation Protocol.

5. The method of claim 1, wherein the packet-based phone uses the Session Initiation Protocol.

6. The method of claim 1, wherein the ERL record includes one or more ELINs, and wherein the phone transmits at least one of the ELINs in an SDP contained in a SIP INVITE message.

7. The method of claim 1, wherein the phone transmits at least a portion of the ERL record to a PSTN gateway device.

8. The method of claim 7, wherein the phone selects the PSTN gateway device according information in the ERL record.

9. The method of claim 7, wherein the portion of the ERL record comprises an ERL ID, and the PSTN gateway device inserts a corresponding ELIN into the caller identification portion of an outgoing emergency services call.

10. The method of claim 7, wherein the portion of the ERL record comprises one or more ELINs, and the PSTN gateway device inserts one of the ELINs into the caller identification portion of an outgoing emergency services call.

11. The method of claim 7, wherein the PSTN gateway device maintains a list of ELINs associated with a caller identification portion of active outgoing emergency services calls, and wherein the PSTN gateway device selects ELINs for new outgoing emergency services calls.

12. The method of claim 1, wherein the phone transmits at least a portion of the ERL record to a call signaling device.

13. The method of claim 12, wherein the portion of the ERL record comprises at least an ERL ID, and the call signaling device selects a corresponding ELIN.

14. The method of claim 13, wherein the signaling device transmits a request to a PSTN gateway to make an outgoing emergency services call using an ELIN inserted into a caller identification portion of the outgoing call.

15. The method of claim 12, wherein the portion of the ERL record comprises one or more ELINs, and the call signaling device selects an ELIN.

16. The method of claim 15, wherein the signaling device transmits a request to a PSTN gateway to make an outgoing emergency services call using an ELIN inserted into a caller identification portion of the outgoing call.

17. The method of claim 12, wherein the call signaling device maintains a list of ELINs assigned to a caller identification portion of active outgoing emergency services calls, and wherein the call signaling device selects ELINs for new outgoing emergency services calls.

18. The method of claim 12, wherein the call signaling device is a SIP Proxy server.

19. The method of claim 12, wherein the request to the PSTN gateway is a SIP INVITE message.

20. The method of claim 1 further comprising the step of determining the emergency response location of the phone based in part on an IP address of the phone.

21. The method of claim 1 further comprising the step of determining the emergency response location of the phone based in part on a MAC address of the phone.

22. The method of claim 1 further comprising the step of determining the emergency response location of the phone based in part on a serial number of the phone.

23. The method of claim 1, further comprising the step of transmitting an address of a PSTN gateway device for use during an emergency call.

24. The method of claim 1, further comprising transmitting a first notification message to a monitoring station when an emergency call is placed by a phone.

25. The method of claim 24, wherein the monitoring station ensures that a corresponding notification message is received from a PSTN gateway.

26. The method of claim 25, wherein the monitoring station issues an alarm if it fails to receive the first notification message from the phone and the corresponding notification message from the PSTN gateway.

27. The method of claim 25, wherein a SIP NOTIFY message is used to send the notification from the PSTN gateway to the monitoring station.

28. The method of claim 24, wherein a SIP NOTIFY message is used to send the notification from the phone to the monitoring station.

29. A method of configuring a packet based phone for initiating an emergency call in a packet based network, comprising:

determining an ERL of the packet based phone; and
transmitting a corresponding ERL record to the packet based phone, said ERL record including parameters enabling the packet based phone to initiate an emergency services call.

30. The method of claim 29, wherein the packet based network is an Internet Protocol network.

31. The method of claim 29, wherein the packet based phone uses SIP.

32. The method of claim 29, wherein the ERL record is transmitted to the packet based phone using SIP.

33. The method of claim 29, wherein the ERL record is transmitted to the packet based phone using a SIP OK message, issued in response to a SIP REGISTER message from the packet based phone to a SIP network.

34. The method of claim 29, wherein the ERL record is transmitted to the packet based phone as a textual message in the body of a SIP OK message, issued in response to a SIP REGISTER message from the packet based phone to a SIP network.

35. The method of claim 29, wherein the step of determining an ERL further comprises receiving an IP address of the phone. and determining the ERL in response to the received IP address.

36. The method of claim 35, wherein the step of determining the ERL in response to the received IP address comprises querying a network management system.

37. The method of claim 29, wherein the step of determining an ERL further comprises receiving a MAC address of the phone, and determining the ERL in response to the received MAC address.

38. The method of claim 37, wherein determining the ERL in response to the received MAC address comprises querying a network management system.

39. The method of claim 29, wherein the step of determining an ERL further comprises receiving a serial number of the phone, and determining the ERL in response to the received serial number.

40. The method of claim 39, wherein determining the ERL in response to the received serial number comprises querying a network management system.

41. A method of configuring a packet based phone for initiating an emergency call in a packet based network, comprising:

receiving an ERL record at a packet based phone, the ERL record containing at least one or more ELINs and address information for contacting one or more emergency PSTN gateways;
responsively storing at least the information in the ERL record required to initiate an emergency services call.

42. The method of claim 41 wherein the packet based network is an Internet Protocol network.

43. The method of claim 41, wherein the packet based phone uses SIP.

44. The method of claim 41, wherein the ERL record is received at the phone using SIP.

45. The method of claim 41, wherein the ERL record is received at the phone using a SIP OK message, received in response to a SIP REGISTER message from the packet based phone to a SIP network.

46. The method of claim 41, wherein the ERL record is received at the phone as a textual message in the body of a SIP OK message, issued in response to a SIP REGISTER message from the phone to a SIP network.

47. The method of claim 41, further comprising the step of deregistering a user profile with a SIP proxy in

the event a user dials an emergency services number.

48. The method of claim 41, wherein, responsive to the event of the packet based phone receiving signaling for an incoming call while an emergency services call placed by the phone is still active, preventing the incoming call from interrupting the active emergency services call.

49. The method of claim 41, wherein, responsive to the event of the user attempting to disconnect an emergency services call, declining to issue the requisite disconnect signaling, and instead entering speaker phone mode.

50. A method of configuring a packet based phone for initiating an emergency call in a packet based network, comprising:

establishing a plurality of ERL records, each of the ERL records containing at least the following information: ERL ID; textual location description; managed network connection points associated with the ERL; ELINs associated with the ERL; PSTN gateways associated with the ERL;
establishing a plurality of phone location information records, each of the phone location records containing at least the following information: a IP address of the phone; a MAC address of the phone; a serial number of the phone; an ERL ID associated with the phone; a managed network connection point associated with the phone; an ELIN associated with the phone; one or more PSTN gateways associated with the phone; and
transmitting to a phone at least part of the ERL record including parameters enabling the packet based phone to initiate an emergency services call.

51. The method of claim 50, wherein the packet based network is an Internet Protocol network.

52. The method of claim 50, wherein the packet based phone uses SIP.

53. The method of claim 50, wherein the plurality of ERL records is maintained in a centralized database.

54. The method of claim 50, wherein the plurality of phone location information records is maintained in a centralized database.

55. The method of claim 50, wherein the at least part of the ERL record transmitted to the packet based phone is identified according to the managed network connection point of the phone.

56. The method of claim 55, wherein the managed network connection point of the phone is determined by querying a network management system with the IP address of the packet based phone.

57. The method of claim 55, wherein the managed network connection point of the phone is determined by querying a network management system with the MAC address of the packet based phone.

58. The method of claim 55, wherein the managed network connection point of the phone is determined by querying a network management system with the serial number of the packet based phone.

59. The method of claim 50, wherein the at least part of the ERL record is transmitted to a packet based phone responsive to a request containing the IP address of the packet based phone.

60. The method of claim 50, wherein the at least part of the ERL record is transmitted to a packet based phone responsive to a request containing the MAC address of the packet based phone.

61. The method of claim 50, wherein the at least part of the ERL record is transmitted to a phone responsive to a request containing the serial number of the packet based phone.

62. The method of claim 50, wherein each of the plurality of phone location information records is associated with a distinct packet based phone, each of the distinct packet based phones being connected to the network at a managed network connection point.

63. The method of claim 50, further comprising the steps of:

receiving a registration request containing identifying information of a packet based phone;
determining that a corresponding phone location information record for the packet based phone does not exist; and
creating a new phone location information record.

64. The method of claim 63, wherein the identifying information comprises an IP address.

65. The method of claim 63, wherein the identifying information comprises a MAC address.

66. The method of claim 63, wherein the identifying in-

formation comprises a serial number.

67. The method of claim 50, further comprising the step of verifying the accuracy of each of the plurality of phone location information records.

68. The method of claim 67 wherein the accuracy is verified by the steps of:

sending a network management query requesting the identity of the managed network connection point of the individual phone using one of the IP address and the MAC address of the phone, as stored in the associated phone location information record, and receiving a network management query response;
sending a phone query to the packet based phone requesting its stored ERL record, and receiving a phone query response;
comparing the managed network connection point reported in the network management query response with the identity of the managed network connection point reported in the phone query response;
comparing the identity of the managed network connection point reported in the network management query response with the identity of the managed network connection point reported in the phone query response; and
comparing the identity of the managed network connection point reported in the phone query response with the identity of the managed network connection point reported in the network management query response;
issuing a software alert if one of the above comparisons are not the same.

69. The method of claim 68 further comprising a programmable schedule upon which the said sequential steps are initiated for each existing individual phone location information record.

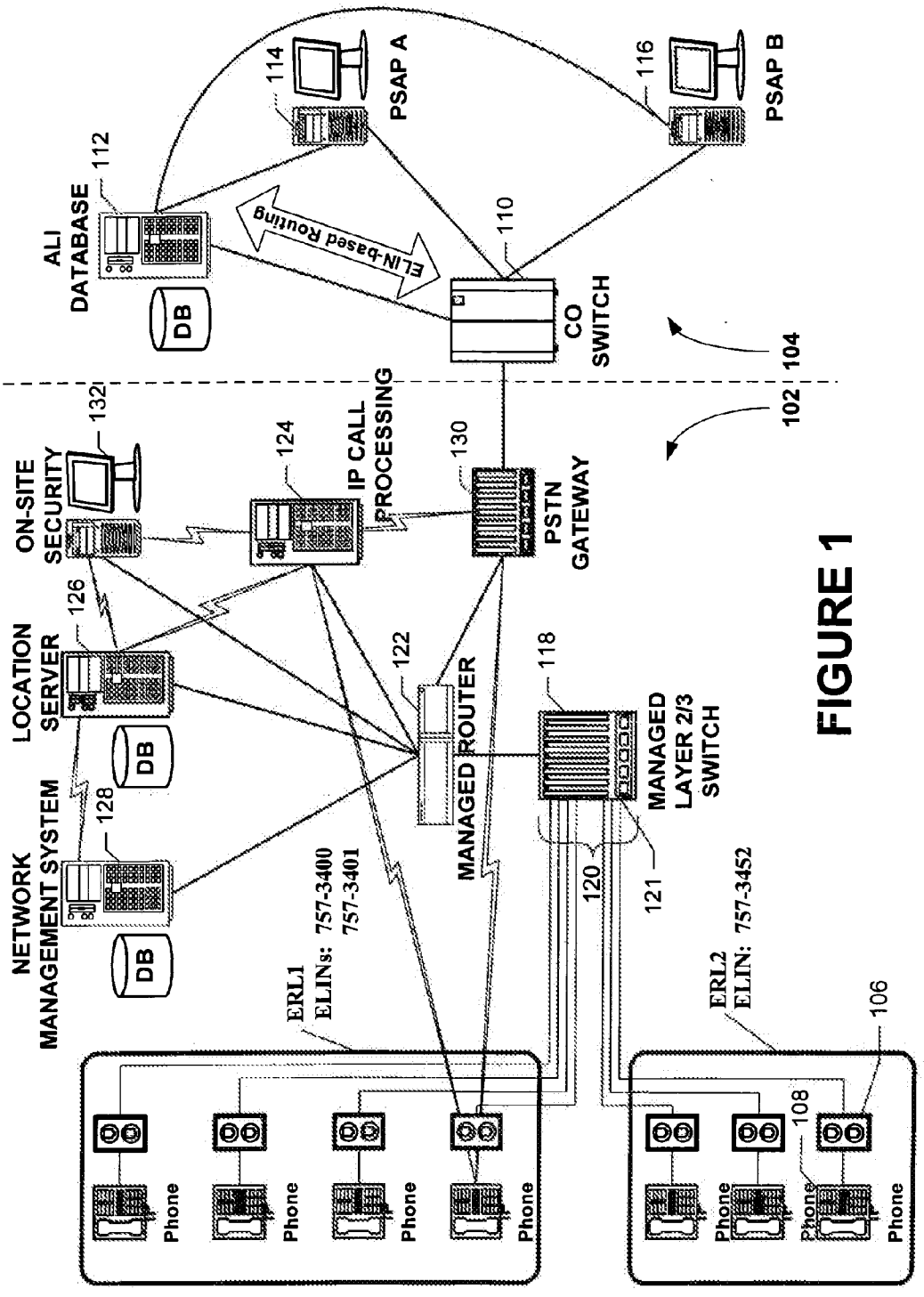


FIGURE 1

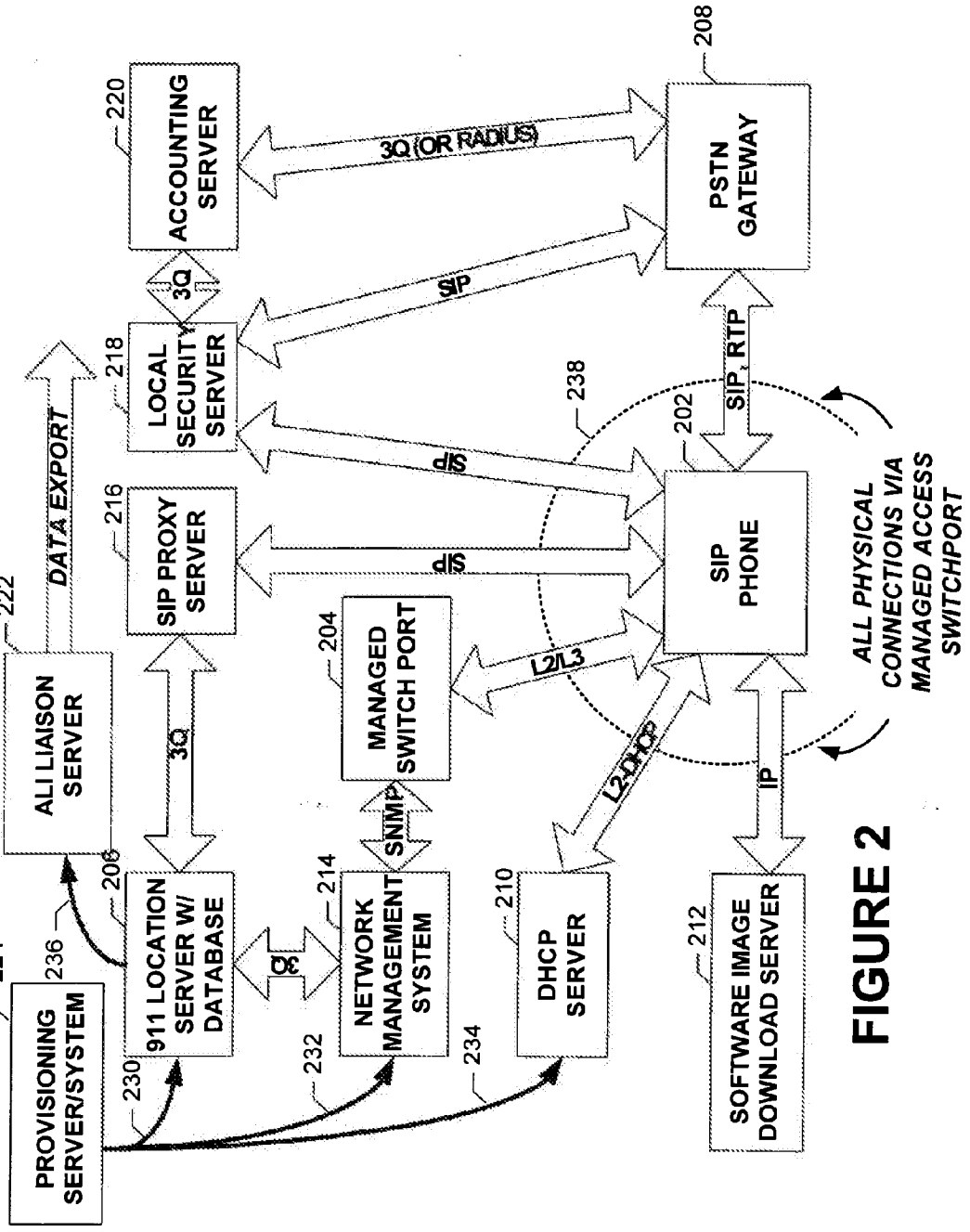


FIGURE 2

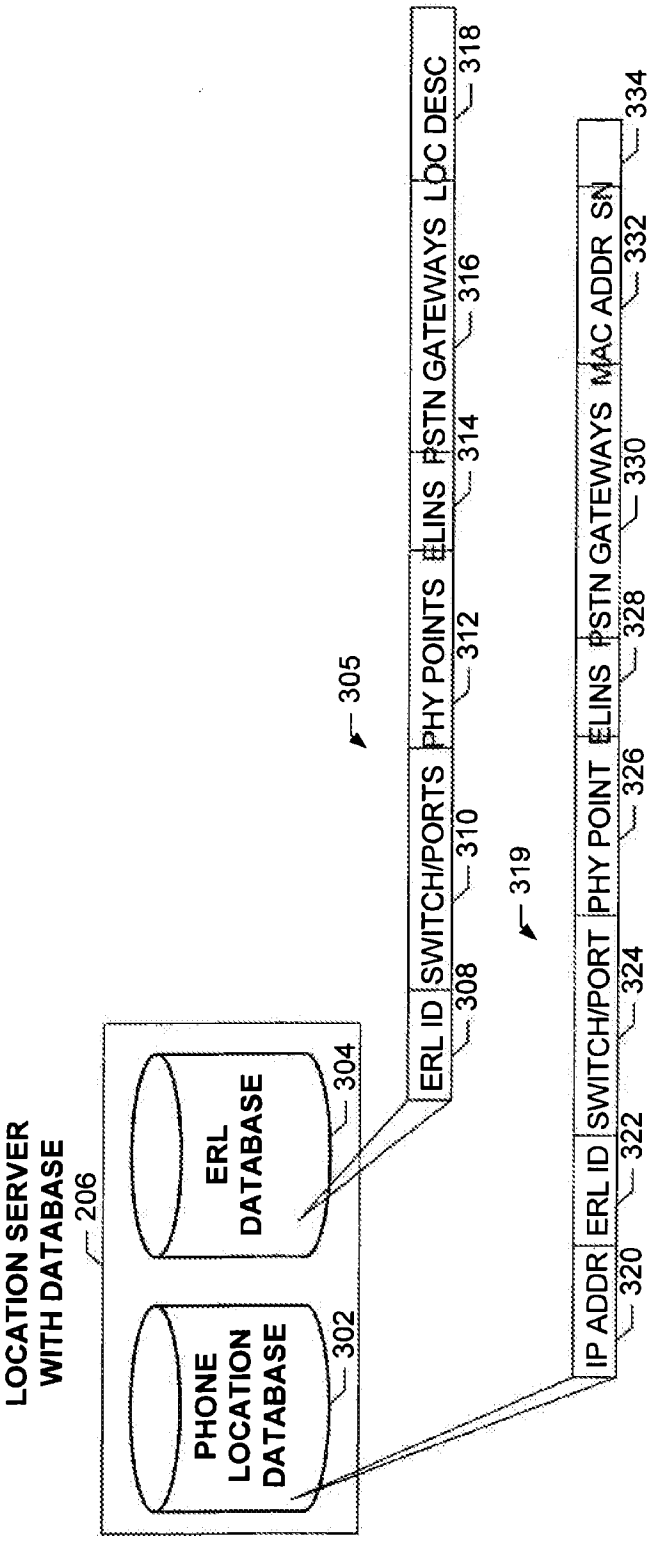


FIGURE 3

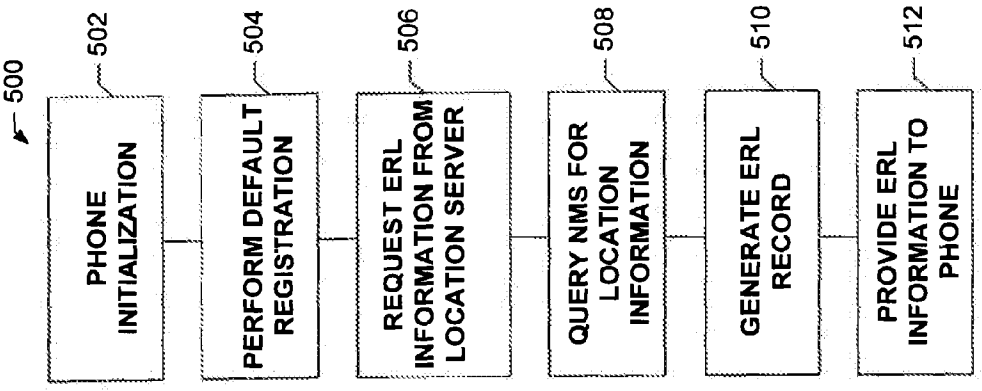


FIGURE 5

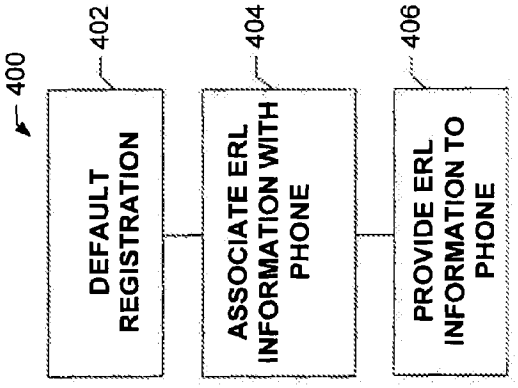


FIGURE 4

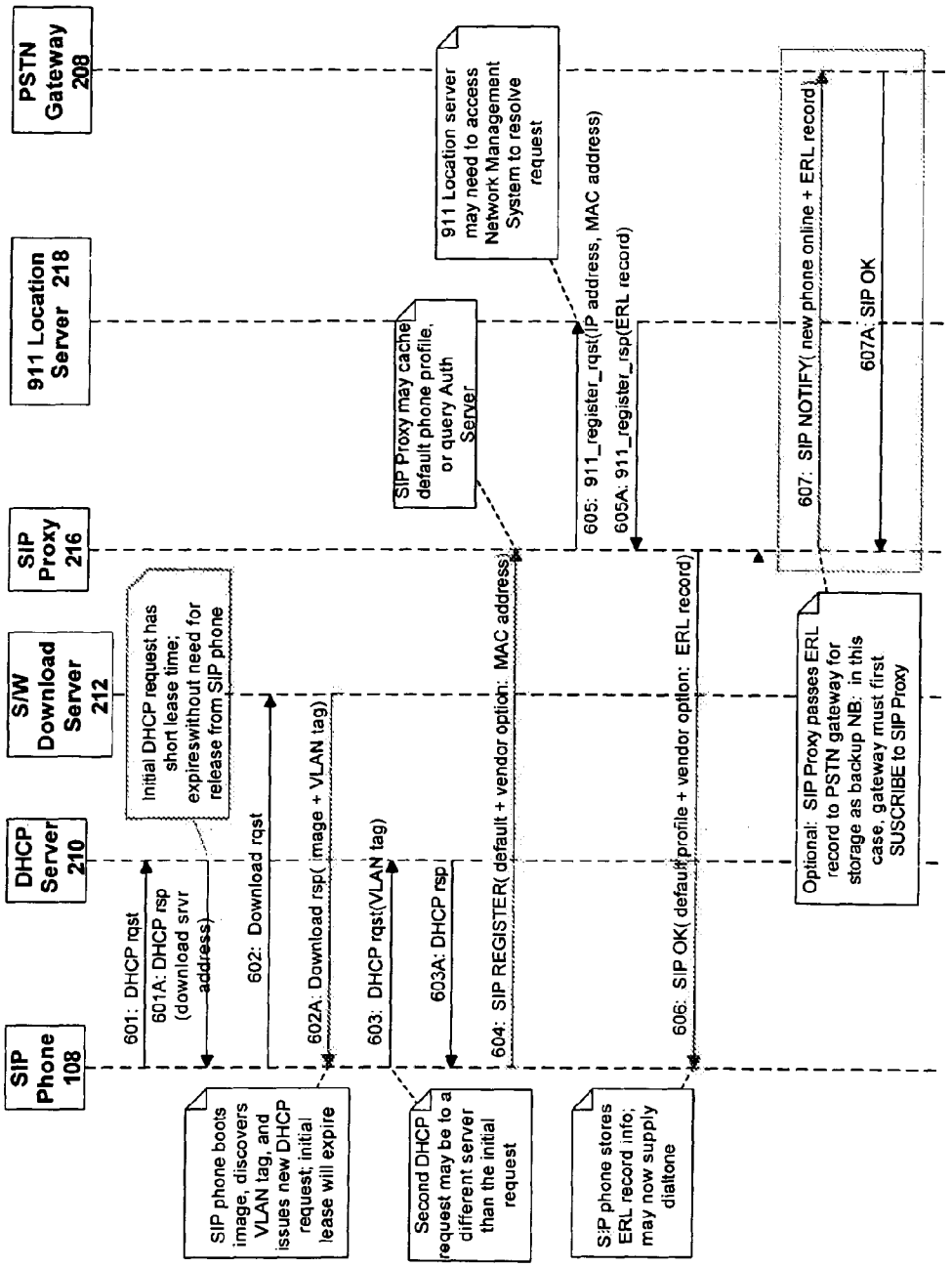


FIGURE 6

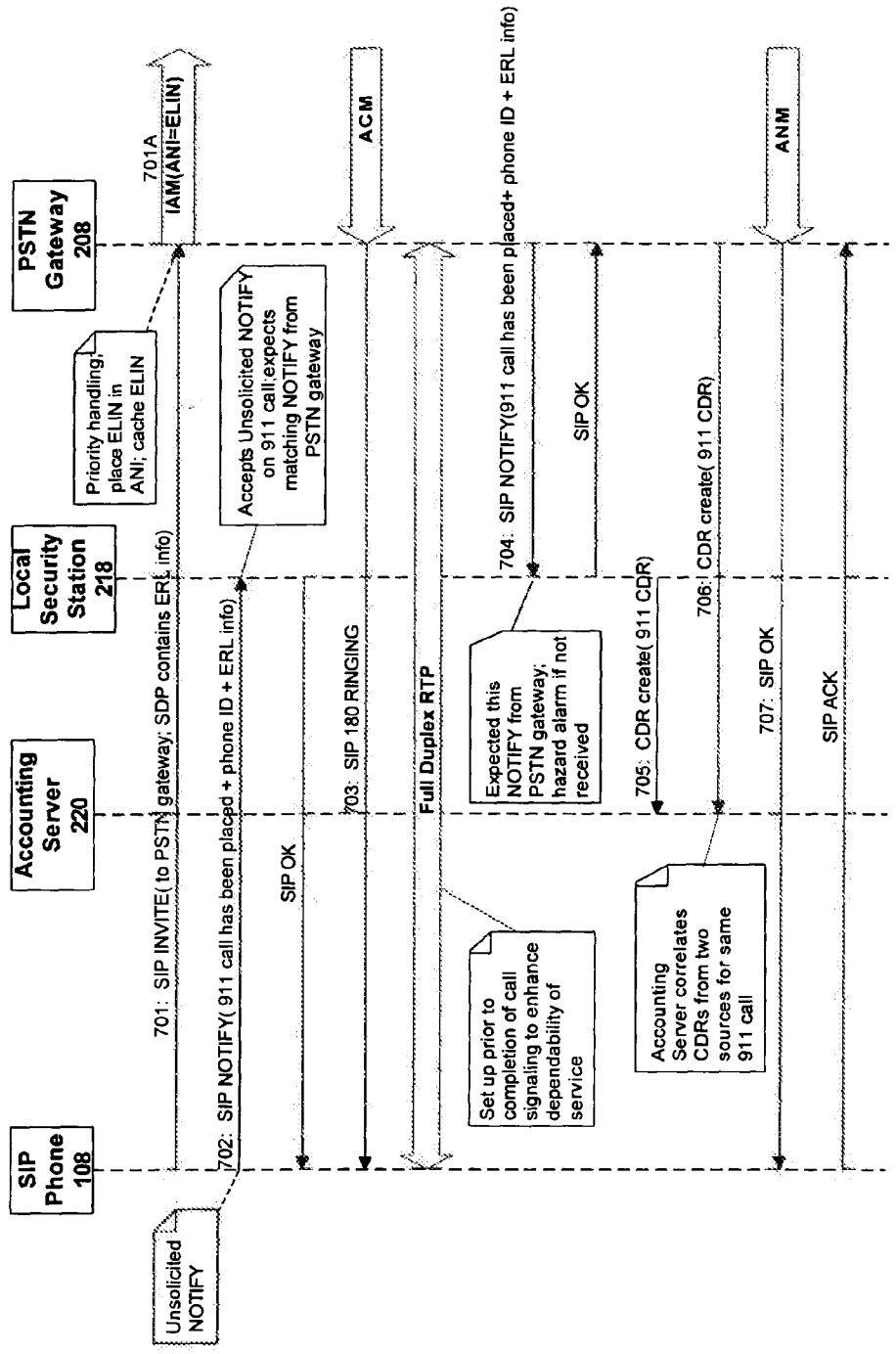


FIGURE 7

Espacenet

Bibliographic data: EP1362456 (A4) — 2005-05-25

SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS

Inventor(s): PYKE CRAIK R [CA]; HERN WILLIAM [GB]; THOMPSON ROGER L [US]; CARON SERGE S [CA]; MOUNJI HALIMA H [CA]; EWOTI CHARLES B [DE]; GOERENS MICHAEL [DE]; STRENG PETE J [CA]; GOERTZEN CHRISTOPHER J [CA]; KITTLITZ CHRISTIAN [CA]; TAYLOR RICHARD C [CA]; WELHAM MICHAEL [DE] + (PYKE, CRAIK, R, ; HERN, WILLIAM, ; THOMPSON, ROGER, L, ; CARON, SERGE, S, ; MOUNJI, HALIMA, H, ; EWOTI, CHARLES, B, ; GOERENS, MICHAEL, ; STRENG, PETE, J, ; GOERTZEN, CHRISTOPHER, J, ; KITTLITZ, CHRISTIAN, ; TAYLOR, RICHARD, C, ; WELHAM, MICHAEL)

Applicant(s): NORTEL NETWORKS LTD [CA] + (NORTEL NETWORKS LIMITED)

Classification: **- international:** ***H04L12/26; H04L29/06; H04M3/22; H04M7/00;*** (IPC1-7): H04L12/56

- cooperative: **H04L29/06**; **H04L63/30**; **H04L69/22**; **H04M3/2281**; **H04M7/006**; H04Q2213/13034; H04Q2213/13196; H04Q2213/13372; H04Q2213/13389

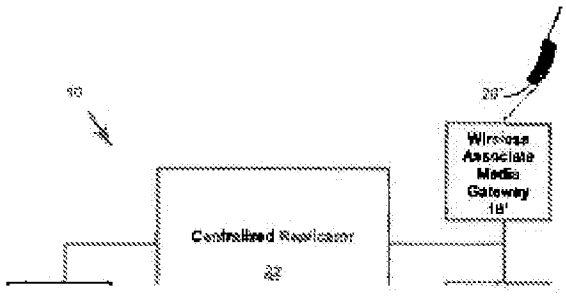
Application number: EP20010273516 20011009

Priority number(s): WO2001US31548 20011009 ; US20000239048P 20001010

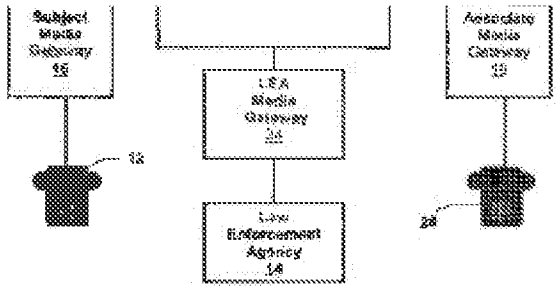
Also published as: EP1362456 (A2) EP1362456 (B1) WO02082782 (A2) WO02082782 (A3) US2003179747 (A1) DE60133316 (T2) CA2437275 (A1) AU2001297701 (A1) less

Abstract not available for EP1362456 (A4)
Abstract of corresponding document: WO02082782 (A2)

A system and method for intercepting a telecommunication signal are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload and



PETITIONER APPLE INC. EX. 1004-700



adding a second header to replicated payload and directing the replicated payload to the address associated with the second.;A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

European Patent Office

Application Number
EP 01 27 3516

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1-30

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 01 27 3516

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-30

Method and system for intercepting, redirecting a packet in a packet telecommunications network by removing the header of the packet, duplicating the payload of the packet, adding a new header and transmitting the packet to the address associated to the new header.

---

2. claims: 31-33

A method of monitoring or redirecting a telecommunication signal to or from a subject being monitored from or to an associate, the method comprising the steps of:
determining that a telecommunication signal is subject to being monitored;
establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject;
establishing a connection between the second gateway and a second termination point representing the first gateway; and
establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connected directly.

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 01 27 3516

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 99/17499 A (NOKIA TELECOMMUNICATIONS OY ; HAUMONT SERGE (FI)) 8 April 1999 (1999-04-08) * abstract * * page 1, lines 19-34 * * page 4, line 33 - page 5, line 25 * * page 10, line 11 - page 13, line 24; claims 1-4,7-10 *	1-30	H04L12/56
X	WO 00/56029 A (NOKIA NETWORKS OY ; ELORANTA JAANA (FI); JOKINEN HANNU T (FI); LUMME M) 21 September 2000 (2000-09-21) * abstract * * page 2, lines 9-31 * * page 9, lines 6-24 * * page 23, lines 15-26 * * page 26, lines 14-34 *	1-30	
X	WO 00/42742 A (NOKIA NETWORKS OY ; HIPPELAEINEN LASSI (FI)) 20 July 2000 (2000-07-20) * abstract * * page 4, lines 4-17 * * page 6, line 6 - page 7, line 7 * * page 8, lines 4-9 * * page 8, line 28 - page 9, line 2 * * page 10, line 8 - page 11, line 21 * * page 13, lines 4-9 * * page 17, lines 5-24 *	1-30	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04M H04L H04Q
X	"UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS); 3G SECURITY; LAWFUL INTERCEPTION ARCHITECTURE AND FUNCTIONS (3G TS 33.107 VERSION 3.0.0 RELEASE 1999)" ETSI TS 133 107 V3.0.0, XX, XX, January 2000 (2000-01), page 55, XP002214517 * page 24 - page 31 * * page 46 - page 52 *	1-30	

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	5 January 2005	Le Bras, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

2

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 27 3516

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-01-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9917499 A	08-04-1999	FI 973806 A	27-03-1999
		AT 268964 T	15-06-2004
		AU 9351598 A	23-04-1999
		CA 2304172 A1	08-04-1999
		CN 1110171 C	28-05-2003
		DE 69824430 D1	15-07-2004
		EP 1018241 A2	12-07-2000
		WO 9917499 A2	08-04-1999
		HK 1031494 A1	31-10-2003
		JP 2001518744 T	16-10-2001
		TW 429710 B	11-04-2001
		US 6654589 B1	25-11-2003
WO 0056029 A	21-09-2000	WO 0056029 A1	21-09-2000
		AU 3517899 A	04-10-2000
		EP 1159817 A1	05-12-2001
		JP 2002539716 T	19-11-2002
		US 2002049913 A1	25-04-2002
WO 0042742 A	20-07-2000	WO 0042742 A1	20-07-2000
		AU 2617399 A	01-08-2000
		EP 1142218 A1	10-10-2001
		JP 2002535883 T	22-10-2002
		US 2002078384 A1	20-06-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 575 327 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
14.09.2005 Bulletin 2005/37

(51) Int Cl.[7]: **H04Q 7/38**

(21) Application number: **05251291.0**

(22) Date of filing: **03.03.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(30) Priority: **11.03.2004 US 798629**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

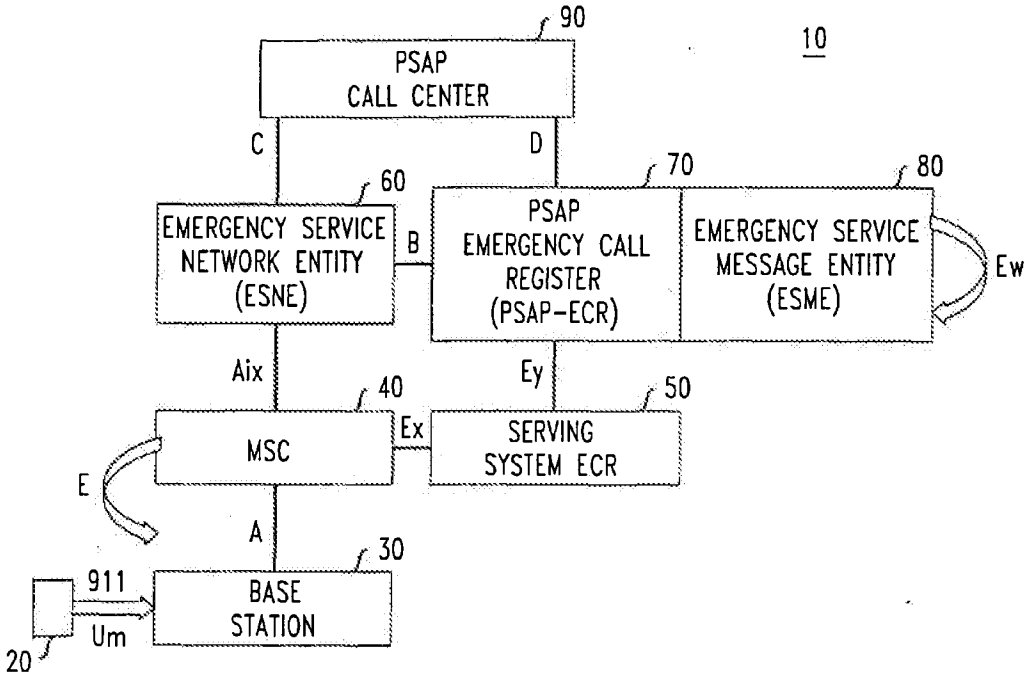
(72) Inventor: **Rollender, Douglas H.**
Bridgewater, NJ 08807 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway et al
Lucent Technologies NS UK Ltd
5 Mornington Road
Woodford Green
Essex, IG8 0TU (GB)

(54) A method of associating call back data with an emergency call to a call center

(57) A method of communication to at least one wireless unit originating an emergency call. The method includes the step of receiving at least one tag identifier in response to the emergency call originating from the at least one wireless unit. Once the tag identifier is received, a wireless call back number corresponding with the at least one tag identifier may be transmitted. A public service answering point emergency call register ("PSAP-ECR") may receive the at least one tag identifier and transmits the wireless call back number over a D interface.

FIG. 1



EP 1 575 327 A1

Description

BACKGROUND OF THE INVENTION

I. FIELD OF THE INVENTION

[0001] The present invention relates to telecommunications, and more particularly, to wireless communications.

II. DESCRIPTION OF THE RELATED ART

[0002] Emergency service calls in North America are originated by dialing "9-1-1." Other parts of the world may use some other abbreviated string of dialable digits, such as "6-1-1" in Mexico, for example. These abbreviated string of digits share the intent of simplify calling for help with an easy to remember number. These calls are routed to a local Public Service Answering Point Call Center ("PSAP-CC") to enable the initiation of an emergency response (e.g., police, fire department, road repair, and/or ambulance) while the caller is kept on the phone. If, however, the call is somehow disconnected or dropped before the emergency is completely reported or the responder arrives, the PSAP-CC may be required to call back the originator.

[0003] It should be noted that the record for a "9-1-1" call originated through a wired network may include Automatic Line Identification ("ALI") or the telephone number of the access line from which the call originated. The directory number ("DN") or telephone number of a wireless subscriber may not, however, be associated with a physical line or wireless unit. Instead, calls to a roaming wireless subscriber are routed to the wireless unit by way of the mobile station identification ("MSID"), as opposed to the mobile DN ("MDN"). Accordingly, performing an emergency call back to a wireless unit poses hurdles not encountered with landline devices, for example.

[0004] Typically, the MSID may be characterized as either a 10-digit mobile identification number ("MIN") or a 15-digit International Mobile Subscriber Identifier ("IMSI"). The IMSI may be programmed into a wireless unit or a Subscriber Identity Module ("SIM") card by the service provider with whom the wireless unit user has entered into a service agreement. Accordingly, the MSID may not necessarily be a dialable number.

[0005] The DN of a wireless unit is a dialable number. The DN is dialed by a caller and used to route a call through the network to the wireless subscriber's home system. At the subscriber's home system, the home location register ("HLR") contains the MSID associated with the subscriber's DN. The MSID, as opposed to the DN, may then be used to route the call through the network to the serving wireless system and page the subscriber. The subscriber's DN may be provided to the serving system from the SIM card through the wireless unit or by the home system to the serving system in a separate data file called the subscriber profile.

[0006] The rollout of systems employing a separate number for DN and MSID is a relatively recent occurrence for some wireless systems. Others have used this technique since their inception. Historically, the mobile identification number of a wireless unit was the same as the DN for some systems, particularly in systems supportive of TIA/EIA-41 standards, prior to implementing wireless number portability ("WNP") or thousands block number pooling ("TBNP") based on the Local Routing Number ("LRN") method and international roaming ("IR"). However, with WNP and TBNP, the MDN became "portable" or "poolable" from one service provider to another service provider. Since MSID may not be portable or poolable, the recipient service provider may assign a new MSID for a subscriber with a ported-in or pooled MDN.

[0007] International roaming has also forced the separation of MSID and MDN. While the MIN is a 10-digit number modeled after the North American Numbering Plan's 10-digit MDN, other nation's carriers using a different directory numbering plan may not allow their subscriber's DN to be equivalent to the internationally recognized MIN format. Another standard MSID is the IMSI. It may be used in TIA/EIA-41 and GSM systems around the world. IMSI is a 15-digit non-dialable number based on ITU-T Recommendation E.212, and therefore, may not serve as a 10-digit MDN.

[0008] Historically, when the MDN was the same as the MIN, the MIN would be delivered to a PSAP-CC and would be used as a call back number. With the separation of MIN and MDN as described above, it became necessary to deliver the MDN as a separate call back number to the PSAP-CC, as well as the caller's MSID. There are certain problems, however, associated with implementing this solution. One issue is that the serving system may not have the caller's MDN, only the MSID, to present to the PSAP-CC with the call. Some of the reasons for this relate to the way MSID-MDN separation has been implemented according to standards. Another reason is that the network interface used to deliver the call to the PSAP-CC may not have the capacity to signal both the DN and MSID or, in some cases, even a full DN.

[0009] An old serving TIA/EIA-41 system may not support WNP, TBNP or IR. This means that the older serving system may be expecting the MIN and the MDN to be the same. The older system would not even know to look for a separate MDN in the subscriber's service profile (e.g., keyed on MIN, not MDN). With this limitation, these subscribers may not be allowed to use basic services, but they must be allowed to call for emergency services. As a result, a roamer who dials "9-1-1" while on an old system will have his or her call delivered to the PSAP-CC with an MSID but no MDN. Accordingly, no call back is possible.

[0010] A newer serving system that is WNP and IR capable may not be able to deliver MDN to the PSAP-CC. This could happen if the calling wireless unit

is not registered with any service provider (e.g., there are mobile phones used for emergency calls only). These wireless units may be referred to as non-subscriber initialized ("NSI") phones. It is also possible for a subscriber to place an emergency call before the HLR has responded to the serving system with the subscriber's service profile containing the DN. Even if the PSAP-CC has been provided with a working DN for callback, the callback to the DN will not go through if the subscriber has call forwarding service for all inbound calls or if the subscriber has a limited, pre-paid service and there is no remaining balance available to pay for the inbound callback from the PSAP-CC. Further, if the callback number is to a visiting international roamer, the PSAP-CC may need to place an international call. Some PSAP-CC may not have the ability to callback an international number. There is also the risk of network congestion or delay in completing an international call which would be detrimental to handling an emergency in a timely manner. Some PSAP-CCs may not even be equipped to place any outbound calls through separate, outbound administrative lines.

[0011] The call back DN for an international roamer would require the PSAP-CC to place an international call to reach a subscriber in their local Emergency Service Zone ("ESZ"). This is not a practical, timely or sufficiently reliable solution for a PSAP-CC that normally does not place international calls and for applications that may require immediate call back information for emergency purposes. In addition, the entire international MDN (up to 15 digits including a country code) may not be presented to the PSAP-CC for call back if the PSAP-CC only supports 10 digits.

[0012] It is also possible that the calling wireless unit is not registered with any service provider. As a result, there may be no DN associated with the wireless unit or no permanent MSID encoded in the wireless unit - such wireless units are referred to as NSI mobile phones, for example. This could be because (a) the NSI phone was never intended to be registered (there are such phones to use for emergency calls only), (b) the phone is new and has not yet been initialized by a service provider, (c) the subscription has expired and the NSI phone is no longer registered with a service provider or (d) the SIM card is lost, stolen, or simply never been inserted or been removed either advertently or inadvertently.

[0013] Some wireless units also support a removable User Identity Module ("R-UIM") or Subscriber Identity Module ("SIM") that may contain the MSID and the DN. If the R-UIM or SIM are not in the phone, then it can still be used to place an emergency call. However, there is no DN or MSID known to the phone or the serving system to provide the PSAP-CC as a call back number.

[0014] Every MS contains a unique mobile equipment identification number ("MEIN") encoded in the phone by the manufacturer. The MEIN may be, for example, an electronic serial number ("ESN"), as used in ANSI/TIA/EIA-41 systems or an International Mobile Equipment Identity ("IMEI") used in GSM systems. The MEIN is independent of the MSID and DN. The MEIN is signaled over the air between the wireless unit and the base station of a wireless system with a call origination attempt or soon thereafter. For example, if not supplied with the call origination attempt, the MEIN may be requested by the serving system.

[0015] Current standards for wireless emergency services call for delivering "9-1-1 + the last seven digits of the MEIN" to the PSAP-CC as the form call back number when the directory number assigned to the wireless subscriber is not available. While this may serve to notify the PSAP-CC that no working callback number is available with the call, this "9-1-1 + the last seven digits of the MEIN (MEIN7)" does not uniquely identify the call (i.e., many emergency calls may be identified by the same "9-1-1+MEIN7) and is not routable through the network. This is attributable because to the "9-1-1 + the last seven digits of the MEID" does not contain a complete MEID, and therefore is not unique.

[0016] While the hereinabove approach provides the PSAP-CC some measure for performing an emergency call back of a wireless unit, several hurdles still exist. For example, the callback number for a wireless unit in certain circumstances may be nothing more than a dummy number with user location data. Consequently, a need exists for a method and system architecture for ensuring the PSAP-CC receives a real call back number for a wireless unit originating a "9-1-1" call.

SUMMARY OF THE INVENTION

[0017] The present invention provides for a method and system architecture for ensuring a real callback number may be provided for a wireless unit originating a "9-1-1" call. More particularly, the present invention enables a call center, such as a local Public Service Answering Point Call Center ("PSAP-CC"), to initiate a callback, irrespective of whether the originating "9-1-1" caller was placed over wireless or wireline communications infrastructure, based on at least one tag identifier. For the purposes of the present disclosure, a tag identifier may correspond with a name or label to uniquely associate signaling from different sources such as, for example, the association of a voice with associated data transmitted over a different channel or in a separate message. Consequently, the tag identifier may include one or more reference keys to a database, such as an emergency call register or an emergency service message entity, for example. The tag identifier(s), therefore, may correspond with an emergency service routing key, a local public safety number, a paging identity and/or a mobile equipment identification number, for example.

[0018] In one embodiment of the present invention, a method of communication is provided to at least one wireless unit originating an emergency call. The method includes the step of receiving at least one tag identifier in response to the emergency call originating from the

at least one wireless unit. Once the tag identifier is received, a wireless call back number corresponding with the at least one tag identifier may be transmitted. It should be noted that a public service answering point emergency call register may receive the tag identifier(s) and transmits the wireless call back number over a D interface.

[0019] In another embodiment of the present invention, a method is provided for establishing an emergency call originated by at least one wireless unit within a communication system having an emergency call register. The method may include transmitting at least one tag identifier from a mobile switching center associated with the at least one wireless unit over an E_x interface, for example, in response to the emergency call from the at least one wireless unit. As in the previously detailed embodiment, the tag identifier(s) may include a reference key to the emergency call register. Moreover, the tag identifier(s) may correspond with at least one of an emergency service routing key, a local public safety number, a paging identity and a mobile equipment identification number. Thereafter, the transmitted tag identifier(s) may be entered into the emergency call register (e.g., a serving system emergency call register or a public service answering point emergency call register).

[0020] In yet another embodiment of the present invention, a method is provided for establishing an emergency callback originated by at least one wireless unit within a communication system having an emergency call register. The method may include transmitting at least one tag identifier from the emergency call register over a B_e interface. The tag identifier may then be received and entered into a database, such as an emergency service message entity. Thereafter, the emergency callback corresponding with the entered tag identifier may be requested.

[0021] In still another embodiment of the present invention, a method is provided for establishing an emergency callback originated by at least one wireless unit within a communication system having an emergency service message entity. The method may include receiving at least one tag identifier from an emergency call register over a B_e interface and entering the tag identifier (s) into the emergency service message entity. Subsequently, the emergency callback corresponding with the entered at least one entered tag identifier may be requested.

[0022] In still another embodiment of the present invention, a method is provided for establishing an emergency call originated by at least one wireless unit associated with a mobile switching center. The method includes transmitting at least one tag identifier from the mobile switching center associated with the wireless unit(s) to an emergency service entity in response to the emergency call from the at least one wireless unit. The method may include transmitting callback and location information associated with the wireless unit(s) from the emergency service message entity over a D interface, wherein the callback and location information correspond with the at least one tag identifier.

[0023] These and other embodiments will become apparent to those skilled in the art from the following detailed description read in conjunction with the appended claims and the drawings attached hereto.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] The present invention will be better understood from reading the following description of non-limiting embodiments, with reference to the attached drawings, wherein below:

FIGS. 1 and **2** depicts an architecture and flow chart of one embodiment of the present invention; and
FIGS. 3 and **4** depicts an architecture and flow chart of another embodiment of the present invention.

[0025] It should be emphasized that the drawings of the instant application are not to scale but are merely schematic representations, and thus are not intended to portray the specific dimensions of the invention, which may be determined by skilled artisans through examination of the disclosure herein.

DETAILED DESCRIPTION

[0026] The present invention provides for a method and system architecture for ensuring a real callback number may be provided for a wireless unit originating a "9-1-1" call. More particularly, the present invention enables a call center, such as a local Public Service Answering Point Call Center ("PSAP-CC"), to initiate a callback, irrespective of whether the originating "9-1-1" caller was placed over wireless or wireline communications infrastructure, based on at least one tag identifier. For the purposes of the present disclosure, a tag identifier may correspond with a name or label to uniquely associate signaling from different sources such as, for example, the association of a voice. Consequently, the tag identifier may include one or more reference keys to a database, such as an emergency call register or an emergency service message entity, for example. The tag identifier(s), therefore, may correspond with an emergency service routing key, a local public safety number, a paging identity and/or a mobile equipment identification number, for example.

[0027] Referring to **FIGS. 1** and **2,** a set of embodiments of the present invention is illustrated. With respect to **FIG. 1,** an architecture **10** of a network reference model ("NRM") supporting mobile emergency service is shown, while **FIG. 2** illustrates a message flow diagram **100** corresponding with the NRM of **FIG. 1.** More particularly, the embodiments of **FIGS. 1** and 2 may be associated with a non-call associated signaling ("NCAS") technique for delivering a call to a call center over a designated interface without the data that may

be necessary to handle the particular call over this designated interface.

[0028] As shown in **FIG. 1,** a wireless unit **20** is shown for communicating a "9-1-1" call to architecture **10.** For the purposes of the present disclosure, a "9-1-1" call corresponds with an emergency call and/or a request for an emergency service(s) (e.g., police, fire department, road repair, and/or ambulance). The communication, as originated by wireless unit **20,** is conveyed to a mobile switching center **40** ("MSC") through a base station **30** over an air interface, U_m. This step of communicating a "9-1-1" call to architecture **10** corresponds with message flow **110** in diagram **100** of **FIG. 2.**

[0029] Once the "9-1-1" call is received by MSC **40,** identification information associated with wireless unit **20** may be communicated to an emergency call register at a serving system **50** ("ECR-SS"). This step of communicating information to ECR-SS **50** corresponds with the message flow **120** of **FIG. 2.** More particularly, the information associated with wireless unit **20** includes, for example, a mobile equipment identification number ("MEIN"). The transfer of the MEIN to ECR-SS **50** is performed by MSC **40** over a first NRM interface, E_x. It should be noted that the MEIN, as transferred to ECR-SS **50**, might be realized by an International Mobile Equipment Identity ("IMEI"), electronic serial number ("ESN"), pseudo ESN ("pESN") and/or mobile equipment identity ("MEID").

[0030] Along with transferring the MEIN, MSC **40** may also communicate a paging identity ("PGID") to ECR-SS **50** as part of message flow **120.** In the event that the "9-1-1" call from wireless unit **20** is dropped or disconnected from base station **30** and MSC **40,** the PGID may be used to page wireless unit **20.** To page wireless unit 20 in the circumstance of a call drop or disconnect, a local public safety number ("LPN") of MSC **40** may be needed to uniquely identify the switch serving "9-1-1" caller (e.g., wireless unit **20).** The LPN may be a realized by a dialable number from a native or non-portable number block assigned to MSC **40.** The LPN may assist in identifying ECR-SS **50** and for originating a call back to the "9-1-1" caller in the event of a call drop or disconnect within architecture **10.**

[0031] In addition to the LPN, an Emergency Service Routing Key ("ESRK") may also be employed for uniquely identifying the "9-1-1" caller as part of message flow **120** of **FIG. 2.** The ESRK may support the communication of location information of wireless unit **20,** as associated with the "9-1-1" call. The network elements and interfaces involved in providing an ESRK may be realized, in one embodiment, using existing communication standards.

[0032] From the hereinabove, the PGID may be one of a number of communication standards-based identifiers supporting paging wireless unit **20** to deliver an inbound call if the "9-1-1" call is dropped or disconnected. With respect to a GSM-based system, wireless unit **20** may be paged via an international mobile station identity ("IMSI") provided by wireless unit **20,** a temporary mobile station identity ("TMSI") associated with the IMSI and/or an IMEI from wireless unit **20.** In a CDMA2000 system, this paging step may be realized using a mobile identification number ("MIN"), an IMSI, a default mobile station identity ("dMSID") from a non-subscriber initiated ("NSI") wireless unit(s), an ESN from wireless unit **20** and/ or a pESN generated from an MEID within wireless unit **20.**

[0033] With identification information associated with wireless unit **20** received from MSC **40,** SS-ECR **50** may then redirect this information over a network interface, E_y, to another emergency call register ("ECR") associated with a public service answering point **70** ("PSAP"). This activity corresponds with message flow **130** of **FIG. 2.** Consequently, the MEIN, LPN, dMSID and/or ESRK may be re-transmitted from SS-ECR 50 to ECR-PSAP **70.** It should be noted that a PSAP-ECR database is shown as associated with an emergency service message entity **80** ("ESME"). Other associated databases in ESME **80,** however, may be keyed on the ESRK, the MEIN, the mobile station identity (e.g., MIN or IMSI) and/ or the directory number of the caller.

[0034] Thereafter, the ESRK may be signaled with the "9-1-1" call from MSC 40 to an emergency service network element **60** ("ESNE"). This transmission is performed over another network interface, A_{ix}. This activity corresponds with message flow **140** of **FIG. 2.**

[0035] Once delivered to ESNE **60,** the ESRK is then re-transmitted to a public safety access point call center **90** ("PSAP-CC"). This further transmission of the ESRK may be performed over another network interface, C. This activity corresponds with message flow **150** of **FIG. 2.**

[0036] Subsequently, PSAP-CC **90** may use the ESRK to query ESME **80** about wireless unit **20** from which the "9-1-1" call originated. It should be noted that ESME **80** now should include the information previously redirected from interface E_y to ECR-PSAP **70.** This query of ESME **80** may be performed over another network interface, D. This activity corresponds with message flow **160** of **FIG. 2.**

[0037] In response to the query from PSAP-CC **90,** ESME **80** may provide a callback number ("CBN"), as well as the cell site location and/or the wireless unit location, the LPN of the serving system and the MEIN of wireless unit **20** to PSAP-CC **90.** This information may be directed to PSAP-CC **90** over the D interface. This activity corresponds with message flow **170** of **FIG. 2.** It should be noted that the CBN directed to PSAP-CC **90,** in one embodiment of the present invention, may not be the directory number of the wireless unit or a non-dialable number as prescribed by exiting standards for NSI phones. In contrast, here, the callback number may consist of the LPN of MSC **40** serving wireless unit **20** and the MEIN of wireless unit **20.**

[0038] With the CBN at its disposal, PSAP-CC **90** may further signal the PSAP-ECR **70** and ESME **80** over the

D interface using the ESRK as a database key. This signaling step may be performed to request a callback through MSC **40** should the "9-1-1" originating call be dropped or disconnected. Callback through MSC **40** allows any PSAP-CC without the ability to immediately place an outbound call to use the D interface as an alternative to signal the PSAP-CC within the ESME to request MSC **40** to originate a new 9-1-1 call between the mobile phone and the PSAP-CC. Here, the request for a callback may be relayed through PSAP-ECR **70** to SS-ECR **50** over the E_y interface. Thereafter, SS-ECR **50** may then request a callback through MSC **40** over the E_x interface. This activity corresponds with message flows **180** through **200** of **FIG. 2.**

[0039] In alternative embodiment, an attendant in PSAP-CC **90** could use the LPN and/ or MEIN to originate a callback directly to MSC **40** serving wireless unit **20** if PSAP-CC **90** were equipped with the appropriately lines and equipment. Here, the MEIN may be inserted in an ISDN user part ("ISUP") relating to global address parameter ("GAP"). It should be noted that PSAP-CC **90** might also use the ESRK to send a request ESME **80** over the D interface to demand ESNE **60.** This demand may be intended to initiate a callback from PSAP-CC **90** to MSC **40** using the LPN and the MEIN. This activity corresponds with message flows **210** through **220** of **FIG. 2.**

[0040] It should be noted that the MEIN might identify wireless unit 20 for paging by MSC **40** to complete the callback. The directory number of PSAP-CC **90** may be contained in the calling party field of the call origination message. This number may be known by MSC **40** and checked in the calling party field to insure the caller may be authorized for emergency callback service.

[0041] Referring to **FIGS. 3** and **4,** a set of another embodiments of the present invention is illustrated. With respect to **FIG. 3,** an architecture **300** of a network reference model ("NRM") supporting mobile emergency service is shown, while **FIG. 4** illustrates a message flow diagram **400** corresponding with the NRM of **FIG. 3.** More particularly, the embodiment of **FIGS. 3** and **4** may be associated with an alternative technique for establishing a call by a call center.

[0042] As shown in **FIG. 3,** a wireless unit **320** is shown for communicating a "9-1-1" call to architecture **300.** The communication, as originated by wireless unit **320,** is conveyed to an MSC **340** through a base station **330** over an air interface, U_m. This step of communicating a "9-1-1" call to architecture **300** corresponds with message flow **410** in diagram **400** of **FIG. 4.**

[0043] Once the "9-1-1" call is received by MSC **340,** identification information associated with wireless unit **320** may be communicated to an ECR-SS **350.** This step of communicating information to ECR-SS 350 corresponds with the message flow **420** of **FIG. 4.** More particularly, the information associated with wireless unit **320** includes, for example, a MEIN. The transfer of the MEIN to ECR-SS 350 is performed by MSC **340** over a first NRM interface, E_x. It should be noted that the MEIN, as transferred to ECR-SS **350,** might be realized by an IMEI, ESN, pESN and/ or MEID.

[0044] Along with transferring the MEIN, MSC **340** may also communicate a PGID to ECR-SS **350** as part of message flow **420.** In the event that the "9-1-1" call from wireless unit **320** is dropped or disconnected from base station **330** and MSC **340,** the PGID may be used to page wireless unit **320.** To call wireless unit 320 in the circumstance of a call drop or disconnect, an LPN of MSC **340** may be needed to uniquely identify the particular switch or end office serving the "9-1-1" caller (e.g., wireless unit **320).** The LPN may be a realized by a dialable number from a native or non-portable number block assigned to MSC **340.** The LPN may assist in identifying ECR-SS **350** and for originating a call back to the "9-1-1" caller in the event of a call drop or disconnect within architecture **300.**

[0045] In addition to the LPN, an ESRK may also be employed for uniquely identifying the "9-1-1" caller (e. g., wireless unit **320)** as part of message flow **420** of **FIG. 4.** The ESRK may support the communication of location information of wireless unit **320,** as associated with the "9-1-1" call. The network elements and interfaces involved in providing an ESRK may be realized, in one embodiment, using existing communication standards.

[0046] From the hereinabove, the PGID may be one of a number of communication standards-based identifiers supporting paging wireless unit **320** if the "9-1-1" call is dropped or disconnected. With respect to a GSM-based system, wireless unit **320** may be paged via an IMSI provided by wireless unit **320,** a TMSI associated with the IMSI and/or an IMEI from wireless unit **320.** In a CDMA2000 system, this paging step may be realized using a MIN, an IMSI, a dMSID from a NSI wireless unit (s), an ESN from wireless unit **320** and/or a pESN generated from an MEID within wireless unit **320.**

[0047] In contrast with approach of the embodiments of **FIGS. 1** and **2,** architecture **300** and message flow diagram **400** depict a combination of call associated signaling ("CAS") and non-call associated signaling ("NCAS"). More particularly, the CAS technique may be associated with ESNE **360,** while the NCAS method is associated with a PSAP-CC **390** based on separating a PSAP-ECR **370** from an ESME **380.** Consequently, this technique may be termed a Hybrid CAS and NCAS for mobile emergency service.

[0048] Achitecture **300** employs a network interface E_y between an SS-ECR 350 and PSAP-ECR **370.** Furthermore, besides the addition of a network interface, E, between MSC **340** and ESME **380,** network interface, B, may now be positioned between ESNE **360** and ESME **380** without PSAP-ECR **370.** Consequently, a direct interface between ESNE **360** and PSAP-ECR **370** is not shown. Moreover, an additional network interface, B_e, has also been included between PSAP-ECR **370** and ESME **380.** Network Interface D may now be positioned

between ESME **380** and PSAP-CC **390.** Finally, a separate additional network interface, D_e, has been incorporated between PSAP-ECR **370** and PSAP-CC **390.**

[0049] With identification information associated with wireless unit 320 received from MSC **340,** unlike the embodiments of FIGS. 1 and 2, SS-ECR **350** may communicate this information about the new emergency call over the Ey interface to PSAP-ECR **370.** This activity corresponds with message flow **430** of **FIG. 4.** It should be noted that PSAP-ECR **370** is logically separated from ESME **380.** Consequently, the LPN, MEIN and ESRK may also be communicated over the Be interface from PSAP-ECR **370** to ESME 380.

[0050] Thereafter, the ESRK may be communicated with the call (e.g., as call associated signaling) by MSC **340** over the A_{ix} interface with the LPN and MEIN to ENSE 360. This activity corresponds with message flow **440** of FIG. 4. It should be noted that the ESRK may be sent over the C interface to the PSAP-CC 390 from ESNE 360, while the LPN and MEIN may be sent from ESNE 360 to ESME 380 over the B interface corresponding with message flow 450.

[0051] Once the ESRK has been communicated with the call and transmitted over the C interface, PSAP-CC 390 may use the ESRK to query ESME 380. This query is intended to provide PSAP-CC 390 with the callback number (i.e., the LPN and MEIN) associated with wireless unit 320. This activity corresponds with message flow 460 of FIG. 4.

[0052] Subsequently, ESME 380 may responds to PSAP-CC 390. More particularly, ESME 380 may provide the callback number, wireless unit location and other pertinent information needed to PSAP-CC 390 for handling the emergency call. This activity corresponds with message flow 470 of FIG. 4.

[0053] If the "9-1-1" call is dropped or disconnected, PSAP-CC 390 may use the ESRK to signal ESME 380 over the D interface. In so doing, a callback may be requested through MSC 340. This activity corresponds with message flow **480** of **FIG. 4.** Thereafter, ESME **380** may use the MEIN associated with the ESRK in its database to request a callback through MSC **340** from PSAP-ECR **370** corresponding with message flow **490.** Alternatively, PSAP-ECR **370** may use the MEIN to signal PSAP-CC **390** may use the MEIN to signal PSAP-ECR **370** directly over the D_e interface to request a callback through MSC **340** corresponding with message flow **495.**

[0054] Subsequently, PSAP-ECR **370** may use the MEIN to request callback through MSC service. Here, the callback is made by MSC **340** with the request from PSAP-ECR **370** sent through the SS-ECR **350.** This activity corresponds with message flow **500** of **FIG. 4.** Finally, SS-ECR **350** may provide MSC **340** with the PGID and request a callback through MSC **340** to wireless unit **320** and to PSAP-CC **390.**

[0055] While the particular invention has been described with reference to illustrative embodiments, this description is not meant to be construed in a limiting sense. It is understood that although the present invention has been described, various modifications of the illustrative embodiments, as well as additional embodiments of the invention, will be apparent to one of ordinary skill in the art upon reference to this description without departing from the spirit of the invention, as recited in the claims appended hereto. Consequently, the method, system and portions thereof and of the described method and system may be implemented in different locations, such as the wireless unit, the base station, a base station controller and/or mobile switching center, for example. Moreover, processing circuitry required to implement and use the described system may be implemented in application specific integrated circuits, software-driven processing circuitry, firmware, programmable logic devices, hardware, discrete components or arrangements of the above components as would be understood by one of ordinary skill in the art with the benefit of this disclosure. Those skilled in the art will readily recognize that these and various other modifications, arrangements and methods can be made to the present invention without strictly following the exemplary applications illustrated and described herein and without departing from the spirit and scope of the present invention It is therefore contemplated that the appended claims will cover any such modifications or embodiments as fall within the true scope of the invention.

Claims

1. A method of communication to at least one wireless unit originating an emergency call, the method comprising:

   receiving at least one tag identifier in response to the emergency call from the at least one wireless unit; and

   transmitting a wireless call back number corresponding with the at least one tag identifier.

2. The method of Claim **1**, wherein the step of transmitting a wireless call back number comprises:

   transmitting location information associated with the at least one wireless unit, the location information corresponding with the at least one tag identifier.

3. A method of establishing an emergency call originated by at least one wireless unit within a communication system having an emergency call register, the method comprising:

   transmitting at least one tag identifier from a

mobile switching center associated with the at least one wireless unit in response to the emergency call from the at least one wireless unit.

4. A method of establishing an emergency callback originated by at least one wireless unit within a communication system having an emergency call register, the method comprising:

transmitting at least one tag identifier from the emergency call register;

entering the at least one tag identifier into an emergency service message entity; and

requesting the emergency callback corresponding with the entered at least one received tag identifier.

5. A method of establishing an emergency call originated by at least one wireless unit within a communication system having an emergency service message entity, the method comprising:

receiving at least one tag identifier from an emergency call register;

entering the at least one tag identifier into the emergency service message entity; and

requesting the emergency call corresponding with the entered at least one entered tag identifier.

6. A method of establishing an emergency call originated by at least one wireless unit associated with a mobile switching center, the method comprising:

transmitting at least one tag identifier from the mobile switching center associated with the at least one wireless unit to an emergency service entity in response to the emergency call from the at least one wireless unit.

7. The method of Claim **6,** comprising:

transmitting callback and location information associated with the at least one wireless unit, the callback and location information corresponding with the at least one tag identifier.

8. The method of Claims **1** or **2** or **3** or **4** or **5** or **6** or **7** or **8,** wherein the at least one tag identifier comprises a reference key to a database,

9. The method of Claim **8,** wherein the database comprises at least one of an emergency call register and an emergency service message entity.

10. The method of Claim **8,** wherein the at least one tag identifier corresponds with at least one of an emergency service routing key, a local public safety number, a paging identity and a mobile equipment identification number.

FIG. 1

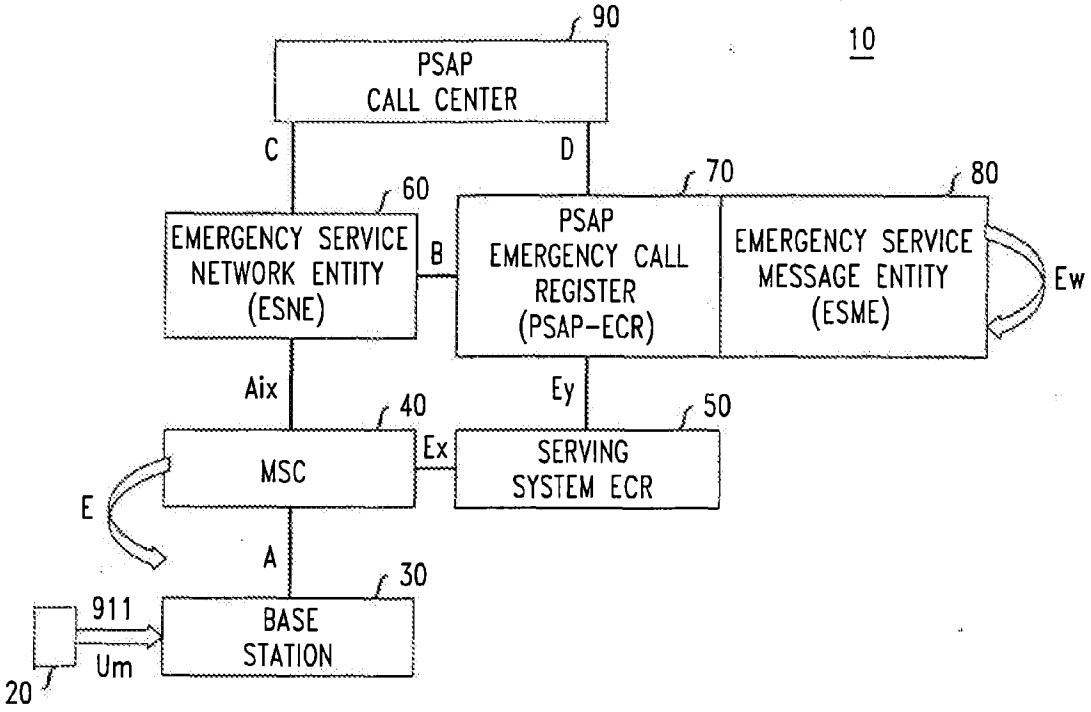

90
PSAP
CALL CENTER
10
C
D
60
70
80
EMERGENCY SERVICE
NETWORK ENTITY
(ESNE)
B
PSAP
EMERGENCY CALL
REGISTER
(PSAP-ECR)
EMERGENCY SERVICE
MESSAGE ENTITY
(ESME)
Ew
Aix
Ey
40
50
MSC
Ex
SERVING
SYSTEM ECR
E
A
30
911
BASE
STATION
Um
20

FIG. 2

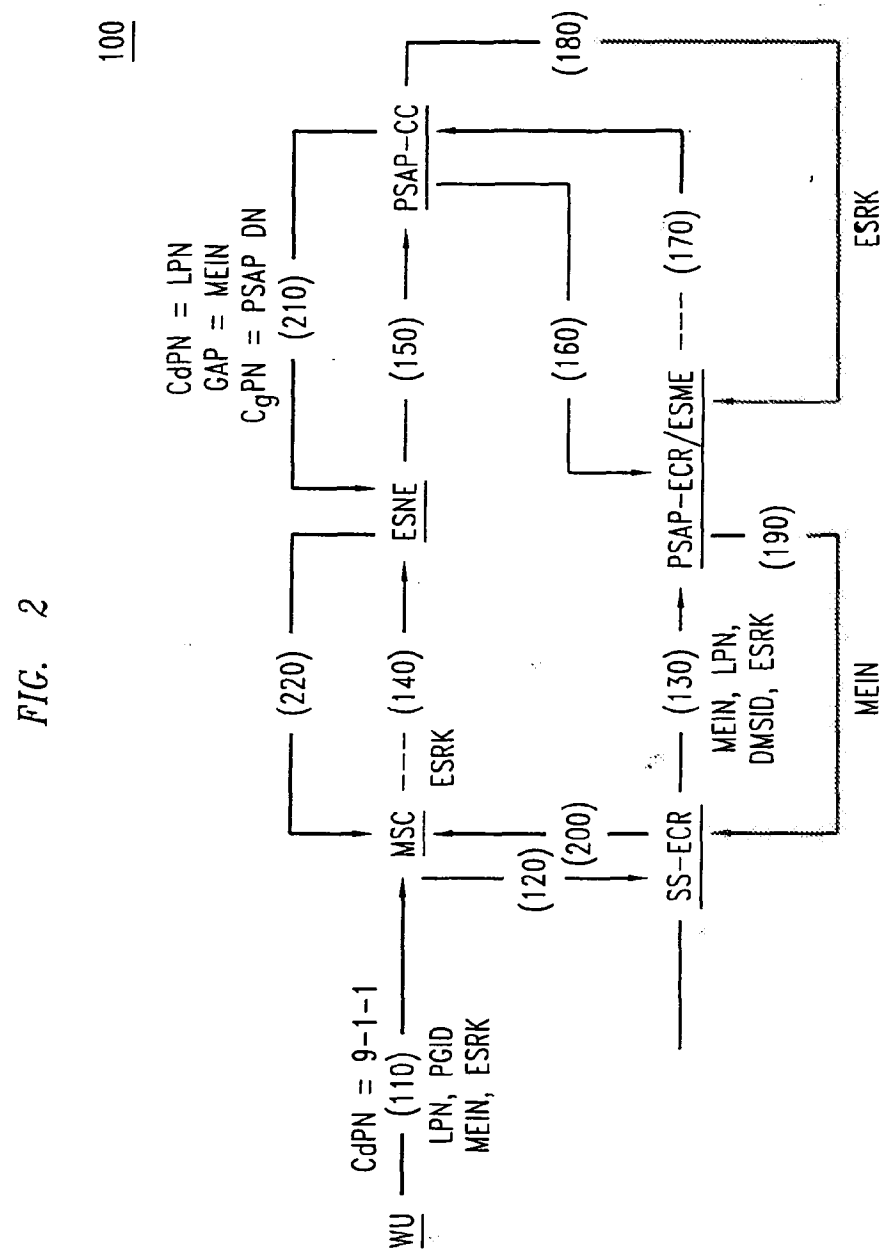

100
WU
CdPN = 9-1-1
(110)
LPN, PGID
MEIN, ESRK
MSC
ESRK
(140)
(120)
(200)
SS-ECR
(130)
MEIN, LPN,
DMSID, ESRK
(190)
MEIN
(220)
ESNE
(150)
(160)
PSAP-ECR/ESME
(170)
ESRK
CdPN = LPN
GAP = MEIN
CgPN = PSAP DN
(210)
PSAP-CC
(180)

FIG. 3

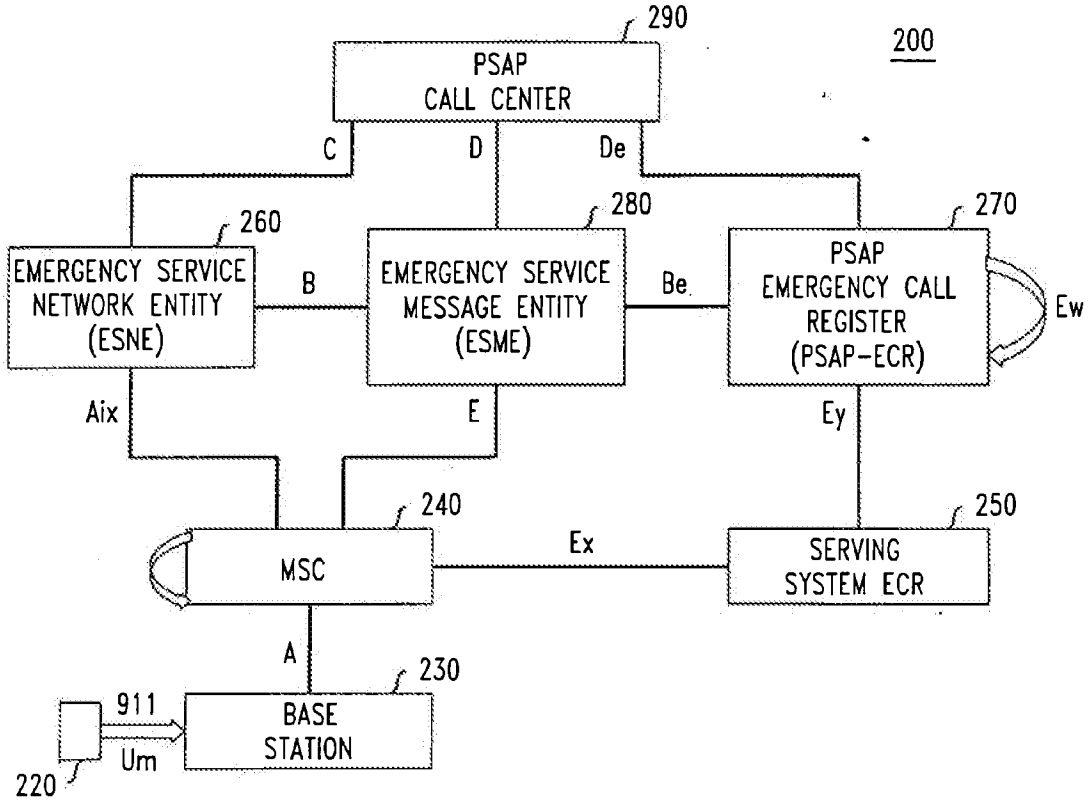
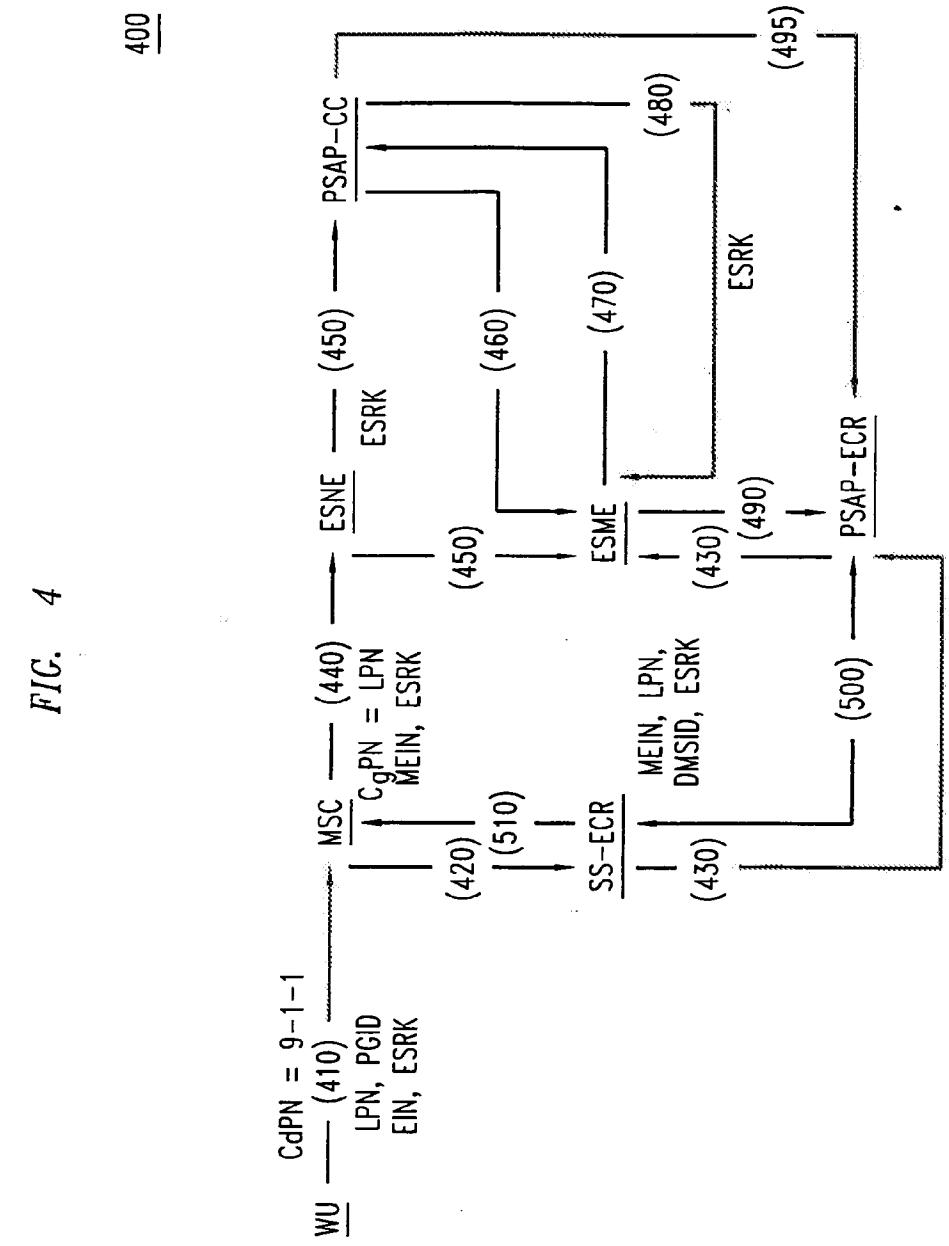

290
200
PSAP
CALL CENTER
C
D
De
260
280
270
EMERGENCY SERVICE
NETWORK ENTITY
(ESNE)
B
EMERGENCY SERVICE
MESSAGE ENTITY
(ESME)
Be
PSAP
EMERGENCY CALL
REGISTER
(PSAP-ECR)
Ew
Aix
E
Ey
240
250
MSC
Ex
SERVING
SYSTEM ECR
A
230
911
BASE
STATION
Um
220

FIG. 4


400
WU
CdPN = 9-1-1
(410)
LPN, PGID
EIN, ESRK
MSC
(420)
CgPN = LPN
MEIN, ESRK
(440)
ESNE
ESRK
(450)
PSAP-CC
(480)
(450)
(460)
(470)
ESRK
(495)
ESME
(430)
(490)
PSAP-ECR
(510)
SS-ECR
(430)
MEIN, LPN,
DMSID, ESRK
(500)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 25 1291

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 864 755 A (KING ET AL) 26 January 1999 (1999-01-26) * column 2, line 1 - line 35 * * column 2, line 54 - column 3, line 56 * -----	1-6	H04Q7/38
X	US 6 038 437 A (ZICKER ET AL) 14 March 2000 (2000-03-14) * column 2, line 45 - column 3, line 2 * * column 5, line 60 - column 6, line 13 * * column 7, line 25 - line 39 * * column 8, line 14 - column 10, line 31 * -----	1-6	
X	EP 1 124 394 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) * paragraph [0007] - paragraph [0012] * -----	1-6	
A	HATFIELD DALE N: "A Report on technical and Operational Issues Impacting The Provision of Wireless Enhanced 911 Services"[Online] 1 November 2002 (2002-11-01), pages 1-47, XP002325700 Retrieved from the Internet: URL:http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239> [retrieved on 2005-04-21] * paragraph [2.2.4] * -----	1	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Berlin	22 April 2005	Rothlübbers, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 25 1291

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-04-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5864755 A	26-01-1999	CA 2257815 A1	18-12-1997
		CN 1234948 A ,C	10-11-1999
		DE 69714445 D1	05-09-2002
		DE 69714445 T2	28-11-2002
		EP 0910922 A2	28-04-1999
		JP 2001502856 T	27-02-2001
		KR 2000016579 A	25-03-2000
		RU 2188517 C2	27-08-2002
		WO 9748247 A2	18-12-1997
US 6038437 A	14-03-2000	US 5937344 A	10-08-1999
EP 1124394 A	16-08-2001	US 6556816 B1	29-04-2003
		CA 2328257 A1	31-07-2001
		EP 1124394 A1	16-08-2001
		JP 2001245360 A	07-09-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 610 583 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.12.2005 Bulletin 2005/52

(51) Int Cl.[7]: **H04Q 7/38**

(21) Application number: **05253822.0**

(22) Date of filing: **21.06.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(30) Priority: **24.06.2004 US 582615 P**
25.06.2004 US 877011

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

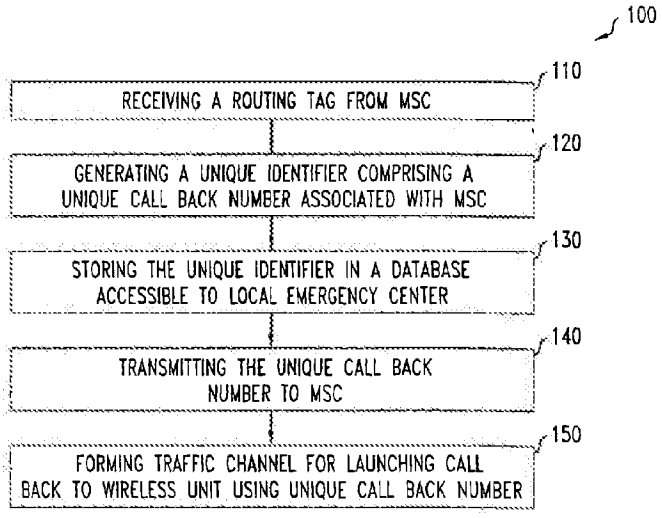
(72) Inventor: **Rollender, Douglas Harold**
Bridgewater, NJ 08807 (US)

(74) Representative: **Sarup, David Alexander**
Lucent Technologies UK Limited,
5 Mornington Road
Woodford Green, Essex IG8 OTU (GB)

(54) A method of providing a unique call back number for wireless 9-1-1 calls

(57) A method of communication to at least one wireless unit originating an emergency call. The method includes the step of receiving one or more routing tags associated with a wireless unit originating a "9-1-1" call. A routing tag may comprise, for example, a string of numbers corresponding with Emergency Service Routing Digits ("ESRD") and/or an Emergency Service Routing Key ("ESRK"). In addition to the routing tag, a mobile equipment identification number ("MEIN") and/or a paging identity ("PGID") may also be received by a database accessible by wireless network infrastructure elements, such as a mobile switching center ("MSC"), as well as the emergency call center, including the local public service answering point, for example. In response to this receiving step, at least one unique identifier (e.g., unique call back number) may be generated. This unique identifier may be a dialable number to enable the emergency call center to call back the wireless unit originating the "9-1-1" call. Thereafter, the unique identifier may be transmitted back to the MSC, along with the emergency call center, for example. Consequently, an emergency call back may be launched by the emergency call center using the unique identifier to reach the MSC generally, and more particularly, the wireless unit originating the "9-1-1" call.

FIG. 2



EP 1 610 583 A1

Description

BACKGROUND OF THE INVENTION

I. FIELD OF THE INVENTION

[0001] The present invention relates to telecommunications, and more particularly, to wireless communications.

II. DESCRIPTION OF THE RELATED ART

[0002] Emergency service calls in North America may be originated by dialing "9-1-1." Other parts of the world may use another abbreviated string of dialable digits, such as "6-1-1" in Mexico, for example. These abbreviated string of digits are intended to simplify an emergency call for help with an easy to remember number. These emergency calls may be routed to a local Public Service Answering Point ("PSAP") call center to enable the initiation of an emergency response (e.g., police, fire department, road repair, and/or ambulance) while the caller is kept on the phone. If, however, the call is somehow disconnected or dropped before the emergency is completely reported or the responder arrives, the PSAP call center may be required to call back the originator.

[0003] Presently, a record for a "9-1-1" call originated through a wired network may include Automatic Line Identification ("ALI") or the telephone number of the access line from which the call originated. The directory number ("DN") or telephone number of a wireless subscriber may not, however, be associated with a physical line or wireless unit. Calls to a roaming wireless subscriber are routed to the wireless unit by way of the mobile station identification ("MSID"), as opposed to the mobile DN ("MDN"). Accordingly, performing an emergency call back to a wireless unit poses hurdles not encountered with landline devices, for example.

[0004] The MSID may typically be characterized as either a 10-digit mobile identification number ("MIN") or a 15-digit International Mobile Subscriber Identifier ("IMSI"). The IMSI may be programmed into a wireless unit or a Subscriber Identity Module ("SIM") card by the service provider with whom the wireless unit user has entered into a service agreement. Accordingly, the MSID may not necessarily be a dialable number.

[0005] The DN of a wireless unit is a dialable number. The DN is dialed by a caller and used to route a call through the network to the wireless subscriber's home system. At the subscriber's home system, the home location register ("HLR") contains the MSID associated with the subscriber's DN. The MSID, as opposed to the DN, may then be used to route the call through the network to the serving wireless system and page the subscriber. The subscriber's DN may be provided to the serving system from the SIM card through the wireless unit or by the home system to the serving system in a separate data file called the subscriber profile.

[0006] The rollout of systems employing a separate number for DN and MSID is a relatively recent occurrence for some wireless systems. Others have used this technique since their inception. Historically, the mobile identification number of a wireless unit was the same as the DN for some systems, particularly in systems supportive of TIA/EIA-41 standards, prior to implementing wireless number portability ("WNP") or thousands block number pooling ("TBNP") based on the Local Routing Number ("LRN") method and international roaming ("IR"). However, with WNP and TBNP, the MDN became "portable" or "poolable" from one service provider to another service provider. Since MSID may not be portable or poolable, the recipient service provider may assign a new MSID for a subscriber with a ported-in or pooled MDN.

[0007] International roaming has also forced the separation of MSID and MDN. While the MIN is a 10-digit number modeled after the North American Numbering Plan's 10-digit MDN, other nation's carriers using a different directory numbering plan may not allow their subscriber's DN to be equivalent to the internationally recognized MIN format. Another standard MSID is the IMSI. It may be used in TIA/EIA-41 and GSM systems around the world. IMSI is a 15-digit non-dialable number based on ITU-T Recommendation E.212, and therefore, may not serve as a 10-digit MDN.

[0008] Historically, when the MDN was the same as the MIN, the MIN would be delivered to a PSAP call center and would be used as a call back number. With the separation of MIN and MDN as described above, it became necessary to deliver the MDN as a separate call back number to the PSAP call center, as well as the caller's MSID. There are certain problems, however, associated with implementing this solution. One issue is that the serving system may not have the caller's MDN, only the MSID, to present to the PSAP call center with the call. Some of the reasons for this relate to the way MSID-MDN separation has been implemented according to standards. Another reason is that the network interface used to deliver the call to the PSAP call center may not have the capacity to signal both the DN and MSID or, in some cases, even a full DN.

[0009] An old serving TIA/EIA-41 system may not support WNP, TBNP or IR. This means that the older serving system may be expecting the MIN and the MDN to be the same. The older system would not even know to look for a separate MDN in the subscriber's service profile (e.g., keyed on MIN, not MDN). With this limitation, these subscribers may not be allowed to use basic services, but they must be allowed to call for emergency services. As a result, a roamer who dials "9-1-1" while on an old system will have his or her call delivered to the PSAP call center with an MSID but no MDN. Accordingly, no call back is possible.

[0010] A newer serving system that is WNP and IR capable may not be able to deliver MDN to the PSAP call center. This could happen if the calling wireless unit

is not registered with any service provider (e.g., there are mobile phones used for emergency calls only). These wireless units may be referred to as non-subscriber initialized ("NSI") phones. It is also possible for a subscriber to place an emergency call before the HLR has responded to the serving system with the subscriber's service profile containing the DN. Even if the PSAP call center has been provided with a working DN for callback, the callback to the DN will not go through if the subscriber has call forwarding service for all inbound calls or if the subscriber has a limited, pre-paid service and there is no remaining balance available to pay for the inbound callback from the PSAP call center. Further, if the callback number is to a visiting international roamer, the PSAP call center may need to place an international call. Some PSAP call center may not have the ability to callback an international number. There is also the risk of network congestion or delay in completing an international call that would be detrimental to handling an emergency in a timely manner. Some PSAP call centers may not even be equipped to place any outbound calls through separate, outbound administrative lines.

[0011] The call back DN for an international roamer would require the PSAP call center to place an international call to reach a subscriber in their local Emergency Service Zone ("ESZ"). This is not a practical, timely or sufficiently reliable solution for a PSAP call center that normally does not place international calls and for applications that may require immediate call back information for emergency purposes. In addition, the entire international MDN (up to 15 digits including a country code) may not be presented to the PSAP call center for call back if the PSAP call center only supports 10 digits.

[0012] It is also possible that the calling wireless unit is not registered with any service provider. As a result, there may be no DN associated with the wireless unit or no permanent MSID encoded in the wireless unit - such wireless units are referred to as NSI mobile phones, for example. This could be because (a) the NSI phone was never intended to be registered (there are such phones to use for emergency calls only), (b) the phone is new and has not yet been initialized by a service provider, (c) the subscription has expired and the NSI phone is no longer registered with a service provider or (d) the SIM card is lost, stolen, or simply never been inserted or been removed either advertently or inadvertently.

[0013] Some wireless units also support a removable User Identity Module ("R-UIM") or SIM that may contain the MSID and the DN. If the R-UIM or SIM are not in the phone, then it can still be used to place an emergency call. However, there is no DN or MSID known to the phone or the serving system to provide the PSAP call center as a call back number.

[0014] Every MS contains a unique mobile equipment identification number ("MEIN") encoded in the phone by the manufacturer. The MEIN may be, for example, an electronic serial number ("ESN"), as used in ANSI/TIA/EIA-41 systems or an International Mobile Equipment Identity ("IMEI") used in GSM systems. The MEIN is independent of the MSID and DN. The MEIN is signaled over the air between the wireless unit and the base station of a wireless system with a call origination attempt or soon thereafter. For example, if not supplied with the call origination attempt, the MEIN may be requested by the serving system.

[0015] Current standards for wireless emergency services call for delivering "9-1-1 + the last seven digits of the MEIN" to the PSAP call center as the form call back number when the directory number assigned to the wireless subscriber is not available. While this may serve to notify the PSAP call center that no working callback number is available with the call, the string of "9-1-1 + the last seven digits of the MEIN (MEIN7)" do not uniquely identify the call (i.e., many emergency calls may be identified by the same "9-1-1+MEIN7) and is not a routable number through the network. This is because the "9-1-1 + the last seven digits of the MEID" do not contain a complete MEID, and therefore is not unique.

[0016] While the hereinabove approach provides the PSAP call center with some measure for performing an emergency call back of a wireless unit, several hurdles still exist. For example, the callback number for a wireless unit in certain circumstances may be nothing more than a dummy number with user location data. Consequently, a need exists for a method and system architecture for uniquely identifying each wireless unit originating a "9-1-1" call. Furthermore, there is a demand for a unique identifier that may be used to enable the PSAP call center to launch a call back of the wireless unit originating a "9-1-1" call.

SUMMARY OF THE INVENTION

[0017] The present invention provides for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, the present invention provides for enabling the call back of a wireless unit originating a "9-1-1" call using a unique identifier. For the purposes of the present disclosure, a unique identifier may correspond with a unique call back number for enabling an emergency call center (e.g., a local public service answering point) to launch a call back of the wireless unit(s) that originated the "9-1-1" call. This unique call back number may be generated from a string of numbers corresponding with a local public safety number ("LPN") associated with wireless network infrastructure element(s), such as a mobile switching center ("MSC"), for example.

[0018] In an embodiment of the present invention, a method includes the step of receiving one or more routing tags associated with a wireless unit originating a "9-1-1" call. A routing tag may comprise, for example, a string of numbers corresponding with Emergency Service Routing Digits ("ESRD") and/or an Emergency Service Routing Key ("ESRK"). In addition to the routing tag, a mobile equipment identification number ("MEIN") and/

or a paging identity ("PGID") may also be received by a database accessible by wireless network infrastructure elements, such as an MSC, as well as the emergency call center, including the local public service answering point, for example. In response to this receiving step, at least one unique identifier (e.g., unique call back number) may be generated. This unique identifier may be a dialable number to enable the emergency call center to call back the wireless unit originating the "9-1-1" call. Thereafter, the unique identifier may be transmitted back to the MSC, along with the emergency call center, for example. Consequently, an emergency call back may be launched by the emergency call center using the unique identifier to reach the MSC generally, and more particularly, the wireless unit originating the "9-1-1" call.

These and other embodiments will become apparent to those skilled in the art from the following detailed description read in conjunction with the appended claims and the drawings attached hereto.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The present invention will be better understood from reading the following description of non-limiting embodiments, with reference to the attached drawings, wherein below:

FIGS. 1 and 2 depict an architecture and flow chart of an embodiment of the present invention; and
FIGS. 3 and 4 depict alternate embodiments of the present invention.

[0020] It should be emphasized that the drawings of the instant application are not to scale but are merely schematic representations, and thus are not intended to portray the specific dimensions of the invention, which may be determined by skilled artisans through examination of the disclosure herein.

DETAILED DESCRIPTION

[0021] The present invention provides for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, the present invention provides for enabling the call back of a wireless unit originating a "9-1-1" call using a unique identifier. For the purposes of the present disclosure, a unique identifier may correspond with a unique call back number for enabling an emergency call center (e.g., a local public service answering point) to launch a call back of the wireless unit(s) that originated the "9-1-1" call. This unique call back number may be generated from a string of numbers corresponding with a local public safety number ("LPN") associated with wireless network infrastructure element(s), such as a mobile switching center ("MSC"), for example.

[0022] Referring to FIG. 1, an embodiment of the present invention is illustrated. FIG. 1 is reflective of an architecture 10 of a network reference model ("NRM") supporting mobile emergency service is shown. Architecture 10 supports the unique identification of a wireless unit originating an emergency "9-1-1" call and for enabling the call back of the wireless unit originating the emergency "9-1-1" call using a unique identifier.

[0023] As shown in FIG. 1, a wireless unit 20 is shown for communicating an emergency "9-1-1" call to architecture 10. For the purposes of the present disclosure, an emergency "9-1-1" call corresponds with a call and/or a request for emergency services (e.g., police, fire department, road repair, and/or ambulance). The communication, as originated by wireless unit 20, is conveyed to a mobile switching center 40 ("MSC") through a base station (not shown).

[0024] Once the emergency "9-1-1" call is received by MSC 40, identification information associated with wireless unit 20 may be communicated to a serving system emergency call register 50 ("SS-ECR"). More particularly, the information associated with wireless unit 20 includes, for example, a mobile equipment identification number ("MEIN"). The transfer of the MEIN to ECR-SS 50 is performed by MSC 40 over a first NRM interface, E_x. It should be noted that the MEIN, as transferred to SS-ECR 50, might be realized by an International Mobile Equipment Identity ("IMEI"), electronic serial number ("ESN"), pseudo ESN ("pESN") and/or mobile equipment identity ("MEID").

[0025] Along with transferring the MEIN, MSC 40 may also communicate a paging identity ("PGID") to SS-ECR **50**. In the event that the emergency "9-1-1" call from wireless unit **20** is dropped or disconnected from the base station and MSC 40, the PGID may be used to page wireless unit 20. To page wireless unit 20 in the circumstance of a call drop or disconnect, a local public safety number ("LPN") of MSC 40 may be needed to uniquely identify the switch serving "9-1-1" caller (e.g., wireless unit 20). The LPN may be realized by a dialable number from a native or non-portable number block assigned to MSC 40. The LPN may assist in identifying SS-ECR 50 and for originating a call back to the wireless unit originating the emergency "9-1-1" call in the event of a call drop or disconnect occurs.

[0026] In addition to the LPN, Emergency Service Routing Digits ("ESRD") or Emergency Service Routing Key ("ESRK") may also be employed for uniquely identifying the emergency "9-1-1" call. ESRD may not uniquely identify the emergency "9-1-1" call, while ESRK may support the communication of location information of wireless unit 20, as associated with the emergency "9-1-1" call. The network elements and interfaces involved in providing an ESRK may be realized, in one embodiment, using existing communication standards. It should be noted that the Emergency Service Routing Digits may include, in one example, a string of numbers associated with a cell sector of the mobile switching center in which the emergency call originates, while the

Emergency Service Routing Key may include a string of numbers associated with at least one of a mobile positioning center and/or geographical mobile location center 90.

[0027] From the hereinabove, the PGID may be one of a number of communication standards-based identifiers supporting paging wireless unit 20 to deliver an inbound call if the emergency "9-1-1" call is dropped or disconnected. With respect to a GSM-based system, wireless unit 20 may be paged via an international mobile station identity ("IMSI") provided by wireless unit 20, a temporary mobile station identity ("TMSI") associated with the IMSI and/or an IMEI from wireless unit 20. In a CDMA2000 system, this paging step may be realized using a mobile identification number ("MIN"), an IMSI, a default mobile station identity ("dMSID") from a non-subscriber initiated ("NSI") wireless unit(s), an ESN from wireless unit 20 and/or a pESN generated from an MEID within wireless unit 20.

[0028] With identification information associated with wireless unit 20 received from MSC 40, ECR-SS 50 may then redirect this information over a network interface, E_y, to another emergency call register ("ECR") **60** associated with a public service answering point ("PSAP") **70**. Consequently, the MEIN, LPN, dMSID, ESRK and/or a unique identifier (e.g., unique call back number or "UCBN") may be re-transmitted from SS-ECR **50** to ECR **60**. It should be noted that ECR 60 might be realized by a database. Other associated databases in, however, may be keyed on the ESRK, the MEIN, the mobile station identity (e.g., MIN or IMSI) and/or the directory number of the caller.

[0029] The E interfaces depicted support signaling of emergency data and service requests through architecture 10 between MSC 40 and PSAP 70. Call handling instructions from PSAP **70**, such as to establish a call-back through MSC **40**, may be communicated from PSAP **70** to ECR **60** over an E_d interface, on to SS-ECR **50** through an E_y interface and from SS-ECR **50** to MSC **40** through an Ex interface. Here, PSAP **70** may communicate with ECR **60** directly over the E_d interface using a unique identifier (e.g., a unique call back number) as a key. Alternatively, PSAP 70 may communicate with ECR 60 indirectly through an automatic line identifier ("ALI") database 80 over the D and E_z interfaces using ESRK or the unique identifier (e.g., a unique call back number) as key.

[0030] SS-ECR 50 and ECR 60 may be implemented as a single entity. As shown, however, SS-ECR 50 and ECR 60 are individual elements to allow consideration for one SS-ECR to serve one MSC and one SS-ECR to interface with many ECRs associated with PSAP 70. In addition, while one ECR may serve many PSAPs, one PSAP need only interface with one ECR. Moreover, PSAP 70 may have access to information in many ECRs through ECR networking over the E_w interface.

[0031] Referring to FIG. 2, a flow chart depicting another embodiment of the present invention is illustrated. More particularly, an algorithmic method (100) is shown for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, algorithmic method (100) enables the call back of a wireless unit originating a "9-1-1" call using a unique identifier. This is of particularly relevance if the originating emergency "9-1-1" call was terminated.

[0032] The algorithmic method (100) of FIG. 2 may initially include the step of receiving a routing tag (step 110). A routing tag is associated with a wireless unit originating a "9-1-1" call and may, for example be transmitted by mobile switching center 40 and received by emergency call register 50 of FIG. 1. For the purposes of the present disclosure, a routing tag may comprise, for example, a string of numbers corresponding with Emergency Service Routing Digits ("ESRD") and/or an Emergency Service Routing Key ("ESRK"). Consequently, while the routing tag may identify the originating system and destination PSAP, the routing tag may not uniquely identify the emergency "9-1-1" call if it is an ESRD or may be unable to uniquely identify the emergency "9-1-1" call once the originating call is no longer in progress. It should be noted that in practice, this step of receiving may also include receiving the mobile equipment identification number ("MEIN"), as well as the paging identifier ("PGID") along routing tag. It should be also noted that, in practice, the MEIN and PGID may be received prior to the receiving of the routing tag.

[0033] Once the step of receiving a routing tag has been achieved, the algorithmic method (100) then includes the step of generating a unique identifier (step 120). Unlike the routing tag, the unique identifier identify the emergency "9-1-1" call even if the originating call is no longer in progress. In one embodiment, the unique identifier may be a ten (10) digit, unique call back number associated with at least one serving mobile switching center. In one embodiment, the unique call back number comprises a string of numbers corresponding with a local public safety number ("LPN") associated with the serving mobile switching center. In one scenario, the unique call back number may comprise six (6) fixed digits associated with the LPN (e.g., NPA+NXX) and four unassigned digits (XXX). In this scenario, the four unassigned digits may translate into 10,000 unique number sequences to be assigned as a result of this generating step.

[0034] Thereafter, the algorithmic method (100) may store the generated unique identifier in a database (step 130). The database is accessible to a local emergency center. In one example, the database is realized by emergency call register **60** accessible to PSAP **70** in FIG. 1.

[0035] Once generated, the algorithmic method (100) may then transmit the unique identifier (step 140). Here, the unique identifier (e.g., unique call back number) may, for example be transmitted by emergency call register 50 and received by mobile switching center 40 of FIG. 1. As a result, mobile switching center 40 may iden-

tifying the emergency "9-1-1" call even if the originating call is no longer in progress. Moreover, the local emergency center, such as PSAP 70, may also identify the emergency "9-1-1" call even if the originating call is no longer in progress, by accessing emergency call register 60.

[0036] With the unique call back number accessible to the local emergency center, such as PSAP 70, and mobile switching center 40, the algorithmic method (100) may then form a traffic channel (step 150). This scenario arises in the event the originating emergency "9-1-1" call from the wireless unit is no longer in progress - e.g., disconnected or terminated. After the traffic channel is formed, the local emergency center (e.g., PSAP **70**) may call back the wireless unit originated the emergency "9-1-1" call using the unique identifier (e.g., unique call back number).

EXEMPLARY EMBODIMENT

[0037] Mobile Emergency Service (E911M) requires the following items to be incorporated into wireless and Emergency Service Network standard protocols and procedures: Local Public Safety Number (LPN); Mobile Equipment Identification Number (MEIN); Mobile Equipment Paging Identity (PGID); Unique Call Back Number (UCBN); Emergency Call Register (ECR); and Mobile E9-1-1 Network.

[0038] A Local Public Safety Number (LPN) is a dialable number where the NPA-NXX uniquely identifies the MSC in the originating network. In order to avoid number portability and pooling complexities, the LPN may be taken from the native number block of the MSC.

[0039] The Mobile Equipment Identity Number (MEIN) is a unique serial number programmed into a wireless unit by the manufacturer. In CMRS phones, it may take the form of a 32-bit Electronic Serial Number (ESN) in TDMA, CDMA or Analog phones, a 15-digit International Mobile Equipment Identity (IMEI) in GSM, UMTS or PCS1900 phones or a 56-bit Mobile Equipment Identity (MEID) in CDMA2000 phones. Every phone has a MEIN but not every wireless system uses MEIN to page the phone. However, this may be modified as needed to allow a mobile phone that is used to originate an emergency 9-1-1 call to be paged for a call back with its MEIN. The alternative is to create a data field in the ECR called the Paging Identity (PGID) to store one of many possible identifiers that may be used by the serving system to page a mobile phone.

[0040] PGID may be the Mobile Subscription Identity (MSID) if it is available from the phone with the emergency 9-1-1 call origination. The MSID may be a 15-digit International Mobile Subscription Identity (IMSI) or a 10-digit Mobile Identification Number (MIN). MSID is not available with an emergency 9-1-1 call origination if a Non-Subscription Initialized (NSI) phone is used to place the call. There is no MSID programmed into a NSI phone by a service provider or in a phone without a Subscriber Identity Module (SIM card). PGID may be a Temporary Mobile Station Identity (TMSI), a default MSID (dMSID) provided by the phone manufacturer and used for Over-The-Air Activation (OTA) of a new phone, a new 56 bit MEID or a pseudo-ESN (pESN) derived from the MEID. The PGID is whatever identity a wireless phone provides for itself when it enters a system and is acceptable by that system to page that phone for a call back.

[0041] The Unique Callback Number (UCBN) is dynamically assigned at the serving system when a 9-1-1 call is originated. It is stored in the ECR as a key to the database. The UCBN is signaled with every emergency 9-1-1 call to uniquely identify the emergency 9-1-1 call, retrieve call back information from the PSAP-ECR and originate a call back. The UCBN is a unique10-digit dialable number based on the NPA-NXX from the LPN of the serving system. The last four digits are uniquely assigned to each call at the serving system. The UCBN is not a Mobile Directory Number (MDN) or Mobile Station ISDN Number (MSISDN) assigned to the calling subscriber by the home service provider. If the UCBN is used for call back, it is signaled to the serving system MSC as the Called Party Number (CPN). The MSC uses the UCBN to request a PGID from the SS-ECR. The PGID is then used to page the phone and complete the callback.

[0042] Based on existing guidelines, the UCBN may be signaled from the MSC to the Selective Router and on to the PSAP as the Call Back Number (CBN) in the Calling Party Number (CPN) or the Charge Number (CHGN) when the ESRD is populated in either the Generic Digits Parameter (GDP) or the Called Party Number (CdPN). When the ESRK is populated as the either the CPN or CHGN, the UCBN may be populated in the other field or in the GDP.

[0043] If the UCBN is not signaled with a call routed by the ESRK, then the PSAP may use the ESRK while the call is still in progress to obtain the UCBN from the PSAP-ECR or the ALI. ALI may get the UCBN from the PSAP-ECR or the MPC. MPC may have the UCBN if it is provided by the MSC.

[0044] The Emergency Call Register (ECR) is a database holding emergency call detail information and call handling instructions for the MSC. The ECR database is keyed on the UCBN and contains the MEIN, PGID, ESRK or ESRD for the emergency 9-1-1 call, as well as the LPN of the serving system. The LPN may be updated automatically as the wireless unit originating the emergency 9-1-1 caller roams and is handed off (or over) from one serving system to another.

[0045] ECR entries may be created in different ways. An entry may be created at the originating network with the origination of a 911 call, through a download of entries from other ECRs or by manual entry. Manual entry of a MEIN and any local LPN into a ECR associated with the PSAP allows the PSAP to call any wireless unit through the MSC even if the wireless unit was not used to originate an emergency 9-1-1 call. LPN Update pro-

cedures allow for the LPN of the serving system to be automatically entered into the SS-ECR after the wireless unit is located in the true serving system. The LPN is updated in other PSAP-ECRs and SS-ECRs through the Mobile E-9-1-1 Network.

[0046] The Mobile E9-1-1 Network may be used to exchange data between ECRs and trigger events in other network elements. An ECR is located with an MSC at the serving system (SS-ECR), a PSAP in the Emergency Services Network (PSAP-ECR), and any other call center handling emergency calls. For example, a secondary PSAP or a Telematics Call Center may have an ECR to track 9-1-1 calls and other outbound calls placed for their clients, to track inbound calls from clients or to remotely request service for clients through the serving system.

[0047] The ECR Network is used for more than exchanging emergency call information and tracking individual phones. The ECR network is also used to manage mobility for mobile phones used to place an emergency 9-1-1 call and request services through the MSC. Messages are signaled through the network to support intersystem operations for Intersystem Roaming and Emergency Short Message Service for NSI Phones and International Roamers, Emergency Call Origination through the MSC for Telematics Call Centers, PSAP-to-PSAP Call Forwarding or Conference Calling through the MSC, LPN Update, Intersystem Paging for Emergency Call Back and possibly many other services. The PSAP-ECR acts like a Home Location Register (HLR) and the SS-ECR acts like a Visitor Location Register (VLR).

[0048] Referring to FIG. 3, a signal flow diagram 200 according to an exemplary embodiment of the present invention is illustrated. FIG. 3 depicts the process in the origination of an emergency "9-1-1" call by a wireless unit. Here, an emergency "9-1-1" call is originated by a wireless unit through a serving MSC using a routing tag, such as an ESRD ("Emergency Service Routing Digits") or an ESRK ("Emergency Service Routing Key"). The emergency "9-1-1" call may be routed to a geographically designated PSAP call center based on the routing tag - e.g., the corresponding ESRD or ESRK. An emergency call register ("ECR") coupled with the serving MSC and the PSAP call center may then be updated with call back information. Thereafter, a unique identifier may be generated for uniquely identifying the emergency "9-1-1" call. This unique identifier may be realized by a unique call back number derived from a local public safety number. Moreover, the routing tag - the corresponding ESRD or ESRK - may identify the originating system and destination PSAP. It should be noted that an ESRD does not uniquely identify the call, while an ESRK may be used to uniquely identify the call so long as the call is in progress.

[0049] Referring to **FIG. 4**, a signal flow diagram 300 according to another exemplary embodiment of the present invention is illustrated. FIG. 3 depicts the process of calling back the wireless unit, which originated the emergency "9-1-1" call. After the original emergency "9-1-1" call was terminated, the PSAP may dial the unique identifier (e.g., unique call back number) derived from a local public safety number to reach the wireless unit originating the emergency "9-1-1" call. Here, the MSC uses the unique identifier to retrieve an associated paging identifier ("PGID") from a serving system emergency call register ("SS-ECR"), page the wireless unit and then complete the call back to the wireless unit. Alternatively, the PSAP may use the unique identifier or the mobile equipment identification number to request a call back from through the MSC from the PSAP emergency call register ("PSAP-ECR").

[0050] While the particular invention has been described with reference to illustrative embodiments, this description is not meant to be construed in a limiting sense. It is understood that although the present invention has been described, various modifications of the illustrative embodiments, as well as additional embodiments of the invention, will be apparent to one of ordinary skill in the art upon reference to this description without departing from the spirit of the invention, as recited in the claims appended hereto. Consequently, the method, system and portions thereof and of the described method and system may be implemented in different locations, such as the wireless unit, the base station, a base station controller and/or mobile switching center, for example. Moreover, processing circuitry required to implement and use the described system may be implemented in application specific integrated circuits, software-driven processing circuitry, firmware, programmable logic devices, hardware, discrete components or arrangements of the above components as would be understood by one of ordinary skill in the art with the benefit of this disclosure. Those skilled in the art will readily recognize that these and various other modifications, arrangements and methods can be made to the present invention without strictly following the exemplary applications illustrated and described herein and without departing from the spirit and scope of the present invention It is therefore contemplated that the appended claims will cover any such modifications or embodiments as fall within the true scope of the invention.

Claims

1. A method of communication with at least one wireless unit originating an emergency call, the method comprising:

   receiving at least one routing tag associated with the at least one wireless unit; and

   transmitting at least one unique identifier for uniquely identifying the at least one wireless

unit in response to the step of receiving at least one routing tag.

2. The method of Claim 1, comprising:

storing the at least one unique identifier in at least one database accessible; and

launching an emergency call back using the stored at least one unique identifier.

3. A method of communication to at least one wireless unit originating an emergency call, the method comprising:

transmitting at least one routing tag associated with the at least one wireless unit; and

receiving at least one unique identifier for uniquely identifying the at least one wireless unit in response to the step of transmitting at least one routing tag.

4. The method of Claim 3, comprising:

forming a traffic channel; and

receiving a launched emergency call back using the received at least one unique identifier over the traffic channel.

5. The method of Claim 3, comprising:

accessing at least one database having the at least one unique identifier stored therein using the at least one routing tag.

6. The method of Claims 1 or 3, wherein the at least one routing tag comprises a string of numbers corresponding with at least one of a Emergency Service Routing Digits and a Emergency Service Routing Key.

7. The method of Claim 6, wherein the Emergency Service Routing Digits comprises a string of numbers associated with a cell sector of the mobile switching center in which the emergency call originates, and the Emergency Service Routing Key comprises a string of numbers associated with at least one of a mobile positioning center and geographical mobile location center.

8. The method of Claims 1 or 3, wherein the unique identifier comprises a unique call back number, the unique call back number comprising a string of numbers associated with a mobile switching center.

9. The method of Claim 8, comprising:

generating the at least one unique identifier from a string of numbers corresponding with a local public safety number associated with the mobile switching center.

10. The method of Claims 1 or 3, comprising:

communicating at least one of a mobile equipment identification number and a paging identity upon originating the emergency call.

FIG. 1

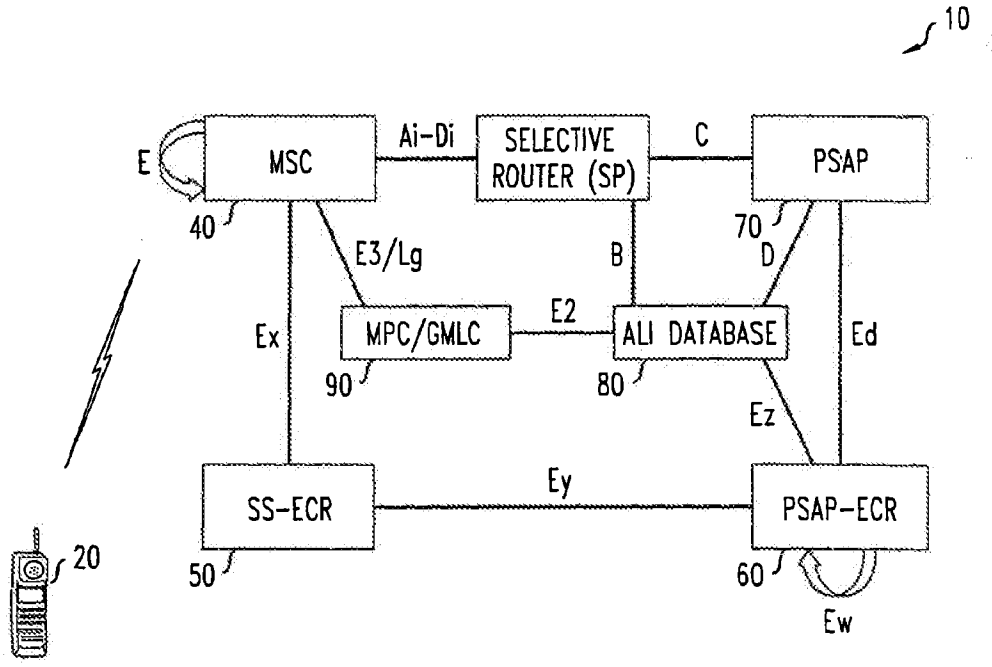


FIG. 2

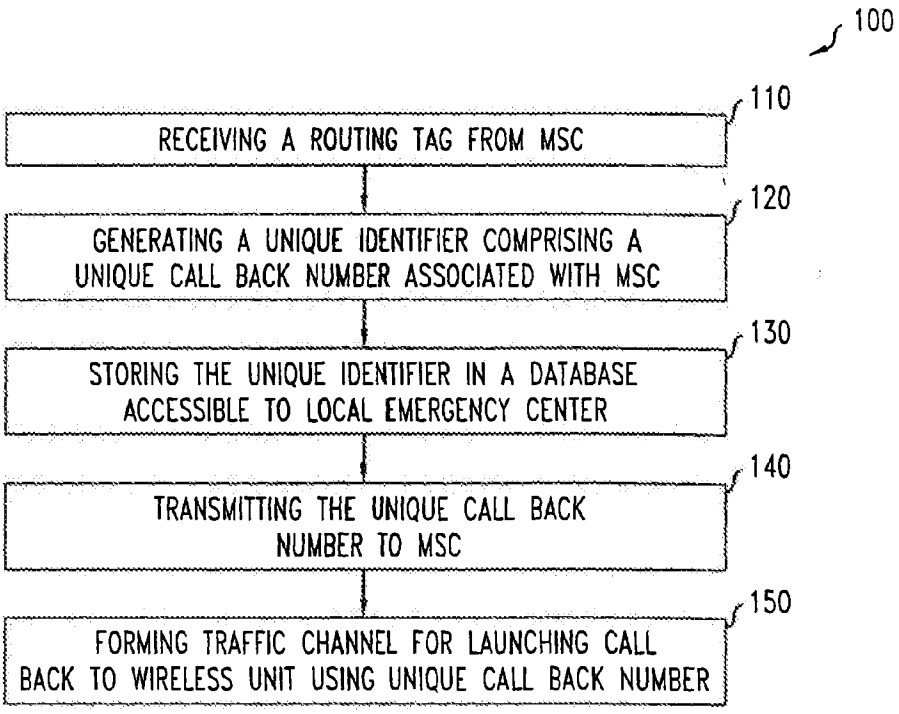


FIG. 3

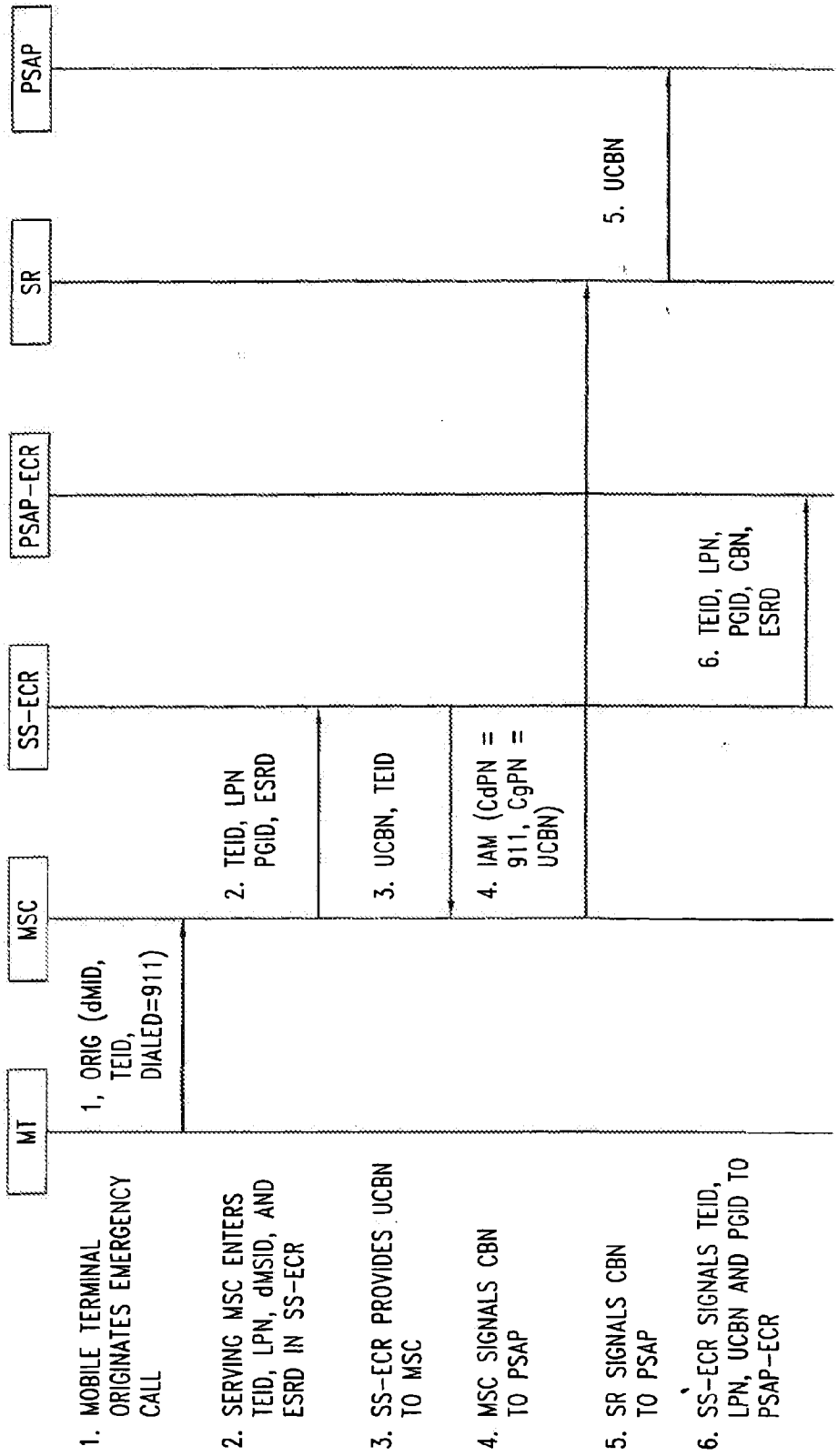
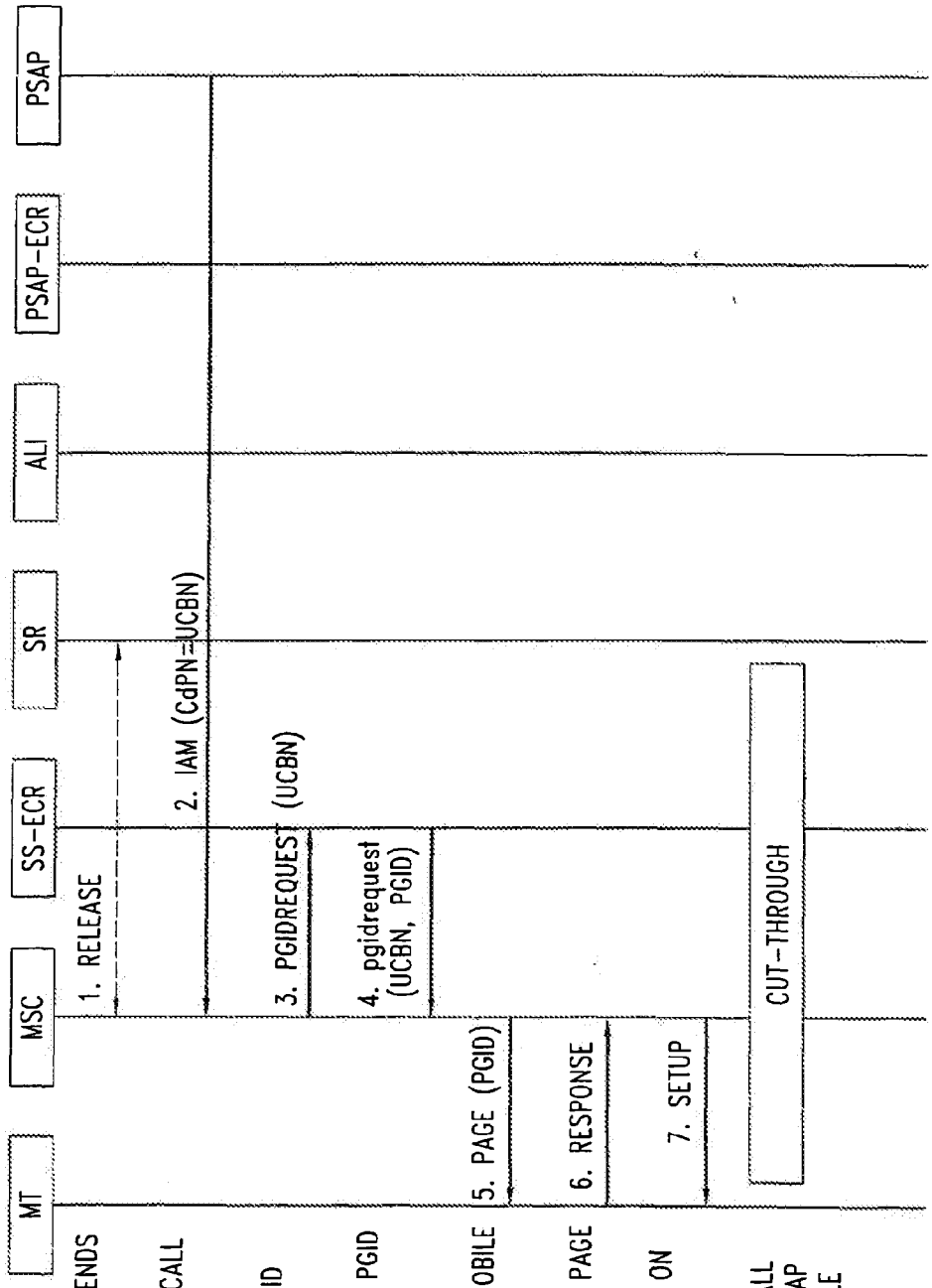


FIG. 4



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 25 3822

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	JEFFREY M. PFAFF: "SPRINT PCS COMMENTS, Enhanced 911 Emergency Calling Systems" DA 00-1975, [Online] 18 September 2000 (2000-09-18), pages 1-17, XP002347969 Washington, D.C. 20554 Retrieved from the Internet: URL:http://www.wutc.wa.gov/webdocs.nsf/0/c551ce36f524ed198825696d007f35a0/$FILE/Comments.pdf> [retrieved on 2005-10-05]	1-7,10	H04Q7/38
Y	* figure 2 *	8,9	
X	US 2002/111159 A1 (FACCIN STEFANO M ET AL) 15 August 2002 (2002-08-15)	1-7,10	
Y	* paragraphs [0003] - [0005], [0014] * * paragraphs [0020] - [0022] *	8,9	
X	US 5 864 755 A (KING ET AL) 26 January 1999 (1999-01-26) * column 2, lines 3-35 * * column 3 * * claim 1 *	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	6 October 2005	Chimet, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 25 3822

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

06-10-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002111159 A1	15-08-2002	EP 1368976 A1	10-12-2003
		WO 02065791 A1	22-08-2002
US 5864755 A	26-01-1999	CA 2257815 A1	18-12-1997
		CN 1234948 A	10-11-1999
		DE 69714445 D1	05-09-2002
		DE 69714445 T2	28-11-2002
		EP 0910922 A2	28-04-1999
		JP 2001502856 T	27-02-2001
		KR 2000016579 A	25-03-2000
		RU 2188517 C2	27-08-2002
		WO 9748247 A2	18-12-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 526 697 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
22.03.2006 Bulletin 2006/12

(43) Date of publication A2:
27.04.2005 Bulletin 2005/17

(21) Application number: **04256443.5**

(22) Date of filing: **20.10.2004**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **21.10.2003 US 690074**

(71) Applicant: **3Com Corporation**
Marlborough, MA 01752-3064 (US)

(72) Inventors:
- **Grabelsky, David**
  Skokie, IL 60076 (US)
- **Homeier, Michael**
  Lake Forest, IL 60045 (US)
- **Tripathi, Anoop**
  Lake Zurich, IL 60047 (US)
- **Joseph, Boby**
  Philadelphia, PA 19131 (US)

(74) Representative: **Finnie, Peter John**
Gill Jennings & Every LLP
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) IP-based enhanced emergency services using intelligent client devices

(57) Providing enhanced emergency services (E-911) to an IP Telephony-based PBX or similar system, by utilizing aspects of the intelligence of end-user SIP client devices to address challenges and difficulties associated with E-911-like services in LAN-based telephony environments.

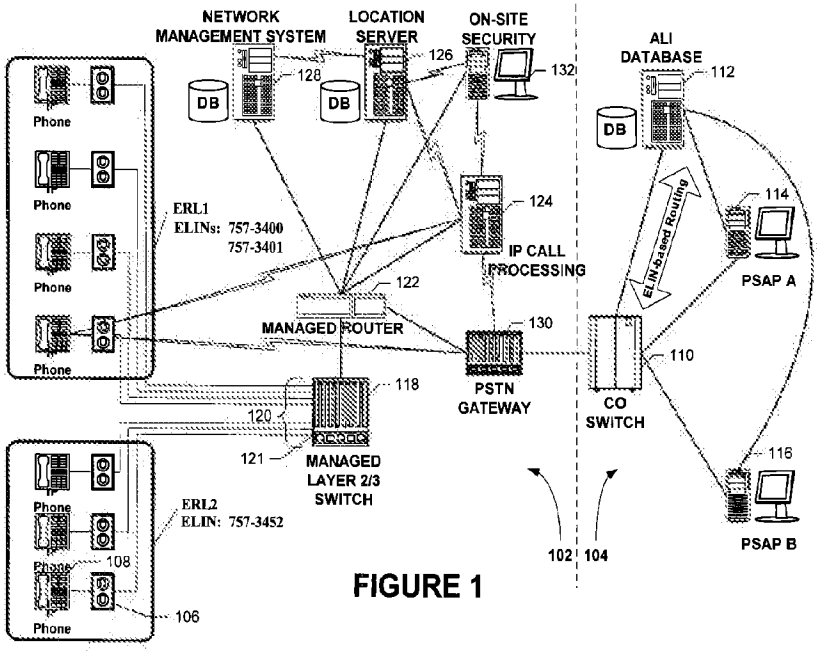


FIGURE 1

EP 1 526 697 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 6443

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	SCHULZRINNE H. COLUMBIA U.: "Emergency Services for Internet Telephony based on the Session Initiation Protocol (SIP)" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 4, 8 January 2003 (2003-01-08), pages 1-14, XP015005201 ISSN: 0000-0004 * page 6 - page 10 *	1-69	H04L29/06
X	TOM TAYLOR NORTEL NETWORKS: "SIP Emergency Assistance Scenarios" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 1, October 2003 (2003-10), pages 1-22, XP015035955 ISSN: 0000-0004 * page 7 - page 18 *	1-69	
X	SCHULZRINNE COLUMBIA U.: "Providing Emergency Call Services for SIP-based Internet Telephony" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, 13 July 2000 (2000-07-13), pages 1-14, XP015035059 ISSN: 0000-0004 * page 2 - page 11 *	1-69	TECHNICAL FIELDS SEARCHED (IPC) H04L
A	US 2003/063714 A1 (STUMER PEGGY M. ET AL.) 3 April 2003 (2003-04-03) * paragraph [0009] - paragraph [0046] *	1-69	
A	US 2002/111159 A1 (FACCIN STEFANO M. ET AL.) 15 August 2002 (2002-08-15) * paragraph [0002] - paragraph [0021] *	1-69	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	1 February 2006	Jurca, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 25 6443

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-02-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003063714 A1	03-04-2003	NONE	
US 2002111159 A1	15-08-2002	EP 1368976 A1	10-12-2003
		WO 02065791 A1	22-08-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP1721446 (A1) — 2006-11-15

DETERMINING THE GEOGRAPHICAL LOCATION FROM WHICH AN EMERGENCY CALL ORIGINATES IN A PACKET-BASED COMMUNICATIONS NETWORK

Inventor(s): DAWSON MARTIN [AU]; LEWIS MARK [US]; BRODA MACIEJ [CA] + (DAWSON, MARTIN, ; LEWIS, MARK, ; BRODA, MACIEJ)

Applicant(s): NORTEL NETWORKS LTD [CA] + (NORTEL NETWORKS LIMITED)

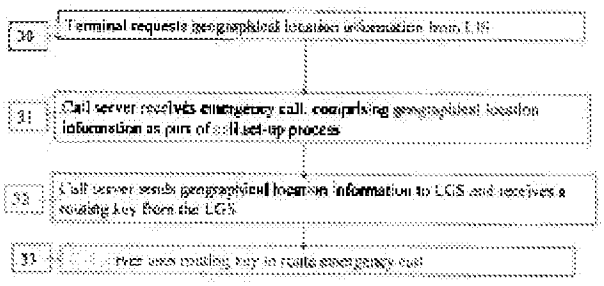
Classification: **- international:*H04M3/42; H04M7/00***
- cooperative: H04M3/42229; H04M7/006; H04M2242/04; H04M2242/30; H04M3/42348

Application number: EP20050708403 20050218

Priority number (s): US20040548746P 20040227 ; US20040861194 20040604 ; WO2005GB00612 20050218

Also published as: US2005190892 (A1) US7177399 (B2) WO2005084002 (A1)

Abstract not available for EP1721446 (A1)
Abstract of corresponding document: US2005190892 (A1)



In order that emergency service vehicles can be dispatched to the correct destination promptly, accurate information about the location of the caller is needed. Another problem concerns routing emergency calls to the correct destination. For emergency calls a universal code is used such as 911 in North America and 112 in Europe. This universal code cannot be used to identify the destination of the call. These problems are particularly acute for nomadic communications systems such as voice over internet protocol communications networks. That is because user terminals change network location. These problems are solved by enabling the geographical location of the emergency caller to be determined by entities within a packet-based network without the need for modification of existing emergency services network infrastructure.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 721 446 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2005/084002 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 2005/084002 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 2005/084002 (art. 158 de la CBE).

Espacenet

Bibliographic data: EP1829300 (A1) — 2007-09-05

METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM

Inventor(s): KALLIO JUHA [FI] ± (KALLIO, JUHA)

Applicant(s): NOKIA CORP [FI] ± (NOKIA CORPORATION)

Classification: - international: ***H04W76/02; H04W8/10;*** *H04W8/26;* ***H04L***
- cooperative: **H04W76/021**; **H04W8/10**; H04W8/26

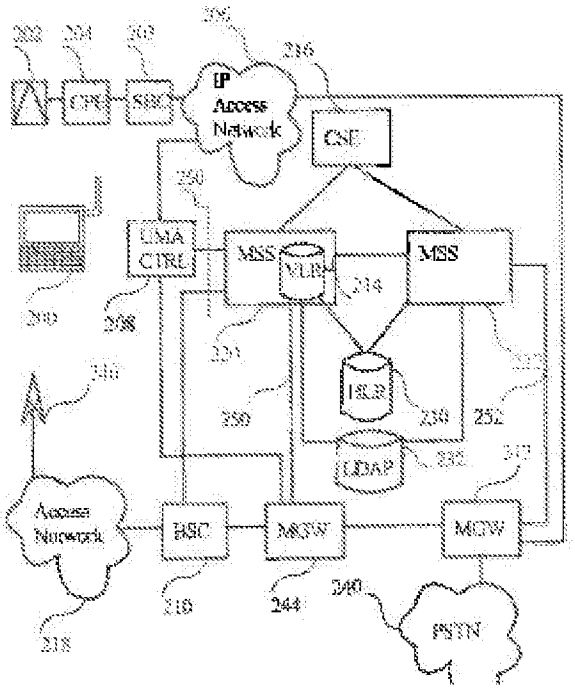
Application number: EP20050821728 20051220

Priority number (s): WO2005FI00540 20051220 ; FI20040001659 20041223

Also published as: EP1829300 (A4) EP1829300 (B1) WO2006067269 (A1) US2006142011 (A1) US7400881 (B2) KR20070097526 (A) KR100886165 (B1) CN101069390 (A) CN101069390 (B) less

Abstract not available for EP1829300 (A1)
Abstract of corresponding document: WO2006067269 (A1)

The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile station. The call control node translates



the called party number to the logical name using the directory.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 829 300 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2006/067269 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 2006/067269 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 2006/067269 (art. 158 de la CBE).

Espacenet

Bibliographic data: EP1371173 (B1) — 2007-11-28

METHOD AND TELECOMMUNICATIONS SYSTEM FOR MONITORING A DATA FLOW IN A DATA NETWORK

Inventor(s): STIFTER HELMUT [DE]; PFAEHLER WOLFGANG [DE]; KREUSCH NORBERT [DE] ± (STIFTER, HELMUT, ; PFAEHLER, WOLFGANG, ; KREUSCH, NORBERT)

Applicant(s): SIEMENS AG [DE] ± (SIEMENS AKTIENGESELLSCHAFT)

Classification: **- international:*H04L12/26; H04L29/06; H04L29/08; H04M3/22***
- cooperative: **H04L12/2602**; **H04L29/06**; **H04L43/00**; **H04L63/00**; **H04L63/30**; **H04L65/103**; **H04L65/1046**; **H04L65/80**; **H04L67/2814**; **H04L67/306**; **H04M3/2281**; H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

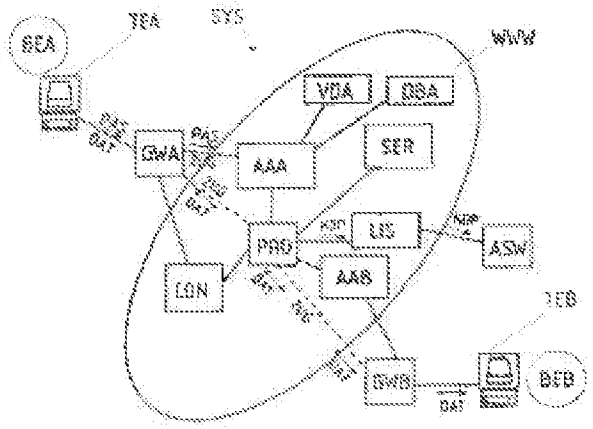
Application number: EP20020759770 20020307

Priority number(s): EP20020759770 20020307 ; WO2002EP02524 20020307 ; EP20010107063 20010321

Also published as: EP1371173 (A1) EP1244250 (A1) US2004181599 (A1) US7979529 (B2) RU2003130974 (A) more

Abstract not available for EP1371173 (B1)
Abstract of corresponding document: EP1244250 (A1)

A data stream (DAT) is monitored in a data network (WWW) between two telecommunications terminals (TEA,TEB) connected to the data network via access servers (AAA,AAB), which operate during a monitoring situation to divert the data stream between the telecommunications terminals through a monitoring server (PRO) that produces a copy (KOP) of the data stream and transmits it to an analyzing unit (ASW). An independent claim is also included for a telecommunication system for monitoring a data stream in a data network between a



telecommunications terminal linked to a data network via a gateway and to a further telecommunications device.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 371 173 B1

(12) # EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
28.11.2007 Patentblatt 2007/48

(21) Anmeldenummer: **02759770.7**

(22) Anmeldetag: **07.03.2002**

(51) Int Cl.:
H04L 12/26 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(86) Internationale Anmeldenummer:
PCT/EP2002/002524

(87) Internationale Veröffentlichungsnummer:
WO 2002/082728 (17.10.2002 Gazette 2002/42)

(54) **VERFAHREN UND TELEKOMMUNIKATIONSSYSTEM ZUR ÜBERWACHUNG EINES DATENSTROMS IN EINEM DATENNETZ**

METHOD AND TELECOMMUNICATIONS SYSTEM FOR MONITORING A DATA FLOW IN A DATA NETWORK

PROCEDE ET SYSTEME DE TELECOMMUNICATION POUR CONTROLER UN FLUX DE DONNEES DANS UN RESEAU DE DONNEES

(84) Benannte Vertragsstaaten:
DE ES FR GB IT

(30) Priorität: **21.03.2001 EP 01107063**

(43) Veröffentlichungstag der Anmeldung:
17.12.2003 Patentblatt 2003/51

(73) Patentinhaber: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

(72) Erfinder:
- **STIFTER, Helmut**
  81739 München (DE)
- **PFÄHLER, Wolfgang**
  85221 Dachau (DE)
- **KREUSCH, Norbert**
  82061 Neuried (DE)

(56) Entgegenhaltungen:
WO-A-00/42742
WO-A-00/56019
WO-A-99/55062

- **METZ CHRISTOPHER: "AAA Protocols: Authentication, Authorization, and Accounting for the Internet" IEEE INTERNET COMPUTING, 1999, Seiten 75-79, XP002176948**

EP 1 371 173 B1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

[0002] Weiters betrifft die Erfindung ein Telekommunikationssystem, welches zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung eingerichtet ist, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

[0003] Von Gesetzgebern wird in zunehmenden Maß verlangt, dass Betreiber von Datennetzen Funktionen zur Verfügung stellen, die es ermöglichen im Bedarfsfall den Datenaustausch einzelner Benutzer zu überwachen.

[0004] Das legale Abhören von Datenströmen die sogenannte "Lawful Interception" in Datennetzen, beispielsweise dem Internet, wird zur Zeit unterschiedlich gelöst.

[0005] Eine bekannte Methode besteht darin, externe Sniffer (Analysatoren) in einem LAN-Segment des zu Überwachenden anzuordnen, welche den gesamten Paket-Datenstrom analysieren und den Verkehr des Überwachten ausfiltern, vervielfältigen und dem Bedarfsträger zustellen. Nachteilig an dieser Methode ist vor allem, dass ein zeitlich befristeter, physikalischer Eingriff in das Netz erforderlich ist. Bei erhöhter Mobilität des zu Überwachenden ist diese Methode praktisch nicht verwendbar.

[0006] Eine andere Methode, die vor allem zum Abhören/Überwachen des e-Mailverkehrs dient, sieht vor, dass an einem oder mehreren e-Mailservern eine automatische Weiterleitungsfunktion implementiert ist, die sowohl ankommende als auch abgehende e-Mails dem Bedarfsträger, beispielsweise eine Behörde, zustellt. Ähnliches gilt für Voice-Mail etc. Bei dieser Methode ist es erforderlich, dass alle e-Mailserver dazu eingerichtet sein müssen, einen Abhör/Überwachungsfall zu erkennen und an die zuständige Behörde weiterzuleiten, was mit einem hohen administrativen Aufwand verbunden sein kann.

[0007] Aus der WO 0042742 sind eine Überwachungsmethode und ein Überwachungssystem zur Durchführen eines gesetzlichen Abhorchens in einem paketorientierten Netz, wie dem GPRS- oder dem UMTS-Netz beschrieben. Hierzu ist ein erstes Netzelement mit Überwachungsfunktionalität für Datenpakete vorgesehen, welches durch ein zweites Netzelement gesteuert wird. Die abgefangenen (überwachten) Daten werden über ein Gateway, welches eine Schnittstelle zu einer zum Abhören berechtigten Behörde darstellt geführt. Nachteilig an dieser Methode ist vor allem, dass auch Datenströme von Benutzern, die nicht abgehört werden sollen durch das Netzelement geführt werden, wodurch sich der technische und administrative Aufwand dieser Methode wesentlich erhöht.

[0008] Zur "Lawful Interception" im Internet siehe beispielsweise ETSI TR 101 750 V1.1.1.

[0009] Nicht außer Acht zu lassen sind die sehr hohen Kosten, die üblicherweise für einen Netzbetreiber bei zur Verfügungstellung der oben erwähnten Abhör/Überwachungsfunktionalität anfallen, die vor allem durch einen hohen administrativen Aufwand verursacht werden.

[0010] Es ist daher eine Aufgabe der Erfindung einen Weg zu schaffen, der es auf einfache und kostengünstige Weise ermöglicht, eine Abhör/überwachungsfunktion in einem Datennetz zu implementieren und anzubieten.

[0011] Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art dadurch gelöst, dass von dem zumindest einem Authentifikationsserver überprüft wird, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei in einem Überwachungsfall eine Kopie des Datenstroms erstellt wird, welcher eine Identifikationskennzeichnung beigefügt wird, und die Kopie samt Identifikationskennzeichnung hierauf an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit übermittelt wird.

[0012] Es ist ein Verdienst der Erfindung, eine Abhörfunktionalität von seiten des Netzes zur Verfügung zu stellen, wodurch ein Eingriff mittels externer Abhörgeräte in das Netz vermieden werden kann. Weiters ist ein Zugriff auf einen Datenstrom eines zu Überwachenden auch dann möglich, wenn er mobil ist und seinen Standort ändert, da er sich über den Authentifizierungsserver eines Providers, der die Maßnahmen zur Überwachung setzt, einwählen muss.

[0013] In einer Variante der Erfindung wird die Kopie von dem Gateway erstellt.

[0014] Eine andere Variante der Erfindung sieht vor, dass die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver erstellt wird.

[0015] Vorteilhafterweise stellt der LI-Server anhand einer Identifikationskennzeichnung fest, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll (en).

[0016] Günstigerweise erstellt der LI-Server die zumindest eine Sekundärkopie, d.h. der LI-Server vervielfältigt die Kopie entsprechend der Anzahl der berechtigten Stellen.

[0017] Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server eine Schnittstellenanpassung zu der Auswerteeinheit durchführt.

[0018] Der Authentifizierungsserver kann anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwa-

chungskennzeichnung feststellen, ob ein Überwachungsfall vorliegt.

[0019] Die verborgene Datenbank steht mit einer Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet wird.

[0020] Im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank werden auch die zugeordneten Überwachungskennzeichnungen in der verborgenen Datenbank gelöscht.

[0021] In einer weiteren Variante der Erfindung wird der Datenstrom als Voice over IP-Datenstrom übertragen, wobei ein Call-Controller den Datenstrom über den Überwachungsserver, der die Kopie erstellt, umleitet.

[0022] Eine andere Möglichkeit besteht darin, dass der Authentifizierunsserver in einem Überwachungsfall den Datenstrom über den Überwachungsserver umleitet.

[0023] Eine Variante des Umleitens besteht darin, dass der Datenzugang von dem Gateway zu dem Überwachungsserver durchgetunnelt wird.

[0024] Um einen Datenverlust zu vermeiden, falls die Kopie nicht sofort an einen Bedarfsträger zugestellt werden kann, kann die Kopie des Datenstroms auf dem Überwachungsserver und/oder auf dem LI-Server zwischengespeichert werden.

[0025] In einer bevorzugten Ausführungsform der Erfindung steuert der Controller sowohl das Gateway als auch den Überwachungsserver.

[0026] Eine weitere sehr vorteilhafte Ausführungsform der Erfindung sieht vor, dass der zumindest eine Authentifizierungsserver den Überwachungsserver steuert.

[0027] Zur Durchführung des erfindungsgemäßen Verfahrens eignet sich insbesondere ein Telekommunikationssystem der eingangs genannten Art, bei welchem der Authentifikationsserver dazu eingerichtet ist, zu überprüfen, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei das Telekommunikationssystem dazu eingerichtet ist, in einem Überwachungsfall eine Kopie des Datenstroms zu erstellen und der Kopie eine Identifikationskennzeichnung hinzuzufügen und die Kopie samt Identifikationskennzeichnung an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit zu übermitteln.

[0028] In einer ersten Variante der Erfindung ist das Gateway dazu eingerichtet, die Kopie des Datenstroms zu erstellen.

[0029] Bei einer zweiten Variante der Erfindung ist ein Überwachungsserver vorgesehen, der dazu eingerichtet ist, die Kopie zu erstellen.

[0030] Weiters ist der LI-Server dazu eingerichtet, anhand der Identifikationskennzeichnung festzustellen, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll (en) .

[0031] Günstiger Weise ist der LI-Server dazu eingerichtet, die zumindest eine Sekundärkopie zu erstellen.

[0032] Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit durchzuführen.

[0033] Der Authentifizierungsserver kann dazu eingerichtet sein, anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwachungskennzeichnung festzustellen, ob ein Überwachungsfall vorliegt.

[0034] Die verborgene Datenbank und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten sind dazu eingerichtet, Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet ist.

[0035] Das Telekommunikationssystem kann dazu eingerichtet sein, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank zugeordnete Überwachungskennzeichnungen in der verborgenen Datenbank zu löschen.

[0036] In einer vorteilhaften Variante der Erfindung, ist der Datenstrom ein Voice over IP-Datenstrom, wobei ein Call-Controller vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

[0037] Eine andere günstige Variante sieht vor, dass der Authentifizierungsserver dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

[0038] Weitere Vorteile lassen sich dadurch schaffen, dass das Telekommunikationssystem dazu eingerichtet ist, den Datenzugang von dem Gateway zu dem Überwachungsserver durchzutunneln.

[0039] Um einem Datenverlust vorzubeugen können der Überwachungsserver und/oder der LI-Server dazu eingerichtet sein, die Kopie des Datenstroms zwischenzuspeichern.

[0040] Weiters kann der Call-Controller dazu eingerichtet sein, sowohl das Gateway als auch den Überwachungsserver zu steuern.

[0041] In einer anderen Variante ist der Authentifizierungsserver dazu eingerichtet, den Überwachungsserver zu steuern. Günstigerweise weist der Uberwachungsserver die Funktionalität eines Proxy-Servers auf.

[0042] Die Erfindung samt weiterer Vorteile ist im folgenden anhand einiger nicht einschränkender Ausführungsbeispiele, die in der Zeichnung veranschaulicht sind dargestellt, in dieser zeigen schematisch:

Fig. 1 ein erfindungsgemäßes Telekommunikationssystem,

Fig. 2a eine Kopie eines Datenstroms mit einer Identifikationskennzeichnung,

Fig. 2b die Identifikationskennzeichnung aus Fig. 2a im näheren Detail und

Fig. 3 einen beispielsweisen Ablauf des erfindungsgemäßen Verfahrens.

[0043] Gemäß Fig. 1 muss sich jeder Benutzer BEA, BEB, eines erfindungsgemäßen Telekommunikationssystems SYS der über sein Telekommunikationsendgerät TEA bzw. Telekommunikationseinrichtung TEB Zugang zu einem Datennetz WWW, beispielsweise dem Internet, haben will, über ein Gateway GWA, GWB einwählen bzw. sich bei einem Zugangsserver AAA anmelden. Unter einer Telekommunikationsvorrichtung wird in diesem Dokument jede Art von Telekommunikationsendgerät, wie beispielsweise ein mit dem Datennetz verbundener PC, bzw. auch Server, die in dem Datennetz WWW stehen können, verstanden.

[0044] Der Zugangsserver AAA, AAB kann als AAA-Server oder als Remote Authentication Dial-In User Service Server kurz RADIUS-Server ausgebildet sein. Um einen Datenzugang ZUG dem Datennetz WWW zu erlangen, ist es für einen Benutzer erforderlich sich zu authentifizieren.

[0045] Die Authentifikation eines Benutzers BEA, BEB kann dabei über Eingabe eines Passwortes PAS bzw. einer Benutzeridentifikation, beispielsweise des Namens des Benutzers, erfolgen.

[0046] Anhand des Identifikationsergebnisses entscheidet der Zugangsserver AAA, AAB, ob einen Datenzugang ZUG zu dem Datennetz WWW gewährt oder verweigert wird.

[0047] Die Authentifikation des Benutzers BEA, BEB kann von seiten des Zugangsservers AAA mittels Abfrage einer Verwaltungsdatenbank VDA, in der die Benutzerdaten verwaltet werden erfolgen.

[0048] Liegt ein positives Authentifizierungsergebnis vor, so wird eine verborgene Datenbank abgefragt, in der jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung UWD zugeordnet ist. Besagt die Überwachungskennzeichnung UWD, dass ein Datenstroms DAT zwischen dem Telekommunikationsendgerät TEA des Benutzer BEA und einem weiteren Telekommunikationsendgerät durchgeführt werden soll, so wird eine Kopie KOP des Datenstromes DAT angefertigt.

[0049] Die Kopie KOP des originalen Datenstromes DAT kann beispielsweise von dem Gateway GWA, welches dem Telekommunikationsendgerät TEA zugeordnet ist, oder von einem eigens hierfür vorgesehenen Überwachungsserver PRO erstellt werden.

[0050] Für den Fall, dass der Überwachungsserver PRO die Kopie des originalen Datenstromes DAT erstellt, wird der Datenstrom DAT zwischen über den Überwachungsserver PRO umgeleitet. Bevorzugter Weise weist dieser Server Proxyfunktionalität auf. Der Überwachungsserver PRO unterscheidet sich von einem Proxy-Server lediglich dadurch, dass der Überwachungsserver PRO dazu eingerichtet ist, die Kopie KOP eines über ihn laufenden (umgeleiteten) Datenstroms DAT zu erstellen und diese Kopie mit einer mitgelieferten Identifikationskennzeichnung IDK (Fig. 2), beispielsweise der IP-Adresse oder einer verschlüsselten Kennzeichnung des abzuhörenden Benutzers, zu versehen und an einen "Lawful Interception"-Server oder kurz LI-Server LIS zu übermitteln, wobei der originale Datenstrom an die durch den Benutzer bestimmte Zieladresse weitergeroutet wird.

[0051] Erstellt das Gateway GWA die Kopie KOP, so ist die soeben beschriebene Funktionalität des Kopierens und Weiterleitens der Kopie KOP an den LI-Server bzw. des Routens des originalen Datenstromes DAT gemäß der benutzerbestimmten Zieladresse in dem Gateway GWA realisiert.

[0052] Ein Datenzugang ZUG zu dem Datennetz WWW kann im Überwachungsfall für den zu überwachenden Benutzer BEA direkt über das Gateway und den Überwachungsserver PRO erfolgen.

[0053] Die Umleitung des Datenstromes DAT an den Überwachungsserver PRO kann mittels Tunneling, beispielsweise gemäß dem in der RFC 2661 spezifizierten L2T-Protokolls erfolgen.

[0054] Eine andere Möglichkeit den Datenstrom DAT über den Überwachungsserver PRO umzuleiten besteht darin, dass dem Überwachungsserver PRO eine Adresse in dem Datennetz zugeordnet wird, im Fall des Internet eine IP-Adresse. Diese Adresse kann in einer Speichereinheit des Zugangsservers AAA, AAB abgelegt sein, wobei im Überwachungsfall der Datenstrom DAT, beispielsweise gemäß dem TCP/IP-Protokolls, an die Adresse des Überwachungsservers PRO weitergeleitet wird.

[0055] Der Überwachungsserver PRO erstellt sodann, wie bereits oben erwähnt, eine Kopie KOP des über ihn umgeleiteten Datenstroms DAT und übermittelt diese Kopie KOP an einen LI-Server, der anhand der Identifikationskennzeichnung IDK, welche der Kopie beigefügt ist, entscheidet was mit der Kopie KOP zu geschehen hat, beispielsweise ob weitere Kopien d.h. Sekundärkopien WKO der Kopie erstellt werden sollen bzw. an welche Auswerteeinheit(en) die Kopie(n) zu übermitteln ist (sind).

[0056] Die weitere Verarbeitung und Auswertung der Kopie KOP erfolgt dann in der Auswerteeinheit ASW, beispielsweise einem dazu eingerichteten PC einer Behörde.

[0057] Der LI-Server LIS ist üblicherweise eine Anordnung mehrerer Workstations. Seine Aufgabe ist es, wie bereits oben erwähnt, die Kopie KOP des Datenstromes DAT zu empfangen, die der Kopie KOP von dem Überwachungsserver beigefügte Identifikationskennzeichnung IDK auszuwerten, gegebenenfalls weitere Kopien WKO der Kopie KOP herzustellen und an die Bedarfsträger zuzustellen.

[0058] Auch ist der LI-Server dazu eingerichtet, eine Schnittstellenanpassung zu unterschiedlichen Auswer-

teeinheiten ASW der Bedarfsträger durchzuführen. So kann es beispielsweise notwendig sein für eine Überwachung zwei H.323 Verbindungen zu einem bekannten Time Division Multiplex oder kurz TDM-Übergabe-Interface der überwachenden Behörde herzustellen. Eine andere Möglichkeit besteht darin, die Kopie über ein IP-Übergabe Interface an die überwachende Behörde zuzustellen.

[0059] Die Informationen, die der LI-Server LIS benötigt, um die Kopie an den Bedarfsträger bzw. die Auswerteeinheit ASW weiterzuleiten, können von Seiten der Bedarfsträger in einer Datenbank LID abgelegt werden.

[0060] Eine weitere Möglichkeit besteht darin, dass die Kopie KOP samt der Identifikationskennzeichnung IDK von dem Überwachungsserver PRO bzw. Gateway GWA direkt an die Auswerteeinheit ASW zugestellt wird.

[0061] Nach dem Erstellen der Kopie KOP des Datenstroms DAT, wird der originale Datenstrom DAT von dem Überwachungsserver PRO auf die herkömmliche Weise, beispielsweise gemäß dem TCP/IP-Protokoll, an den zweiten Benutzer BEB bzw. die Telekommunikationseinrichtung TEB, SER weitergeroutet.

[0062] Nach Fig. 2a wird der Kopie KOP des Datenstromes DAT eine Identifikationskennzeichnung IDK als Header vorangestellt. Die Identifikationskennzeichnung kann zumindest einen IP-Header IPH aufweisen, beispielsweise die IP-Adresse des überwachten Benutzers BEA. Weiters kann ein spezieller LI-Header LIH vorgesehen sein (Fig. 2b), der Informationen betreffend die weitere Datenübermittlung für den LI-Server enthält. So kann beispielsweise die erste Zeile die Art TYP der Nachricht enthalten, ob es zum Beispiel um eine Sprachnachricht oder eine "abgehörte" e-Mail handelt. Eine nächste Zeile kann die Länge LEN des Headers enthalten, während in einer dritten Zeile eine Operator-ID OID gemäß dem Standard ETSI ES 201671 enthalten kann. Eine Rufidentifizierungsnummer CIN kann zur Identifizierung eines "abgehörten" Benutzers BEA dienen, während eine Behördenidentifizierung LID dazu dient den Bedarfsträger, an den die Kopie KOP zugestellt werden soll, zu identifizieren. Weitere Informationen SUP können an die soeben genannten im Bedarfsfall angehängt werden.

[0063] Gemäß Fig. 3 wird im Fall einer Sprachübertragung gemäß dem Voice over IP-Protokoll eine entsprechende Applikation APP auf dem Telekommunikationsendgerät TEA des Anrufers BEA gestartet, welches daraufhin eine Verbindung über ein erstes Gateway GWA zu einem ersten Zugangsserver AAA aufbaut. Dieser Zugangsserver AAA überprüft, welcher Teilnehmer den Dienst zur Sprachübertragung in Anspruch nehmen will, und ob dieser zur Inanspruchnahme dieses Dienstes berechtigt ist. Zu diesem Zweck findet eine H.323 oder RADIUS-Kommunikation zwischen dem Gateway GWA und dem Zugangsserver AAA statt.

[0064] Ist der anrufende Benutzer BEA zur Benutzung des Sprachdienstes berechtigt, so überprüft der Zugangsserver AAA anhand der Authentifizierung dieses Benutzers BEA, ob der Datenaustausch zwischen dem Anrufer und einem Angerufenen überprüft werden soll.

[0065] Nach erfolgreicher Zugangsprüfung ermittelt der Call-Controller CON durch Kommunikation mit einem zweiten Zugangsserver AAB die IP-Adresse des angerufenen Telekommunikationsendgerätes TEB und veranlasst den Signalisierungsverkehr über ein weiteres Gateway GWB zu diesem Telekommunikationsendgerät TEB.

[0066] Ist nun der Anrufer zu überwachen, dann baut der Controller CON die Verbindung vom Gateway GWA nicht direkt zu dem angerufenen Telekommunikationsendgerät TEB auf, wie es üblicherweise der Fall ist, sondern schleift den Überwachungsserver PRO ein. D. h. die Verbindung von dem ersten Telekommunikationsendgerät TEA zu dem zweiten Telekommunikationsendgerät TEB wird in zwei Strecken zerlegt, nämlich in die Strecke von dem ersten Telekommunikationsendgerät TEA zum Überwachungsserver PRO und in die Strecke von dem Überwachungsserver PRO zu dem zweiten Telekommunikationsendgerät TEB.

[0067] Der Controller CON steuert im Normalfall das erste Gateway GWA. Da aber nun wegen der Überwachung der Zugang zum Datennetz WWW bis zu dem Überwachungsserver PRO verlängert wird und dort eigentlich erst das normale Routing für den Datenstrom DAT des Benutzers BEA anfängt, ist der Controller CON dazu eingerichtet, einen "Handover" vom Gateway zu dem Überwachungsserver durchführen. D. h. der Controller CON wird durch den ersten Zugangsserver AAA informiert, dass ein Überwachungsfall vorliegt und der Datenzugang ZUG des zu überwachenden Telekommunikationsendgerätes TEA zu einem Überwachungsserver PRO durchzutunneln ist. Der Controller betrachtet den Überwachungsserver PRO von nun an als "neues" erstes Gateway GWA und steuert diesen Server als ob es das Gateway GWA wäre. Im Überwachungsfall verhält sich der Call-Controller CON also so, als ob der Überwachungsserver PRO das Gateway GWA wäre, dies gilt sowohl für die rufende als auch die gerufene Seite.

[0068] Der Überwachungsserver PRO erstellt dann, wie bereits oben erwähnt, eine Kopie KOP des Datenstromes DAT zwischen den beiden Telekommunikationsendgeräten TEA, TEB. Zur Erstellung der Kopie KOP wird der ursprüngliche Datenstrom DAT in dem Überwachungsserver PRO verdoppelt. Der ursprüngliche Datenstrom DAT wird nach der Verdoppelung von dem Überwachungsserver PRO an das zweite Telekommunikationsendgerät TEB weitergeroutet, während die Kopie KOP des Datenstromes DAT, wie bereits oben erwähnt, an einen LI-Server oder eine Auswerteeinheit ASW übermittelt wird.

[0069] Der Überwachungsserver PRO als auch der LI-Server LIS können dazu eingerichtet sein, die Kopie KOP zwischenzuspeichern, um für den Fall, dass eine unmittelbare Zustellung an die Auswerteeinheit ASW nicht möglich ist, einen Datenverlust zu vermeiden.

[0070] Um ein Abhören ohne merkliche Beeinträchtigung der Qualität und der Geschwindigkeit des ursprüng-

lichen Datenstroms DAT zu verwirklichen, sollte die Strecke zwischen dem Überwachungsserver PRO und dem Gateway GWA gering sein, weshalb es vorteilhaft ist, wenn eine große Anzahl von Überwachungsservern PRO in dem Datennetz WWW angeordnet sind.

[0071] Soll der angerufene Benutzer BEB überwacht werden erfolgt das Verfahren im wesentlichen so wie oben beschrieben, wobei der zweite Zugangsserver AAB anhand der IP-Adresse des gerufenen Teilnehmers BEB die Authentifizierung durchführen kann und den Datenstrom DAT über den Überwachungsserver PRO umleitet.

[0072] Zu Zweck der Authentifizierung des gerufenen Teilnehmers BEB anhand seiner IP-Adresse kann der zweite Zugangsserver AAB eine Datenbank DAB aufweisen, welche die IP-Adresse des gerufenen Teilnehmers und einen Eintrag ob dieser abgehört werden soll enthält.

[0073] Der Befehl zur Überwachung des Benutzers BEA von einer zur Überwachung berechtigten Behörde gegeben und in der versteckten Datenbank DBA eingetragen.

[0074] Wenn der überwachte Benutzer BEA eine Applikation zur Datenübertragung in dem Datennetz WWW auf seinem Telekommunikationsendgerät startet, erfolgt die Authentifizierung des Benutzers und die Feststellung ob ein Überwachungsfall vorliegt, wie bereits oben erwähnt.

[0075] Der A-Seite wird in einem Überwachungsfall anstelle der Adresse des gerufenen Benutzers BEB bzw. einer Telekommunikationseinrichtung TEB SER, wie beispielsweise einem Server, auf dem eine Homepage oder andere Daten abgelegt sind, die Adresse des Überwachungsservers PRO übermittelt. Das B-seitige Gateway GWB erhält von dem Authentifizierungsserver AAA oder Call-Controller CON anstelle der Netzwerkadresse des rufenden Benutzers BEA die Netzwerkadresse des Überwachungsservers PRO.

[0076] Der Überwachungsserver PRO wird von dem Authentifizierungsserver AAA oder Call Controler CON informiert, dass eine Überwachung stattfinden soll. Alle zur Überwachung und Verbindung notwendigen Informationen, z. B. "Verbinde die A-Seite mit der B-Seite" und ähnliche Informationen, können mittels H.248 Übertragung von dem Authentifizierungsserver AAA bzw. Call-Controler CON an den Überwachungsserver PRO übertragen werden.

[0077] In dem Überwachungsserver wird, wie bereits oben erwähnt,der Datenstrom DAT zwischen dem A-seitigen und B-seitigen Benutzer bzw. Server verdoppelt, wobei die verdoppelten Daten mit einer Identifikationskennzeichnung IDK versehen werden. Die so erstellte Kopie KOP wird in weiterer Folge an den LI-Server übermittelt.

[0078] Für den originalen Datenstrom funktioniert der Überwachungsserver wie ein Proxyserver und verbindet lediglich die A-Seite mit der B-Seite.

[0079] Eine andere Variante der Erfindung sieht vor, dass die A-Seite von dem Authentifizierungsserver AAA oder Call-Controler CON die Netzwerkadresse der B-Seite erhält, wobei das A-seitige Gateway mittels H. 248-Übertragung dazu aufgefordert wird, den gesamten Datenverkehr, der von dem Benutzer BEA stammt, zu dem Überwachungsserver zu tunneln. Hierbei wird der B-Seite, deren Netzwerkadresse bekannt ist anstelle der Netzwerkadresse der A-Seite von dem Call-Controler die Adresse des Überwachungsservers PRO übermittelt.

[0080] Der Überwachungsserver PRO erhält von dem Call-Controler die entsprechenden Informationen für das Tunnneln und verbindet die A-Seite mit der B-Seite.

[0081] Die Vorteile des Tunnelns bestehen darin, dass für den überwachten Benutzer BEA die für das Umleiten des Datenstroms über den Überwachungsserver PRO notwendigen Adressänderungen nicht sichtbar sind.

[0082] Wenn der Überwachungsserver PRO von dem Authentifizierungsserver AAA, AAB oder dem Call-Controler über eine H.248 Kommunikation informiert wird, dass ein Datenstrom DAT umgeleitet wird, so kann er eine Startnachricht an den LI-Server übermitteln, sodass dieser die notwendigen Daten aus der LI-Datenbank LID abfragt und diese bei eintreffen der Kopie KOP schon zur Verfügung stehen.

[0083] Wenn der zu überwachende Datenaustausch beendet wird, dann informiert der Call-Controler CON den Überwachungsserver PRO, dass er die Kommunikation bezüglich der konkreten Überwachung mit dem LI-Server abbrechen soll. Nach Erhalt einer von dem Überwachungsserver PRO stammenden Beendigungsnachricht kann der LI-Server die aus LI-Datenbank stammenden Daten wieder löschen und die Kommunikation mit den Bedarfsträgern einstellen.

Patentansprüche

1. Verfahren zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB), wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
   dadurch gekennzeichnet, dass von dem zumindest einem Authentifikationsserver (AAA, AAB) überprüft wird, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) erstellt wird, welcher eine Identifikationskennzeichnung (IDK) beigefügt wird, und die Kopie samt Identifikationskennzeichnung (IDK) hierauf an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) übermittelt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass die Kopie (KOP) von dem Gateway (GWA, GWB) erstellt wird.

3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver (PRO) erstellt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass der LI-Server anhand der Identifikationskennzeichnung (IDK) feststellt, ob zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll(en).

5. Verfahren nach Anspruch 4,
dadurch gekennzeichnet, dass der LI-Server (LIS) die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt.

6. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet, dass der LI-Server (LIS) eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchführt.

7. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) anhand einer dem zumindest einem Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB)zugeordneten Überwachungskennzeichnung (UWD) feststellt, ob ein Überwachungsfall vorliegt.

8. Verfahren nach Anspruch 6,
dadurch gekennzeichnet, dass die verborgene Datenbank (DBA, DBB) mit einer Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung steht und jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenem Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet wird.

9. Verfahren nach Anspruch 7,
dadurch gekennzeichnet, dass im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwachungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) gelöscht werden.

10. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet, dass der Datenstrom (DAT) als Voice over IP-Datenstrom übertragen wird.

11. Verfahren nach Anspruch 9,
dadurch gekennzeichnet, dass ein Call-Controller (CON) den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet, der die Kopie (KOP) erstellt.

12. Verfahren nach Anspruch 3 bis 10,
dadurch gekennzeichnet, dass der Authentifizierunsserver (AAA, AAB) in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet.

13. Verfahren nach einem der Ansprüche 3 bis 11,
dadurch gekennzeichnet, dass der Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchgetunnelt wird.

14. Verfahren nach einem der Ansprüche 3 bis 12,
dadurch gekennzeichnet, dass die Kopie (KOP) des Datenstroms (DAT) auf dem Überwachungsserver (PRO) zwischengespeichert werden.

15. Verfahren nach einem der Ansprüche 1 bis 11,
dadurch gekennzeichnet, dass die Kopie des Datenstroms (DAT) auf dem LI-Server zwischengespeichert wird.

16. Verfahren nach einem der Ansprüche 10 bis 14,
dadurch gekennzeichnet, dass der Controller (CON) sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) steuert.

17. Verfahren nach einem der Ansprüche 11 bis 14,
dadurch gekennzeichnet, dass der zumindest eine Authentifizierungsserver (AAA, AAB) den Überwachungsserver steuert.

18. Telekommunikationssystem, welches zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB) eingerichtet ist, wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
dadurch gekennzeichnet, dass der Authentifikationsserver (AAA, AAB) dazu eingerichtet ist, zu überprüfen, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei das Telekommunikationssystem (SYS) dazu eingerichtet ist, in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) zu erstellen und der Kopie (KOP) eine Identifikationskennzeichnung

(IDK) hinzuzufügen und die Kopie (KOP) samt Identifikationskennzeichnung (IDK) an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) zu übermitteln.

19. Telekommunikationssystem nach Anspruch 17, **dadurch gekennzeichnet, dass** das Gateway (GWA, GWB) dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zu erstellen.

20. Telekommunikationssystem nach Anspruch 17, **dadurch gekennzeichnet, dass** ein Überwachungsserver (PRO) vorgesehen ist, der dazu eingerichtet ist die Kopie (KOP) zu erstellen.

21. Telekommunikationssystem nach einem der Ansprüche 17 bis 19, **dadurch gekennzeichnet, dass** der LI-Server dazu eingerichtet ist, anhand der Identifikationskennzeichnung (IDK) festzustellen, ob zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll (en).

22. Telekommunikationssystem nach Anspruch 21, **dadurch gekennzeichnet, dass** der LI-Server dazu eingerichtet ist, die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) zu erstellen.

23. Telekommunikationssystem nach einem der Ansprüche 17 bis 22, **dadurch gekennzeichnet, dass** der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchzuführen.

24. Telekommunikationssystem nach einem der Ansprüche 17 bis 23, **dadurch gekennzeichnet, dass** der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, anhand einer dem zumindest einen Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB)zugeordneten Überwachungskennzeichnung (UWD) festzustellen, ob ein Überwachungsfall vorliegt.

25. Telekommunikationssystem nach Anspruch 24, **dadurch gekennzeichnet, dass** die verborgene Datenbank (DBA, DBB) und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten dazu eingerichtet sind Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenen Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet ist.

26. Telekommunikationssystem nach Anspruch 25, **dadurch gekennzeichnet, dass** es dazu eingerichtet ist, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwachungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) zu löschen.

27. Telekommunikationssystem nach einem der Ansprüche 17 bis 26, **dadurch gekennzeichnet, dass** der Datenstrom (DAT) ein Voice over IP-Datenstrom ist.

28. Telekommunikationssystem nach Anspruch 27, **dadurch gekennzeichnet, dass** ein Call-Controller (CON) vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

29. Telekommunikationssystem nach einem der Ansprüche 20 bis 28, **dadurch gekennzeichnet, dass** der Authentifizierunsserver (AAA, AAB) dazu eingerichtet ist, in einem überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

30. Telekommunikationssystem nach einem der Ansprüche 20 bis 29, **dadurch gekennzeichnet, dass** es dazu eingerichtet ist, den Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchzutunneln.

31. Telekommunikationssystem nach einem der Ansprüche 20 bis 30, **dadurch gekennzeichnet, dass** der Überwachungsserver dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

32. Telekommunikationssystem nach einem der Ansprüche 17 bis 31, **dadurch gekennzeichnet, dass** der LI-Server dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

33. Telekommunikationssystem nach einem der Ansprüche 28 bis 32, **dadurch gekennzeichnet, dass** der Call-Controller (CON) dazu eingerichtet ist, sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) zu steuern.

34. Telekommunikationssystem nach einem der Ansprüche 29 bis 32, **dadurch gekennzeichnet, dass** der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, den Überwachungsserver zu steuern.

35. Telekommunikationssystem nach einem der Ansprüche 20 bis 34,
dadurch gekennzeichnet, dass der Überwachungsserver (PRO) die Funktionalität eines Proxy-Servers aufweist.

Claims

1. Method for monitoring a data stream (DAT) in a data network (WWW) between at least one telecommunications terminal (TEA) connected to the data network (WWW) via at least one gateway (GWA, GWB), and at least one other telecommunications device (SER, TEB), at least one authentication server (AAA, AAB) being provided which is set up to perform access control (ZUG) to the data network (WWW),
characterised in that a check is performed by the authentication server (AAA, AAB), of which there is at least one, to determine whether the data stream (DAT) between the telecommunications terminal (TEA), of which there is at least one, and the other telecommunications device (SER, TEB), of which there is at least one, is to be monitored. If this is the case, a copy (KOP) of the data stream (DAT) is created to which an identifying designation (IDK) is added, and the copy together with the associated identifying designation (IDK) is transmitted to at least one LI server (LIS) and/or directly to an analyser unit (ASW).

2. Method according to claim 1,
characterised in that the copy (KOP) is created by the gateway (GWA, GWB).

3. Method according to claim 1,
characterised in that the copy is created by a dedicated monitoring server (PRO).

4. Method according to one of claims 1 to 3,
characterised in that the LI server establishes on the basis of the identifying designation (IDK) whether at least one secondary copy (WKO) of the copy (KOP) is to be created, and to whom the copy (KOP) and/or the secondary copy (WKO), of which there is at least one, is/are to be delivered.

5. Method according to claim 4,
characterised in that the LI server (LIS) creates the secondary copy (WKO), of which there is at least one, of the copy (KOP).

6. Method according to one of claims 1 to 4,
characterised in that the LI server (LIS) performs interface adaptation to the analyser unit (ASW).

7. Method according to one of claims 1 to 5,
characterised in that the authentication server (AAA, AAB) establishes whether monitoring is to take place on the basis of a monitoring designation (UWD) assigned to the telecommunications terminal (TEA), of which there is at least one, and contained in a hidden database (DBA, DBB).

8. Method according to claim 6,
characterised in that the hidden database (DBA, DBB) is linked to an administration database (VDA, VDB) for administering user profile and user authentication data and that a monitoring designation (UWD) contained in the hidden database (DBA, DBB) is assigned to each user (BEA, BEB) entered in the administration database (VDA, VDB).

9. Method according to claim 7,
characterised in that in the event of deletion of user authentication data in the administration database (VWA, VWB), assigned monitoring designations (UWD) are deleted in the hidden database (DBA, DBB).

10. Method according to one of claims 1 to 6,
characterised in that the data stream (DAT) is transmitted as a Voice over IP data stream.

11. Method according to claim 9,
characterised in that a call controller (CON) diverts the data stream (DAT) via the monitoring server (PRO) which creates the copy (KOP).

12. Method according to claim 3 to 10,
characterised in that, if monitoring is to take place, the authentication server (AAA, AAB) diverts the data stream (DAT) via the monitoring server (PRO).

13. Method according to one of claims 3 to 11,
characterised in that the data access (ZUG) is tunnelled from the gateway (GWA, GWB) through to the monitoring server (PRO).

14. Method according to one of claims 3 to 12,
characterised in that the copy (KOP) of the data stream (DAT) is buffered on the monitoring server (PRO).

15. Method according to one of claims 1 to 11,
characterised in that the copy of the data stream (DAT) is buffered on the LI server.

16. Method according to one of claims 10 to 14, **characterised in that** the controller (CON) controls both the gateway (GWA, GWB) and the monitoring server (PRO).

17. Method according to one of claims 11 to 14, **characterised in that** the authentication server (AAA, AAB), of which there is at least one, controls the mon-

itoring server.

18. Telecommunications system which is set up for monitoring a data stream (DAT) in a data network (WWW) between at least one telecommunications terminal (TEA) connected to the data network (WWW) via at least one gateway (GWA, GWB), and at least one other telecommunications device (SER, TEB), at least one authentication server (AAA, AAB) being provided which is set up to perform access control (ZUG) to the data network (WWW),
characterised in that the authentication server (AAA, AAB) is set up to check whether the data stream (DAT) between the telecommunications terminal (TEA), of which there is at least one, and the other telecommunications device (SER, TEB), of which there is at least one, is to be monitored. If this is the case, the telecommunications system (SYS) is set up to create a copy (KOP) of the data stream (DAT) and to add an identifying designation (IDK) to the copy (KOP) and to transmit the copy (KOP) and associated identifying designation (IDK) to at least one LI server (LIS) and/or directly to an analyser unit (ASW).

19. Telecommunications system according to claim 17, **characterised in that** the gateway (GWA, GWB) is set up to create the copy (KOP) of the data stream (DAT).

20. Telecommunications system according to claim 17, **characterised in that** a monitoring server (PRO) is provided which is set up to create the copy (KOP).

21. Telecommunications system according to one of claims 17 to 19,
characterised in that the LI server is set up to establish, on the basis of the identifying designation (IDK), whether at least one secondary copy (WKO) of the copy (KOP) is to be created, and to whom the copy (KOP) and/or the secondary copy (WKO), of which there is at least one, is/are to be delivered.

22. Telecommunications system according to claim 21, **characterised in that** the LI server is set up to create the secondary copy (WKO), of which there are at least one, of the copy (KOP).

23. Telecommunications system according to one of claims 17 to 22,
characterised in that the LI server is set up to perform an interface adaptation to the analyser unit (ASW).

24. Telecommunications system according to one of claims 17 to 23,
characterised in that the authentication server (AAA, AAB) is set up to establish, on the basis of a monitoring designation (UWD) assigned to the telecommunications terminal (TEA), of which there is at least one, in a hidden database (DBA, DBB), whether monitoring is to take place.

25. Telecommunications system according to claim 24, **characterised in that** the hidden database (DBA, DBB) and an administration database (VDA, VDB) for administering user profiles and user authentication data and assigned to the authentication server are set up to exchange data with one another, every user (BEA, BEB) entered in the administration database (VDA, VDB) being assigned a monitoring designation (UWD) in the hidden database (DBA, DBB).

26. Telecommunications system according to claim 25, **characterised in that** it is set up to delete assigned monitoring designations (UWD) in the hidden database (DBA, DBB) in the event of user authentication data being deleted in the administration database (VWA, VWB).

27. Telecommunications system according to one of claims 17 to 26,
characterised in that the data stream (DAT) is a Voice over IP data stream.

28. Telecommunications system according to claim 27, **characterised in that** a call controller (CON) is provided which is set up to divert the data stream (DAT) via the monitoring server (PRO) if monitoring is to take place.

29. Telecommunications system according to one of claims 20 to 28,
characterised in that the authentication server (AAA, AAB) is set up to divert the data stream (DAT) via the monitoring server (PRO) if monitoring is to take place.

30. Telecommunications system according to one of claims 20 to 29,
characterised in that it is set up to tunnel the data access (ZUG) from the gateway (GWA, GWB) through to the monitoring server (PRO).

31. Telecommunications system according to one of claims 20 to 30,
characterised in that the monitoring server is set up to buffer the copy (KOP) of the data stream (DAT).

32. Telecommunications system according to one of claims 17 to 31,
characterised in that the LI server is set up to buffer the copy (KOP) of the data stream (DAT).

33. Telecommunications system according to one of claims 28 to 32,

characterised in that the call controller (CON) is set up to control both the gateway (GWA, GWB) and the monitoring server (PRO).

34. Telecommunications system according to one of claims 29 to 32,
characterised in that the authentication server (AAA, AAB) is set up to control the monitoring server.

35. Telecommunications system according to one of claims 20 to 34,
characterised in that the monitoring server (PRO) has proxy server functionality.

Revendications

1. Procédé pour surveiller un flux de données (DAT) dans un réseau de données (WWW) entre au moins un terminal de télécommunications (TEA) qui est relié au réseau de données (WWW) via au moins une passerelle (GWA, GWB) et au moins un autre dispositif de télécommunications (SER, TEB), au moins un serveur d'authentification (AAA, AAB) étant prévu, lequel est aménagé pour effectuer un contrôle d'accès (ZUG) au réseau de données (WWW), **caractérisé en ce que** l'au moins un serveur d'authentification (AAA, AAB) vérifie si le flux de données (DAT) entre l'au moins un terminal de télécommunications (TEA) et l'au moins un autre dispositif de télécommunications (SER, TEB) doit être surveillé, une copie (KOP) du flux de données (DAT) à laquelle est annexé un marqueur d'identification (IDK) étant créée, dans un cas de surveillance, et la copie, avec le marqueur d'identification (IDK), étant ensuite transmise à l'au moins un serveur LI (LIS) et/ou directement à une unité d'évaluation (ASW).

2. Procédé selon la revendication 1, **caractérisé en ce que** la copie (KOP) est créée par la passerelle (GWA, GWB).

3. Procédé selon la revendication 1, **caractérisé en ce que** la copie est créée par un serveur de surveillance (PRO) expressément prévu à cet effet.

4. Procédé selon l'une des revendications 1 à 3, **caractérisé en ce que** le serveur LI constate, à l'aide du marqueur d'identification (IDK), s'il y a lieu de créer au moins une copie secondaire (WKO) de la copie (KOP) et à qui la copie (KOP) et/ou l'au moins une copie secondaire (WKO) doit (doivent) être notifiée(s).

5. Procédé selon la revendication 4, **caractérisé en ce que** le serveur LI (LIS) crée l'au moins une copie secondaire (WKO) de la copie (KOP).

6. Procédé selon l'une des revendications 1 à 4, **caractérisé en ce que** le serveur LI (LIS) effectue une adaptation de l'interface à l'unité d'évaluation (ASW).

7. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** le serveur d'authentification (AAA, AAB), à l'aide d'un marqueur de surveillance (UWD) affecté à l'au moins un terminal de télécommunications (TEA) dans une base de données cachée (DBA, DBB), constate s'il y a cas de surveillance.

8. Procédé selon la revendication 6, **caractérisé en ce que** la base de données cachée (DBA, DBB) est en contact avec une base de données administratives (VDA, VDB) pour gérer des profils d'utilisateurs et des données d'authentification d'utilisateurs, et un marqueur de surveillance (UWD) est affecté, dans la base de données cachée (DBA, DBB), à chaque utilisateur (BEA, BEB) enregistré dans la base de données administratives (VDA, VDB).

9. Procédé selon la revendication 7, **caractérisé en ce que**, en cas d'effacement de données d'authentification d'utilisateurs dans la base de données administratives (VWA, VWB), des marqueurs de surveillance (UWD) associés sont également effacés dans la base de données cachée (DBA, DBB).

10. Procédé selon l'une des revendications 1 à 6, **caractérisé en ce que** le flux de données (DAT) est transmis en tant que flux de données «Voice over IP».

11. Procédé selon la revendication 9, **caractérisé en ce qu'**un contrôleur d'appels (CON) dévie le flux de données (DAT) via le serveur de surveillance (PRO) qui crée la copie (KOP).

12. Procédé selon l'une des revendications 3 à 10, **caractérisé en ce que** le serveur d'authentification (AAA, AAB), dans un cas de surveillance, dévie le flux de données (DAT) via le serveur de surveillance (PRO).

13. Procédé selon l'une des revendications 3 à 11, **caractérisé en ce que** l'accès de données (ZUG) est tunnelé de la passerelle (GWA, GWB) vers le serveur de surveillance (PRO).

14. Procédé selon l'une des revendications 3 à 12, **caractérisé en ce que** la copie (KOP) du flux de données (DAT) est stockée temporairement sur le serveur de surveillance (PRO).

15. Procédé selon l'une des revendications 1 à 11, **caractérisé en ce que** la copie du flux de données

(DAT) est stockée temporairement sur le serveur LI.

16. Procédé selon l'une des revendications 10 à 14, **caractérisé en ce que** le contrôleur (CON) commande non seulement la passerelle (GWA, GWB), mais aussi le serveur de surveillance (PRO).

17. Procédé selon l'une des revendications 11 à 14, **caractérisé en ce que** l'au moins un serveur d'authentification (AAA, AAB) commande le serveur de surveillance.

18. Système de télécommunications, aménagé pour surveiller un flux de données (DAT) dans un réseau de données (WWW) entre au moins un terminal de télécommunications (TEA) qui est relié au réseau de données (WWW) via au moins une passerelle (GWA, GWB) et au moins un autre dispositif de télécommunications (SER, TEB), au moins un serveur d'authentification (AAA, AAB) étant prévu, lequel est aménagé pour effectuer un contrôle d'accès (ZUG) au réseau de données (WWW), **caractérisé en ce que** le serveur d'authentification (AAA, AAB) est aménagé pour vérifier s'il y a lieu de surveiller le flux de données (DAT) entre l'au moins un terminal de télécommunications (TEA) et l'au moins un autre dispositif de télécommunications (SER, TEB), le système de télécommunications (SYS) étant aménagé pour, dans un cas de surveillance, créer une copie (KOP) du flux de données (DAT), ajouter un marqueur d'identification (IDK) à la copie (KOP) et transmettre la copie (KOP), avec le marqueur d'identification (IDK), à au moins un serveur LI (LIS) et/ou directement à une unité d'évaluation (ASW).

19. Système de télécommunications selon la revendication 17, **caractérisé en ce que** la passerelle (GWA, GWB) est aménagée pour créer la copie (KOP) du flux de données (DAT).

20. Système de télécommunications selon la revendication 17, **caractérisé en ce qu'**est prévu un serveur de surveillance (PRO) qui est aménagé pour créer la copie (KOP).

21. Système de télécommunications selon l'une des revendications 17 à 19, **caractérisé en ce que** le serveur LI est aménagé pour constater, à l'aide du marqueur d'identification (IDK), s'il y a lieu de créer au moins une copie secondaire (WKO) de la copie (KOP) et à qui la copie (KOP) et/ou l'au moins une copie secondaire (WKO) doit (doivent) être notifiée (s).

22. Système de télécommunications selon la revendication 21, **caractérisé en ce que** le serveur LI est aménagé pour créer l'au moins une copie secondaire (WKO) de la copie (KOP).

23. Système de télécommunications selon l'une des revendications 17 à 22, **caractérisé en ce que** le serveur LI est aménagé pour effectuer une adaptation de l'interface à l'unité d'évaluation (ASW).

24. Système de télécommunications selon l'une des revendications 17 à 23, **caractérisé en ce que** le serveur d'authentification (AAA, AAB) est aménagé pour constater, à l'aide d'un marqueur de surveillance (UWD) affecté à l'au moins un terminal de télécommunications (TEA) dans une base de données cachée (DBA, DBB), s'il y a cas de surveillance.

25. Système de télécommunications selon la revendication 24, **caractérisé en ce que** la base de données cachée (DBA, DBB) et une base de données administratives (VDA, VDB) associée au serveur d'authentification pour gérer des profils d'utilisateurs et des données d'authentification d'utilisateurs sont aménagées pour échanger des données entre elles, un marqueur de surveillance (UWD) étant, dans la base de données cachée (DBA, DBB), affecté à chaque utilisateur (BEA, BEB) enregistré dans la base de données administratives (VDA, VDB).

26. Système de télécommunications selon la revendication 25, **caractérisé en ce qu'**il est aménagé pour, en cas d'effacement de données d'authentification d'utilisateurs dans la base de données administratives (VWA, VWB), effacer des marqueurs de surveillance (UWD) associés dans la base de données cachée (DBA, DBB).

27. Système de télécommunications selon l'une des revendications 17 à 26, **caractérisé en ce que** le flux de données (DAT) est un flux de données «Voice over IP».

28. Système de télécommunications selon la revendication 27, **caractérisé en ce qu'**est prévu un contrôleur d'appels (CON) qui est aménagé pour, dans un cas de surveillance, dévier le flux de données (DAT) via le serveur de surveillance (PRO).

29. Système de télécommunications selon l'une des revendications 20 à 28, **caractérisé en ce que** le serveur d'authentification (AAA, AAB) est aménagé pour, dans un cas de surveillance, dévier le flux de données (DAT) via le serveur de surveillance (PRO).

30. Système de télécommunications selon l'une des revendications 20 à 29, **caractérisé en ce qu'**il est aménagé pour tunneler l'accès de données (ZUG) de la passerelle (GWA, GWB) vers le serveur de surveillance (PRO).

31. Système de télécommunications selon l'une des revendications 20 à 30, **caractérisé en ce que** le ser-

veur de surveillance est aménagé pour stocker temporairement la copie (KOP) du flux de données (DAT) .

32. Système de télécommunications selon l'une des revendications 17 à 31, **caractérisé en ce que** le serveur LI est aménagé pour stocker temporairement la copie (KOP) du flux de données (DAT) .

33. Système de télécommunications selon l'une des revendications 28 à 32, **caractérisé en ce que** le contrôleur d'appels (CON) est aménagé pour commander non seulement la passerelle (GWA, GWB), mais aussi le serveur de surveillance (PRO).

34. Système de télécommunications selon l'une des revendications 29 à 32, **caractérisé en ce que** le serveur d'authentification (AAA, AAB) est aménagé pour commander le serveur de surveillance.

35. Système de télécommunications selon l'une des revendications 20 à 34, **caractérisé en ce que** le serveur de surveillance (PRO) comporte la fonctionnalité d'un serveur proxy.

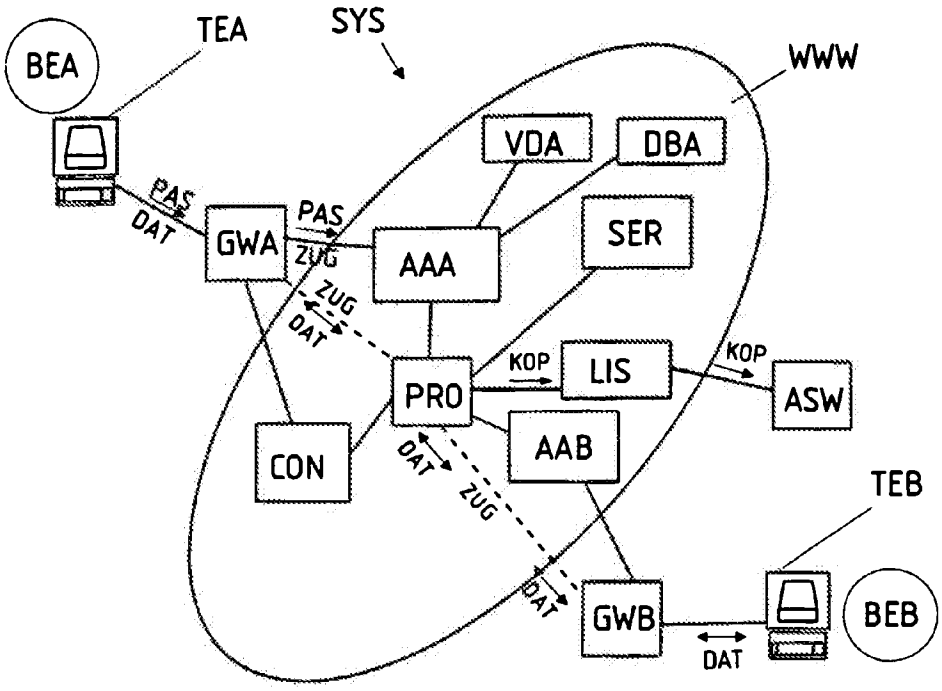


Fig. 1

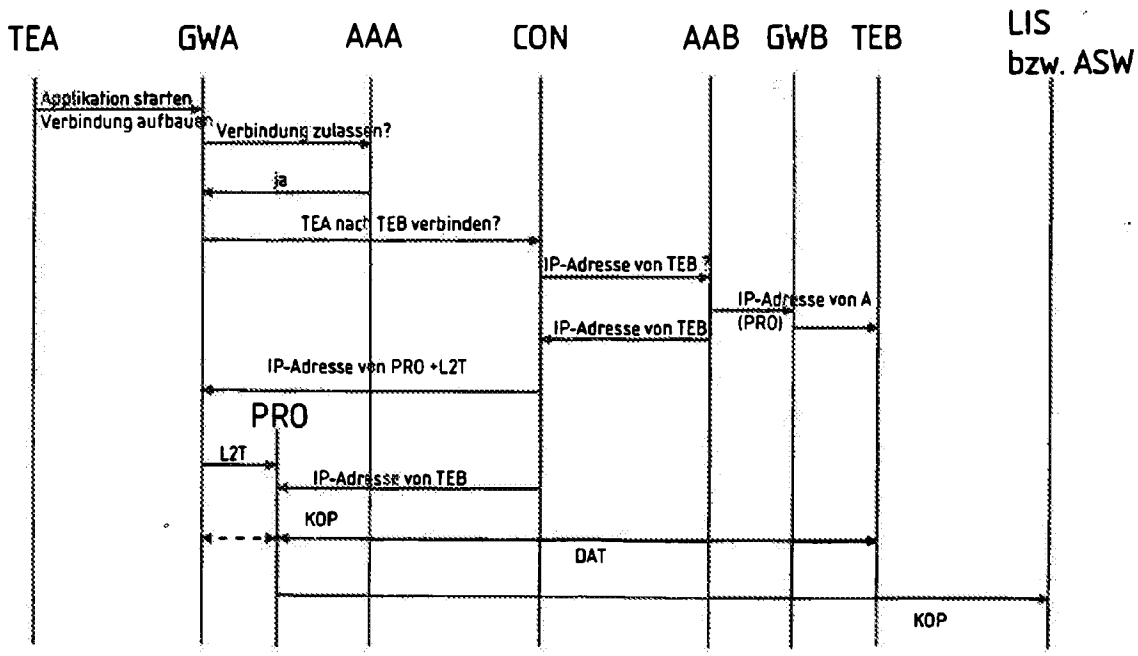


Fig. 3

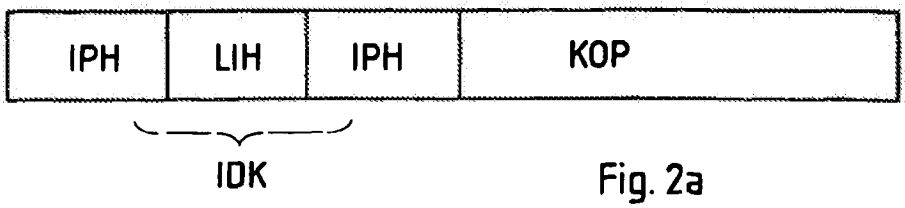


Fig. 2a

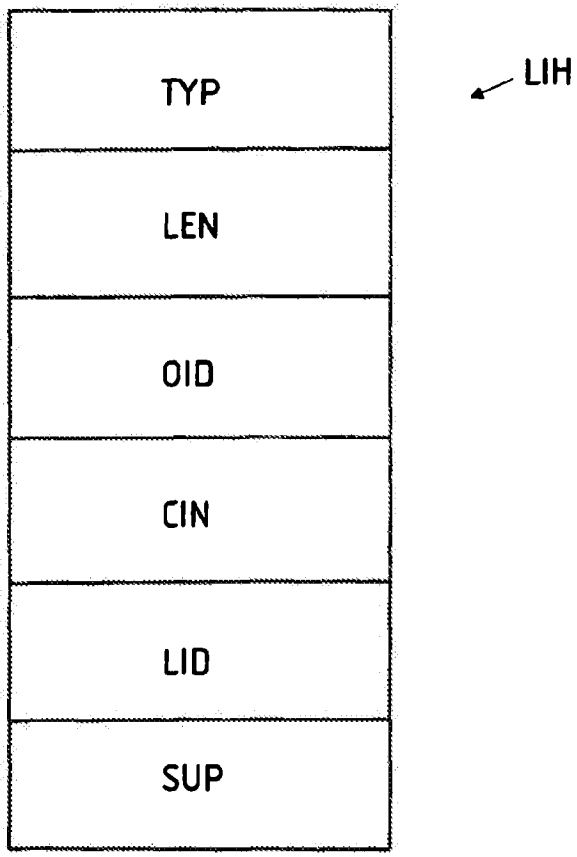


Fig. 2b

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- WO 0042742 A **[0007]**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 411 743 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.11.2007 Bulletin 2007/48

(21) Application number: **03256372.8**

(22) Date of filing: **09.10.2003**

(51) Int Cl.:
H04Q 7/38 *(2006.01)* ***H04M 11/04*** *(2006.01)*

(54) **An emergency call back method**

Verfahren für einen Notfall Rückruf

Procedé de rappel d'urgence

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

(30) Priority: **16.10.2002 US 270629**

(43) Date of publication of application:
21.04.2004 Bulletin 2004/17

(73) Proprietor: **Lucent Technologies Inc.**
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventors:
- **Chin, Mary**
  Westmont,
  Illinois 60559 (US)
- **Rollender, Douglas**
  Bridgewater,
  New Jersey 08807 (US)

(74) Representative: **Sarup, David Alexander et al**
Alcatel-Lucent Telecom Limited
Unit 18, Core 3,
Workzone
Innova Business Park
Electric Avenue
Enfield, EN3 7XU (GB)

(56) References cited:
WO-A-00/11879 **US-A- 5 689 548**

- **RICARDO GOMEZ: "Global title translation (GTT) routing " IFAST, vol. 2, no. 1, March 2003 (2003-03), pages 2-3, XP002270040**

EP 1 411 743 B1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

[0001] Emergency service calls in North America are originated by dialing "9-1-1." Other parts of the world may use some other abbreviated string of dialable digits such as "6-1-1" in Mexico; all share the intent to provide the caller with an easy way to call for help with an easy to remember number. These calls are routed to a local Public Service Answering Point (PSAP) where an emergency response may be initiated (police, fire department, road repair, ambulance, etc.) while the caller is kept on the phone. If the call is somehow disconnected or dropped before the emergency is completely reported or the responder arrives, the PSAP may call back the originator using a call back number provided through its databases.

[0002] For example, the call record for a 911 call originated through a wired network may include Automatic Line Identification (ANI) or the telephone number of the access line from which the call originated. However, the mobile directory number (MDN) or telephone number of a wireless subscriber is not associated with a physical line or mobile station. Instead, calls to a wireless subscriber are routed to the mobile station by way of the mobile station identification (MSID), not the MDN. Accordingly, performing an emergency call back to a mobile station poses hurdles not encountered with, e.g., land line devices.

[0003] Typically, the MSID is either a 10-digit mobile identification number (MIN) or a 15-digit International Mobile Subscriber Identifier (IMSI) programmed into a mobile station by the service provider with whom the mobile station user has entered into a service agreement. Accordingly, the MSID is not necessarily a dialable number.

[0004] The MDN of a mobile station is a dialable number. The MDN is dialed by a caller and used to route a call through the network to the wireless subscriber's home system. At the subscriber's home system, the home location register (HLR) contains the MSID associated with the subscriber's MDN. The MSID, not the MDN, is then used to route the call through the network to the serving wireless system and page the subscriber. The subscriber's MDN is provided by the home system to the serving system in a separate data file called the subscriber profile.

[0005] The use of a separate number for MDN and MSID is new to some systems. Historically, in TIA/EIA-41 systems before the implementation of wireless number portability (WNP) or thousands block number pooling (TBNP) based on the Local Routing Number (LRN) method and international roaming (IR), the mobile identification number (MIN) of a mobile station was the same as the MDN. However, with WNP and TBNP, the MDN became "portable" or "poolable" from one service provider to another service provider. Since MSID is not portable or poolable, the recipient service provider assigns a new MSID for a subscriber with a ported-in or pooled MDN.

[0006] International roaming also forced the separation of MSID and MDN. While the MIN is a 10-digit number modeled after the North American Numbering Plan's 10-digit MDN, other nation's carriers using a different directory numbering plan may not allow their MDN to be equivalent to the internationally recognized MIN format. Another standard MSID is the IMSI. It is used in both TIA/EIA-41 and GSM systems around the world. IMSI is a 15-digit number, and therefore, can not serve as a 10-digit MDN.

[0007] Historically, when the MDN was the same as the MIN, the MIN would be delivered to a PSAP and would be used for a call back number. With the separation of MIN and MDN as described above, it became necessary to deliver the MDN as a separate call back number to the PSAP as well as the caller's MSID. There are certain problems associated with implementing this solution. The primary problem is that the serving system may not have the caller's MDN, only the MSID, to present to the PSAP with the call. Some of the reasons for this relate to the way MSID-MDN separation has been implemented according to standards.

[0008] An old serving TIA/EIA-41 system may not support WNP, TBNP or IR. This means that the older serving system may be expecting the MIN and the MDN to be the same. The older system would not even know to look for a separate MDN in the subscriber's service profile (keyed on MIN, not MDN). With this limitation, these subscribers may not be allowed to use basic services, but they must be allowed to call for emergency services. As a result, a roamer who dials "9-1-1" while on an old system will have his or her call delivered to the PSAP with an MSID but no MDN. Accordingly, no call back is possible.

[0009] A newer serving system that is WNP and IR capable may not be able to deliver MDN to the PSAP. This could happen if the calling mobile station is not registered with any service provider (e.g., there are mobile phones used for emergency calls only). It is also possible for a subscriber to place an emergency call before the HLR has responded to the serving system with the subscriber's service profile containing the MDN.

[0010] The call back MDN for an international roamer would require the PSAP to place an international call to reach a subscriber in their local Emergency Service Zone (ESZ). This is not a practical, timely or sufficiently reliable solution for a PSAP that normally does not place international calls and may require immediate call back information in order to save someone's life. In addition, the entire international MDN (up to 15 digits including a country code) may not be presented to the PSAP for callback.

[0011] One proposed solution to these problems calls for delivering 9-1-1+the last 7 digits of the electronic serial number (ESN) of the calling mobile station to the PSAP as the call back number when the MDN is not available. While this may serve to identify the caller to the PSAP and the serving system, this "9-1-1+ESN7" can not be

routed through the network and can not be used to place a call back.

[0012] US-B-5 689 548 discloses an emergency call back using MSC numbers. It discloses including an MSC directory number within the Cdpn between the serving MSC/VLR and the PSAP. The MSC directory number is a common routing tool for routing all types of messaging to and from the MSC.

Summary of the Invention

[0013] Methods according to the invention are as set out in the independent claims. Preferred forms are set out in the dependent claims.

[0014] The call back method according to the present invention assigns an emergency local routing number (ELRN) to each switch in a wireless network. When a switch of the wireless network routes an emergency call to a Public Service Answering Point (PSAP), the switch sends the emergency local routing number as the calling party number (CgPN) and provides the PSAP with the identifier of the mobile station (MSID). If the emergency call drops, the PSAP performs a call back using the emergency routing number as the called party number (CdPN). As a result the switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. This MSID is used to page the correct mobile station. In an embodiment of the present invention, the PSAP signals the mobile station identifier to the switch in a generic address parameter.

[0015] When a switch receives its emergency local routing number as the called party number, the switches recognizes an emergency call back situation and pages the mobile station identified by the mobile station identifier received in association with the emergency routing number. In an embodiment of the present invention, the switch gives higher priority to handling the call back than other tasks when an ELRN is the CdPN. In this manner, the PSAP is reconnected with the mobile station.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] The present invention will become more fully understood from the detailed description given herein below and the accompanying drawings which are given by way of illustration only, wherein like reference numerals designate corresponding parts in the various drawings, and wherein:

[0017] Figs. 1-6 are communication flow diagrams illustrating the operation of the call back method according to the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0018] The call back method according to the present invention assigns a unique routable call back number to each switch (e.g., a mobile switching center (MSC)) in a wireless communication system. This number will be referred to as an "Emergency Local Routing Number" or ELRN hereafter. The ELRN can be thought of as similar to the local routing number (LRN) assigned to each local switch to implement wireless number portability (WNP) or thousands block number pooling (TBNP). However, an ELRN can only be routed to the switch that owns the number, and the ELRN for each switch is unique and is not portable.

[0019] As is known, when a mobile station makes an emergency call, the mobile station identifier (MSID) is supplied in association with the emergency call. For example, the MSID is the mobile identification number (MIN), a ten digit International Roaming Mobile Identification Number (IRM) for those 10 digit numbers outside the range of the North American Numbering Plan, or the International Mobile Subscriber Identifier (IMSI). When a switch of the wireless system receives an emergency call (e.g., a 9-1-1 call) from a mobile station, particularly, a mobile station with no MDN, the switch sends the ELRN of the switch to the Public Service Answering Point (PSAP) serving the switch. The switch supplies ELRN as the calling party number (CgPN), and also provides the PSAP with the MSID of the mobile station. For example, the MSID is signaled such as in the ISUP generic address parameter (GAP).

[0020] If the emergency call drops, the PSAP performs a call back using the ERLN as the called party number (CdPN). As a result, the switch that routed the emergency call from the mobile station to the PSAP receives the call back. The PSAP also sends the identifier of the mobile station to the switch. For example, the MSID is signaled with the call back such as in the ISUP generic address parameter (GAP).

[0021] When a switch receives its emergency routing number as the called party number, the switch recognizes an emergency call back situation and pages the mobile station identified by the MSID received in association with the ERLN and establishes the emergency call back. This ERLN technique may also be provisioned with priority queuing in the switches; wherein the switch handles the call back number at a higher priority than tasks involving other calls. This should improve the emergency call back completion rate even during peak traffic periods at the switch. Furthermore, while described as performed for all emergency calls, use of the method could be limited to just emergency calls made by mobile stations with no or unavailable MDNs.

[0022] Figs. 1-6 are communication flow diagrams illustrating the operation of the call back method according to the present invention. As shown in Fig. 1, a first mobile station MS1 places an emergency call, a 9-1-1 call in this example, that is received by a MSC. Accordingly, the called party number is 9-1-1, and the MSID 1 of the first mobile station MS1 is supplied to the MSC as well. The MSC then routes the emergency call to the serving PSAP. In so doing, the called party number remains 9-1-1, but the MSC supplies its ERLN as the calling party number.

The MSC also supplies the MSID1 of the first mobile station MS1 in the generic address parameter (GAP).

[0023] If the emergency call is dropped, the PSAP performs a call back using the ERLN as the called party number because the ERLN was supplied to the PSAP as the calling party number. The result is that the call back is routed to the MSC as shown in Fig. 2. As further shown in Fig. 2, the MSID 1 of the first mobile station is signaled with the call back in the ISUP GAP. As shown in Fig. 3, the MSC uses the MSID1 of the first mobile station MS1 to page the first mobile station MS 1 and complete the call back.

[0024] Assume that while the call back to the first mobile station MS1 is in progress, a second mobile station MS2 places a 9-1-1 emergency call as shown in Fig. 4. As with the emergency call from the first mobile station MS1, the second mobile station MS2 supplies its mobile station identifier MSID2 along with the emergency call (e.g., called party number is 9-1-1). Then, the MSC then routes the emergency call to the PSAP. In so doing, the called party number remains 9-1-1, but the MSC supplies its ERLN as the calling party number. The MSC also supplies the MSID2 of the second mobile station MS2 to the PSAP. Accordingly, Fig. 4 demonstrates that the MSC supplies the same calling party number (i.e., the ERLN) to the PSAP for both of the emergency calls.

[0025] If the second emergency call is dropped, the PSAP performs a call back using the ERLN as the called party number because the ERLN was supplied to the PSAP as the calling party number. The result is that a second call back is routed to the MSC as shown in Fig. 5. As further shown in Fig. 5, the MSID2 of the second mobile station is signaled with the second call back in the ISUP GAP. As shown in Fig. 6, the MSC uses the MSID2 of the second mobile station MS2 to page the second mobile station MS2 and complete the call back.

[0026] The emergency call back method of the present invention ensures a routable call back number is provided to a PSAP with every emergency call from a mobile station. Specifically, the ELRN is one number used to route one or many emergency service call backs to the originating switch (e.g., MSC). The ELRN of the originating switch is signaled to the PSAP as the calling party number (CgPN), particularly when there is no local MDN available to accompany an emergency call.

[0027] In the North American Numbering Plan, the ELRN is a 10-digit number (NPA-NXX-XXXX) where the leading 6-digits (NPA-NXX) are uniquely assigned to each local switch in North America for call routing purposes. The subsequent four digits are assigned by the switch operator. However, the emergency call back method is applicable in a public switched network anywhere in the world. Namely, the ELRN contains those digits assigned from any national numbering plan to route calls to a particular switch. Also, the emergency call back method may be applied with any mobile service or wireless access technology.

[0028] The emergency call back method is independent of number portability and number pooling. These network capabilities depend upon the Local Routing Number (LRN) Method to route a call to a serving switch based on the LRN associated with a ported or pooled dialed number. In comparison, the ELRN is not associated with a dialed number, instead it is associated with a switch.

[0029] In some ways, the ELRN functions in the public network like the Local Routing Number (LRN) required for local number portability; for instance, both function as a single number to route many calls to a particular switch. However, no database query is required to identify the ELRN required to route a call to a serving MSC. As a result, when used as the called party number (CdPN) to route a callback from a PSAP to the serving MSC, the ELRN may be accompanied with the ISUP Forward Call Indicator (FCI) set to indicate no number portability database query is required.

[0030] As discussed above, an ELRN is not associated with any particular MDN and is used to route a call back directly to the serving switch, not the home system. The ELRN eliminates the need for the PSAP to use a MDN to place an emergency call back. There is no need to request an MDN or an LRN to route a callback through a home system as per existing mobile application part (MAP) standards. Also, there is no need to place an international call through a foreign home system to call back an international roamer in the local area. This reduces signaling, saves time and improves service reliability. Further, there is no need for a Temporary Long Distance Number (TLDN), as in TIA/EIA-41 networks, or a Mobile Station Routing Number (MSRN), as in GSM networks, to route a call back from the home system to the serving system. This reduces signaling, saves time and places no demand on the supply of TLDNs or MSRNs.

[0031] The invention being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the and scope of the invention, and all such modifications are intended to be included within the scope of the following claims.

Claims

1. An emergency call back method, comprising:

   assigning an emergency routing number to each switch in a wireless network only for use as the calling party number of emergency wireless calls routed to a Public Service Answering Point by each switch;

   sending the emergency routing number of a switch in the wireless network handling communication needs of a mobile station initiating an emergency call and an identifier of the mobile station to a Public Service Answering Point

2. The method of claim 1, wherein each assigned emergency routing number is not portable.

3. An emergency call back method, comprising:

receiving an emergency routing number of a switch in a wireless network handling communication needs of a mobile station initiating an emergency call and an identifier of the mobile station at a Public Service Answering Point, the emergency routing number being assigned only for use as the calling party number of the emergency call; and
initiating a call back to the mobile station at the Public Service Answering Point by calling the emergency routing number when the emergency call made by the mobile station drops, such that the switch receiving the emergency routing number assigned thereto as the called party number in a call recognizes the call as an emergency call back.

4. The method of claim 1, further comprising:

signaling the identifier of the mobile station to the switch when initiating the call back.

5. The method of claim 4, wherein the signaling step sends the identifier of the mobile station in a generic address parameter.

6. An emergency call back method, comprising:

assigning an emergency routing number to each switch in a wireless network only for use as the calling party number of emergency wireless calls routed to a Public Service Answering Point by each switch;
receiving, at a switch of the wireless network, a called party number and a mobile station identifier; and
paging a mobile station identified by the mobile station identifier when the called party number matches the emergency routing number assigned to the switch.

7. The method of claim 6, wherein the receiving step receives the identifier of the mobile station in a generic address parameter.

8. The method of claim 6, wherein the paging step is performed with priority over other tasks at the switch.

9. The method of claim 6, wherein the switch is a mobile switching center.

Patentansprüche

1. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:

Zuweisen einer Not-Leitwegnummer zu jeder Vermittlung in einem drahtlosen Netz nur zur Verwendung als die Rufnummer des Anrufers von durch jede Vermittlung zu einer öffentlichen Dienstabfragestelle geleiteten drahtlosen Notrufen;
Senden der Not-Leitwegnummer einer Vermittlung in dem drahtlosen Netz, die die Kommunikationsbedürfnisse einer Mobilstation bearbeitet, die einen Notruf einleitet, und einer Kennung der Mobilstation zu einer öffentlichen Dienstabfragestelle.

2. Verfahren nach Anspruch 1, wobei jede zugewiesene Not-Leitwegnummer nicht portabel ist.

3. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:

Empfangen einer Not-Leitwegnummer einer Vermittlung in einem drahtlosen Netz, die Kommunikationsbedürfnisse einer einen Notruf einleitenden Mobilstation bearbeitet, und einer Kennung der Mobilstation an einer öffentlichen Dienstabfragestelle, wobei die Not-Leitwegnummer nur zur Verwendung als die Rufnummer des Anrufers des Notrufes zugewiesen wird; und
Einleiten eines Rückrufs zur Mobilstation an der öffentlichen Dienstabfragestelle durch Rufen der Not-Leitwegnummer, wenn der durch die Mobilstation getätigte Notruf abfällt, so daß die die ihr als die Rufnummer des angerufenen in einer Verbindung zugewiesene Not-Leitwegnummer empfangende Vermittlung die Verbindung als einen Notfall-Rückruf erkennt.

4. Verfahren nach Anspruch 1, weiterhin mit folgendem:

Signalisierung der Kennung der Mobilstation an die Vermittlung bei Einleitung des Rückrufs.

5. Verfahren nach Anspruch 4, wobei der Schritt des Signalisierens die Kennung der Mobilstation in einem generischen Adressenparameter sendet.

6. Verfahren für einen Notfall-Rückruf, mit folgenden Schritten:

Zuweisen einer Not-Leitwegnummer zu jeder Vermittlung in einem drahtlosen Netz nur zur Verwendung als die Rufnummer des Anrufers

von zu einer öffentlichen Dienstabfragestelle geleiteten drahtlosen Notrufen durch jede Vermittlung;
Empfangen an einer Vermittlung des drahtlosen Netzes einer Rufnummer des Angerufenen und einer Mobilstationskennung; und
Rufen einer durch die Mobilstationskennung identifizierten Mobilstation, wenn die Rufnummer des Angerufenen der der Vermittlung zugewiesenen Not-Leitwegnummer entspricht.

7. Verfahren nach Anspruch 6, wobei der Schritt des Empfangens die Kennung der Mobilstation in einem generischen Adressenparameter empfängt.

8. Verfahren nach Anspruch 6, wobei der Schritt des Rufens mit Priorität gegenüber anderen Aufgaben an der Vermittlung durchgeführt wird.

9. Verfahren nach Anspruch 6, wobei die Vermittlung eine Mobilvermittlungsstelle ist.

Revendications

1. Procédé de rappel d'urgence, comprenant :

l'assignation d'un numéro de routage d'urgence à chaque commutateur dans un réseau sans fil destiné à n'être utilisé que comme numéro d'appelant d'appels sans fil d'urgence routés jusqu'à un Point de Réponse de Service public par chaque commutateur ;
l'envoi du numéro de routage d'urgence d'un commutateur dans le réseau sans fil prenant en charge les besoins de communication d'une station mobile effectuant un appel d'urgence et d'un identifiant de la station mobile à un Point de Réponse de Service public.

2. Procédé selon la revendication 1, dans lequel aucun numéro de routage d'urgence assigné n'est portable.

3. Procédé de rappel d'urgence, comprenant :

la réception d'un numéro de routage d'urgence d'un commutateur dans un réseau sans fil prenant en charge les besoins de communication d'une station mobile effectuant un appel d'urgence et d'un identifiant de la station mobile au niveau d'un Point de Réponse de Service public, le numéro de routage d'urgence étant assigné uniquement pour être utilisé comme numéro d'appelant de l'appel d'urgence ; et
l'exécution d'un rappel de la station mobile au niveau du Point de Réponse de Service public en appelant le numéro de routage d'urgence quand l'appel d'urgence effectué par la station mobile est perdu, de telle sorte que le commutateur recevant le numéro de routage d'urgence qui lui est assigné comme numéro d'appelé dans un appel reconnaisse l'appel comme un rappel d'urgence.

4. Rappel selon la revendication 1, comprenant en outre :

la signalisation de l'identifiant de la station mobile au commutateur lors de l'exécution du rappel.

5. Procédé selon la revendication 4, dans lequel l'étape de signalisation envoie l'identifiant de la station mobile dans un paramètre d'adresse générique.

6. Procédé de rappel d'urgence, comprenant :

l'assignation d'un numéro de routage d'urgence à chaque commutateur dans un réseau sans fil destiné à n'être utilisé que comme numéro d'appelant d'appels sans fil d'urgence routés jusqu'à un Point de Réponse de Service public par chaque commutateur ;
la réception, au niveau d'un commutateur du réseau sans fil, d'un numéro d'appelé et d'un identifiant de station mobile ; et
l'exécution d'un appel de recherche d'une station mobile identifiée par l'identifiant de station mobile quand le numéro d'appelé correspond au numéro de routage d'urgence assigné au commutateur.

7. Procédé selon la revendication 6, dans lequel l'étape de réception reçoit l'identifiant de la station mobile dans un paramètre d'adresse générique.

8. Procédé selon la revendication 6, dans lequel l'étape d'appel de recherche est exécutée en priorité aux autres tâches au niveau du commutateur.

9. Procédé selon la revendication 6, dans lequel le commutateur est un centre de commutation mobile.

Fig. 1

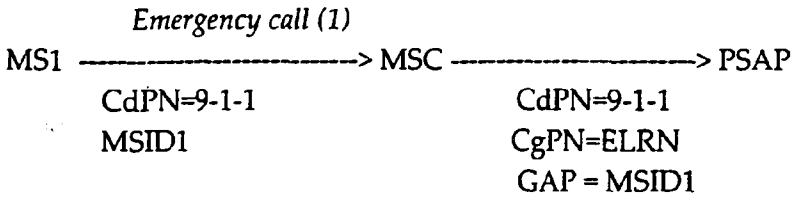


Fig. 2

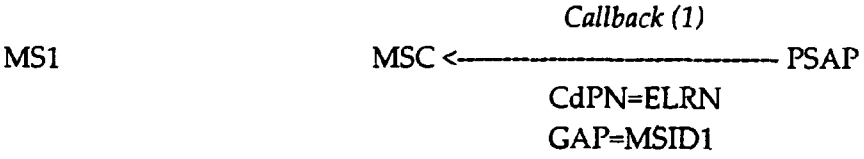


Fig. 3

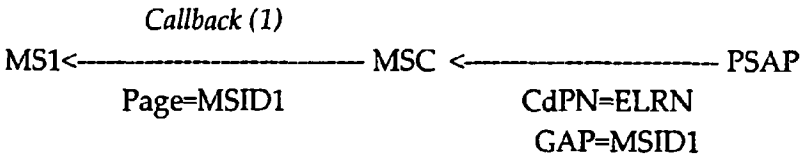


Fig. 4

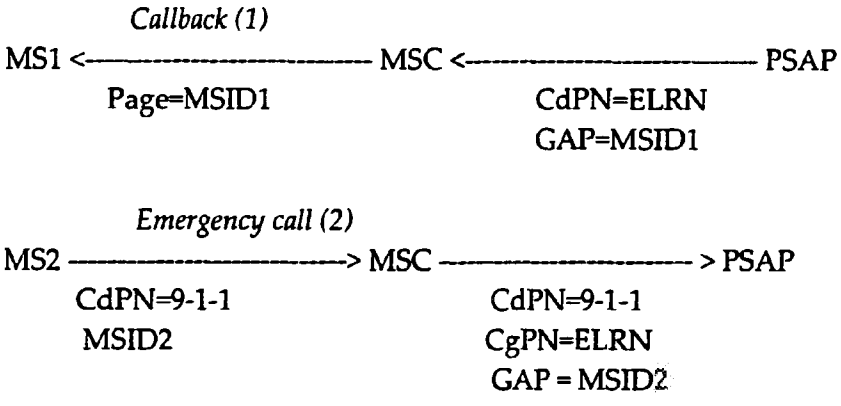


Fig. 5

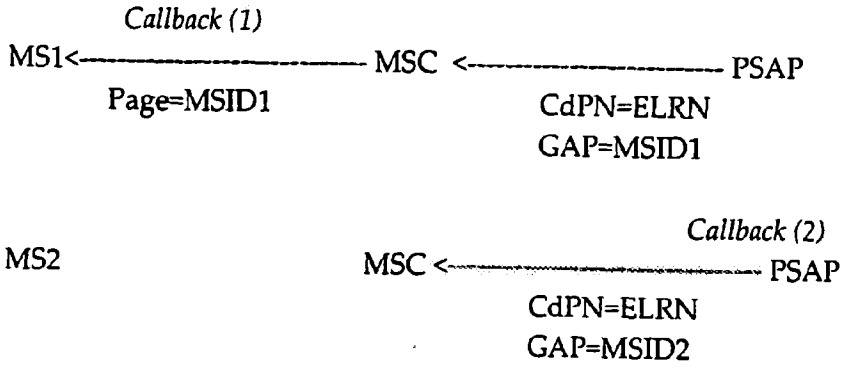
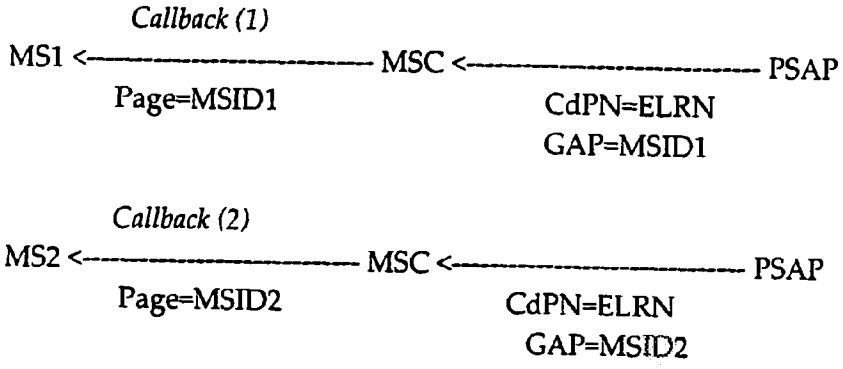


Fig. 6



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5689548 B **[0012]**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 362 456 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
19.03.2008 Bulletin 2008/12

(21) Application number: **01273516.3**

(22) Date of filing: **09.10.2001**

(51) Int Cl.:
H04L 12/56 *(2006.01)*

(86) International application number:
PCT/US2001/031548

(87) International publication number:
WO 2002/082782 (17.10.2002 Gazette 2002/42)

(54) **SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS**

SYSTEM UND VERFAHREN ZUM ABFANGEN VON TELEKOMMUNIKATIONEN

SYSTEME ET PROCEDE D'INTERCEPTION DE TELECOMMUNICATIONS

(84) Designated Contracting States:
DE FR GB

(30) Priority: **10.10.2000 US 239048 P**

(43) Date of publication of application:
19.11.2003 Bulletin 2003/47

(73) Proprietor: **Nortel Networks Limited**
St Laurent, Québec H4S 2A9 (CA)

(72) Inventors:
- **PYKE, Craik, R.**
  Nepean, ON K2H 8A6 (CA)
- **HERN, William**
  Knowl hill, Reading RG 10 9UP (GB)
- **THOMPSON, Roger, L.**
  RTP, NC 27709 (US)
- **CARON, Serge, S.**
  Gatineau, PQ J8V 1X9 (CA)
- **MOUNJI, Halima, H.**
  Kanata, ON K2T 1E2 (CA)
- **EWOTI, Charles, B.**
  88677, Markdorf (DE)
- **GOERENS, Michael**
  88045 Friedrichshafen (DE)
- **STRENG, Pete, J.**
  Manotick, ON K4M 1G5 (CA)
- **GOERTZEN, Christopher, J.**
  Ottawa, ON K1G 6N6 (CA)
- **KITTLITZ, Christian**
  Ottawa, ON K1V 8G1 (CA)
- **TAYLOR, Richard, C.**
  Manotick, ON K4M 1A2 (CA)
- **WELHAM, Michael**
  88662 Lippertsreute (DE)

(74) Representative: **Mackenzie, Andrew Bryan et al**
Scott & York
Intellectual Property Ltd
45 Grosvenor Road
St. Albans
Hertfordshire, AL1 3AW (GB)

(56) References cited:

WO-A-00/42742	**WO-A-00/56029**
WO-A-99/17499	**US-A- 6 147 994**
US-B1- 6 246 688	**US-B1- 6 356 546**

- **"UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM (UMTS); 3G SECURITY; LAWFUL INTERCEPTION ARCHITECTURE AND FUNCTIONS (3G TS 33.107 VERSION 3.0.0 RELEASE 1999)" ETSI TS 133 107 V3.0.0, XX, XX, January 2000 (2000-01), page 55, XP002214517**

EP 1 362 456 B1

Description

Background of the Invention

[0001] In law enforcement, it is sometimes necessary to monitor an individual or group of individuals to support allegations of illegal activity. Indeed, many countries mandate that telecommunications service providers and equipment manufacturers provide a law enforcement agency the ability to perform lawful interception of telecommunications to and from a subject being monitored.

[0002] Historically, lawful intercept consisted of using alligator clips which a law enforcement agency would physically clip to, thereby tapping into, the telecommunication line of a subject (the monitored party) and monitor calls to or from an associate (a party calling or being called by the subject.)

[0003] There are two categories of intercept, call data and call content. Call data intercept includes monitoring call events, for example, monitoring if the subject originates a call, or if a call is terminated on the subject, or if a call is forwarded elsewhere. This type of monitoring, known as pen register, provides the phone number of both the person called and the person calling, along with call events and time-date stamps of when the events occurred. In contrast, call content includes the actual content of the call, i.e., the conversation that takes place, plus call data. Call content is transmitted to the law enforcement agency in real time so that the law enforcement agency can monitor the conversation as it happens. This transmission must be transparent to the subject and the associates so that they are not aware that they are being monitored.

[0004] As telecommunications equipment evolved, modules were provided in the telecommunication switch that provided the law enforcement agency the ability to lawfully intercept telecommunications. For example, in a Time Division Multiplexed (TDM) switch such as Nortel Networks' DMS-100, a switch network fabric provides an access point that allows a law enforcement agency to tap the subject's phone line. This type of centrally located access point is known as an Intercept Access Point (IAP). The resulting information is then provided to the law enforcement agency.

[0005] As telecommunications have evolved to packet-based communications, to include Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) protocols, the changing architecture of the telecommunications switches has necessarily made the interception of content more difficult.

[0006] One way in which it has been attempted to overcome this difficulty is described in International Patent Application No. 99/17499. In this application the use of a legal interception nodded is described where at least some of the packets originating from such a mobile station or terminated thereto are routed and/or copied from at least one of the support nodes (SGSN, GGSN) via the legal interception node to the law enforcement authority. However, as the LIN appears as a transmitting or receiving node to the support nodes the system may not be completely transparent.

[0007] A method by which interception can be initiated are described further in International Patent Application Number 00/56029. This patent application describes an interception data collection function that can be implemented in an existing network node, such as a GPRS support node, allowing flexible implementation of an interception system. Finally, a method for transferring intercepted packets from an intercepting network element to a Law Enforcement Agency is described in International Patent Application 00/42742. In this application data sent to the law enforcement agency is transmitted via a secure tunnel provided by encryption processing.

[0008] In September of 1998, the Federal Communications Committee (FCC) ruled that new TDM equipment must have lawful intercept capability built in. Moreover, in August of 1999 the FCC ruled that packet communications interception capability will be required by September 30, 2001.

[0009] Accordingly, there is a need to be able to intercept voice over packet communication in a manner that satisfies governmental requirements, is transparent to the subject and the associate, in real time, and works with standard protocols such as IP and ATM applications.

Summary of the Invention

[0010] The invention results from the realization that a truly efficient and effective system and method for intercepting voice over packet communications is achieved in which a packet communication signal directed to or from a subject is received by a centralised replicator. The header is stripped from the packet leaving only the payload, the payload is replicated, a header is added to the replicated payload and the replicated payload is transmitted to a Law Enforcement Agency. A header is added to the original payload and the packet is retransmitted to the intended recipient. Alternatively, the entire packet can be replicated and the headers stripped off both the original packet and the replicated packet and a new header added to each payload. The payloads are then transmitted to the intended recipient and the Law Enforcement Agency.

[0011] According to one aspect of the present invention there is provided a method of intercepting a telecommunication signal transmitted between a first media gateway and a second media gateway as recited in Claim 1. According to a second aspect of the present invention there is provided a system for intercepting a telecommunication signal transmitted between a first media gateway and a second media gateway as recited in Claim 9.

[0012] In one embodiment, there is provided a method of intercepting a telecommunication signal including receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload,

adding a new header to the replicated payload and directing the replicated payload to the address associated with the new header.

[0013] It can be determined whether a telecommunication packet is to be monitored. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with the second predetermined header.

[0014] In another embodiment there is provided a system for intercepting a telecommunication signal. The system includes an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet comprising a predetermined header and a payload, a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to replicated payload and a relay point for directing the replicated payload to the address associated with the new header.

[0015] The new header can be associated with one of an intended recipient and a law enforcement agency. There can be a media gateway for directing the telecommunication signal to the audio server and also a media gateway controller, responsive to the media gateway, for determining that the telecommunication packet is to be intercepted. The media gateway controller can include a call discriminator, responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception. There can be a second termination point for adding a second predetermined header to the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. There can be a second relay point for directing the payload to the address associated with the second predetermined header.

[0016] In yet another embodiment, there is provided a method for intercepting a telecommunication signal by receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload, adding a new header to replicated payload and directing the replicated payload to the address associated with the new header.

[0017] It can be determined whether the telecommunication packet is to be intercepted. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be removed from the payload and replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with second predetermined header.

[0018] There is further provided a method of redirecting a telecommunication signal. The method includes receiving a telecommunication packet comprising a header and a payload, removing the predetermined header from the packet, adding a second predetermined header to payload and directing the replicated payload to the address associated with the second predetermined header.

[0019] It can be determined whether a telecommunication packet is to be redirected. The second predetermined header can be associated with one of an intended recipient and a law enforcement agency. The payload can be replicated. This replication can occur before or after the predetermined header is removed. A new header can be added to the replicated payload and the replicated payload can be directed to the address associated with second predetermined header. The new header can be associated with the other of the intended recipient and the law enforcement agency.

[0020] There is still further provided a method of monitoring a telecommunication signal to or from a subject being monitored from or to an associate. The method includes determining that a telecommunication signal is subject to being monitored, establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject, establishing a connection between the second gateway and a second termination point representing the first gateway and establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connection directly. ,

[0021] A connection can be established from at least one of the first termination point and the second termination point to a gateway associated with other than the subject and the associate concurrently with the connection between the first termination point and the second termination point.

[0022] There is provided even still further a method of redirecting a telecommunications signal intended for one of a subject and an associate by associating a first termination point with a first intended termination point of a first media gateway, associating a second termination point with a second intended termination point of a second media gateway, establishing a connection between the first intended termination point and the second termination point, establishing a connection between the second intended termination point and the first termination point and establishing a connection between the first termination point and the second termination point wherein the first intended termination point and the second termination point appear to be connected directly.

Brief Description of the Drawings

[0023]

Figure 1 is a schematic block diagram generally representing a system for intercepting packet communications including a centralized replicator according to the present invention;

Figure 2 is a more detailed schematic block diagram, similar to Figure 1, including a media gateway controller associated with each media gateway for implementing the necessary connections to affect interception of packet communications;

Figure 3 is a schematic block diagram, similar to Figure 1, demonstrating the actual and ephemeral connections when implementing the call intercept according to one aspect of the present invention;

Figure 4 is a schematic block diagram demonstrating associated connections internal to the centralized replicator for affecting bearer channel tandeming for intercepting packet communications;

Figure 5 is a schematic block diagram representing bearer channel tandeming by the call discriminator in response to a requirement to intercept packet communications;

Figure 6 is a flow chart representing one method of intercepting packet communications according to the present invention;

Figure 7 is a schematic block diagram, similar to Figure 2, in which a second associate establishes a call to a subject being monitored and a call waiting feature is invoked;

Figure 8 is a schematic block diagram, similar to figure 4, demonstrating the connection topology within the centralized replicator when the call-waiting feature is invoked; and

Figure 9 is a schematic block diagram, similar to Figure 8, demonstrating the connection topology within the centralized replicator when a conference call feature is invoked.

Detailed Description

[0024] According to the present invention there is generally provided a system **10,** Figure 1, which can intercept a packet telecommunication signal to or from a subject **12** being monitored, for example, by a Law Enforcement Agency (LEA) **14.** There is a first, or subject, media gateway **16** associated with subject **12** being monitored and a second, or associate, media gateway **18** associated with an associate **20** who is calling or being called by subject **12.** There can also be a wireless associate media gateway **18'** where an associate **20'** is communicating with subject **12** over a wireless phone.

[0025] A call is initiated between subject **12** and associate **20.** It is determined that the telecommunication signal is one targeted for monitoring and is to be intercepted. Accordingly, for a call from associate **20** to subject **18,** the telecommunication signal, rather than being sent directly to the intended associate media gateway **18,** is redirected from subject media gateway **16** to a centralized replicator **22** which may, for example, comprise a universal audio server associated with LEA **14.** When centralized replicator **22** receives the telecommunication signal, comprised of individual packets with each packet including a header and a payload, centralized replicator **22** removes the header from the packet leaving the payload intact. Centralized replicator **22** replicates the payload, adds a header to the replicated payload and transmits the replicated payload to a law enforcement agency gateway **24.** Once the payload has been replicated a header is added to the original payload and that packet is retransmitted by centralized replicator **22** to associate media gateway **18/18'** for delivery to associate **20/20'.**

[0026] Alternatively, the entire incoming packet can be replicated, including header and payload. Once the packet has been replicated, the headers of the original and replicated packets are removed. A new header is added to the replicated payload for delivery to law enforcement agency **14** and a new header is added to the original payload for delivery to the respective intended recipient, subject **12** or associate **20.**

[0027] Referring now to Figure 2, associated with each media gateway **16, 24** and **18,** can be a media gateway controller **26, 28** and **30,** respectively. As used herein, a media gateway controller refers to one or more devices whose functionality can include performing media gateway control signaling and call processing functions. Each associated gateway controller can include a call discriminator **32** comprising call processing software that determines that a call from or between associated gateways, for example subject media gateway **16** to associate media gateway **18,** is in fact subject to monitoring. There can be included within discriminator **32,** for example, a lawful intercept database that identifies subscribers, e.g., subject **12,** who are subject to a surveillance order.

[0028] Once it has been determined that the call is subject to monitoring, subject media gateway controller **26** sends a first message, for example using Media Gateway Control Protocol (MGCP) or H.248 protocol, to LEA media gateway **28** to effect a connection between subject media gateway **16** and centralized replicator **22** and another message to effect a connection between associate media gateway **18** and centralized replicator **22.** The redirection of the call through centralized replicator **22** is transparent to call processing and service functions and the call appears to be set up normally as if subject media gateway **16** and associate media gateway **18** were connected directly. The above example assumes that subject **12** and associate **20** do not share a common gateway. However, a shared gateway would not change the operation of the subject invention as call discrimination and packet replication would take place in the same manner, transparent to the caller.

[0029] LEA Media gateway controller **28** effects redirection of the call from the intended recipient and instructs

centralized replicator **22** to make internal connections, referred to as bearer channel tandeming, in order to facilitate packet replication as will be discussed further in reference to Figure 4. Once media gateway controller **28** has established the necessary connections between subject media gateway **16**, centralized replicator **22** and associate media gateway **18,** media gateway controller **28** initiates the connections between centralized replicator **22** and law enforcement agency media gateway **24** which is then connected to LEA **14.**

[0030] Accordingly, a call subject to monitoring will contain packets whose headers have been altered or substituted such that instead of the packets being transmitted to and from gateways **16** and **18** directly (the intended recipients), the packets are redirected to centralized replicator **22** for replication. Media gateway controller **28** alters the address information of the messages such that it appears to subject media gateway **16** that the message is coming from associate media gateway **18** and messages sent to associate media gateway **18** appear to come from subject media gateway **16.**

[0031] As shown in Figure 3, subject media gateway controller **26** sends a message **27** with the session description information, for example using a protocol such as the Session Description Protocol (SDP), of subject media gateway **16** to LEA media gateway controller **28.** Media gateway controller **28** sends a message **29** including the session information of media gateway **16** to associate media gateway controller **30,** but with the address of centralized replicator **22.**

[0032] Similarly, associate media gateway controller **30** sends a message **31** acknowledging the session description of media gateway **16** with the session description of associate media gateway **18.** LEA media gateway controller **28** sends a message **33** acknowledging the session description of subject media gateway **16** with the session description of associate media gateway **18**, but with the address of centralized replicator **22.**

[0033] Accordingly, a communication path from subject media gateway **16** to associate media gateway **18** is tandemed through centralized replicator **22**, but is transparent to subject **12** or associate **20.**

[0034] Figure 4 further demonstrates how bearer channel tandeming can be accomplished through centralized replicator **22** by modifying the association between packet streams and endpoints to affect the connections and representations demonstrated in Figure 3.

[0035] Packet streams **34, 36, 38** and **40** originate from associated endpoints **42, 44, 46** and **48**, respectively. Accordingly, the respective transmit and receive streams **34/36** of endpoint **42,** while appearing to be associated with endpoint **46** (associate media gateway **18),** are associated with end point **44** within centralized replicator **22.** Similarly, respective transmit and receive streams **38/40** of endpoint **46** are associated with end point **48** while appearing to be associated with end point **42** (subject media gateway **16).** Finally, internal streams **50** and **52** are associated with end points **44** and **48.** Connections to end points **42, 44, 46** and **48** are initiated from media gateway controller **28** (Figure 3) where endpoints **42** and **46** are the recognized originator and terminator endpoints.

[0036] Endpoints **42** and **46** are typically configured to convert the TDM information from subject **12** or associate **20** into, for example, IP or ATM packets or cells depending upon the fabric of centralized replicator **22.** Similarly, information received at these endpoints from centralized replicator **22** is converted from IP/ATM to TDM. In contrast, endpoints **44** and **48** within centralized replicator **22** are typically configured only as packet relay points and do not provide any transcoding or jitter correction in order to minimize latency and reduce the risk of detection by subject **12** or associate **20** of the monitoring. Flow control buffers (not shown) can be provided to avoid loosing packets.

[0037] Packet relay endpoints **44** and **48,** respectively, strip the header off incoming packet streams **34** and **38** that they receive from respective endpoints **42** and **46,** replicate the payload, add a new header to the replicated payload and transmit replicated packet streams **54** and **56** to law enforcement agency gateway **24** via endpoints **58** and **60.** Packet relay endpoints **44** and **48** also transmit the original payload via streams **50** and **52**, respectively, to each other, adding new headers directing the packets to respective gateways **16** and **18.** Alternatively, the entire packet may be replicated, then the replicated headers are stripped off and new headers added to redirect the replicated packets to their respective gateways.

[0038] In order to ensure transparency to subject **12** and associate **20** of the intercept, streams **54** and **56** destined for law enforcement agency **14** should be unidirectional. Accordingly, endpoints **58** and **60** should be configured as send only in the direction of law enforcement agency gateway **24.** Endpoints **58, 60** should be from the same resource pool as endpoints **44** and **48** so that the resource pools reflect what endpoints within centralized replicator **22** have internal connections between them so that media gateway controller **28** can send the appropriate connectivity messages to centralized replicator **22.** Accordingly, a resource manager **62** is provided. Moreover, endpoints **58** and **60,** as with packet relay endpoints **44** and **48,** should achieve a transmission time between endpoints that maintains low latency such that the total trip delay of the packets, including time to traverse centralized replicator **22,** does not exceed the engineered threshold of the echo cancellers of the respective media gateways.

[0039] Resource manager **62** performs several basic functions to include allocation of resources, returning resources to a free pool and reporting on resources. Resource manager **62** can provide an interface to operating personnel to indicate what resources in centralized replicator **22** are to be used for bearer channel tandeming. The connection to law enforcement agency **14** can occur in several forms to include dedicated lines, switched local links, dedicated trunks or switched remote links without

departing from the scope of the invention.

[0040] A monitoring point **64** within law enforcement agency **14,** which may include an audio device, can receive the call content via a TDM multiplexed mixing bridge **66.** Monitoring point **64** receives the call content in real time, thus at the same time subject **12** hears the ring from associate **20,** law enforcement agency **14** also hears the ring back. As will be apparent to those skilled in the art, law enforcement agency gateway **24** should be able to support all possible CODEC's that can be negotiated between a subject **12** and an associate **20.**

[0041] While system **10** has been described as only performing a single replication for a single law enforcement agency, it should be understood that this is not a limitation of the present invention, as the incoming packet streams can be replicated at endpoints **44** and **48** multiple times, depending on the number of law enforcement agencies monitoring subject **12,** by configuring the hardware comprising endpoints **44** and **48** for multiple replications.

[0042] Despite the changes in the connection messages as described above, neither subject **12** nor associate **20** are provided an indication that the call is being redirected through centralized replicator **22.**

[0043] When it is determined that a call is to be monitored, the standard connectivity message from the call server can either be altered to perform the appropriate connection or the message can be split into multiple messages to perform the requested connection.

[0044] By way of example, the connection operation from the call server requesting a connection between subject **12** and associate **20** is modified into three separate connectivity operations. This is done by requesting separate connections from endpoints **42** and **44,** from endpoints **46** and **48** and from endpoints **44** to **48.**

[0045] As shown in Figure 5, a call agent or call processing **68,** in response to electronic surveillance software **69,** issues a connectivity message **70** to call discriminator **32** to make a subject to associate connection from a discriminator layer in connectivity software **72** to bearer channel tandeming connectivity software **74** which issues three separate media gateway control messages. A first message **76** can initiate a connection from subject media gateway **16** (Figure 4) to centralized replicator **22.** A second message **78** can initiate a connection from associate media gateway **18** to centralized replicator **22.** A third message **80** can instruct centralized replicator **22** to make an internal association between the centralized replicator **22** to subject media gateway **16** connection and the centralized replicator **22** to associate media gateway **18** connection.

[0046] Once the associated connection between subject **12** and associate **20** has been configured, media gateway controller **28** (Figure 3) initiates the respective connections to law enforcement media gateway **24** by requesting two connections from endpoints **44** to **58** and **48** to **60** (Figure 4) within centralized replicator **22** to law enforcement media gateway **24,** where endpoints **58** and **60** connect to law enforcement media gateway **24,** as illustrated in Figure 4 above.

[0047] A flowchart of the present invention is presented in Figure 6. A call is initiated between a subject and an associate, Block **82.** The media gateway controller associated with the subject being monitored determines that the call is to be monitored, Block **84,** and redirects the call to the media gateway controller of the LEA by associating the LEA media gateway with the destination (associate) media gateway, Block **86.** The media gateway controller associated with the law enforcement agency effects bearer channel tandeming by associating the endpoints of the subject and associate media gateways with endpoints within the centralized replicator, Block **88.**

[0048] Once tandeming of the bearer channel has been affected, packets to and from the subject are redirected to the centralized replicator, Block **90,** where the payload is replicated, Block **92,** and new headers added to both the replicated payload and the original payload, Block **94.** The respective payloads are then transmitted to the recipient subject or associate and the LEA, Block **96.**

[0049] Figure 7 represents generally the situation where a call-waiting feature is invoked. For illustrative purposes, each agent is serviced by a different media gateway controller. A call is originated between subject **12** and first associate **20,** as discussed above, until subject **12** and first associate **20** enter the talking state as discussed above with the law enforcement agency **14** receiving the call content.

[0050] A second associate **20"** originates a call to subject **12.** Associate media gateway controller **30'** performs call processing routing the call to subject media gateway **16** and it is determined that the call is subject to interception. Centralized replicator **22** recognizes that subject **12** is engaged in an existing call. LEA media gateway controller **28** instructs media gateway **16** to play a call waiting tone to subject **12.**

[0051] Referring now to Figure 8, subject **12** invokes a feature flash to receive the call originated by second associate **20".** Subject media gateway controller **26** (Figure 7) instructs centralized replicator **22** to break the connection between subject **12** and first associate **20.** However, Tandeming Connectivity software **74** (Figure 5) intercepts this message, and alters it to only break the connection between endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA **14** be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** remain in tact.

[0052] Tandeming Connectivity software **74** obtains two more endpoints **44'** and **48** from resource manager **62** to tandem the call between subject **12,** second associate **20"** and LEA **14.** Tandeming Connectivity software **74** initiates a connection between end points **42** and **44'.** Tandeming Connectivity software **74** further Initiates a

connection between endpoints **44'** and **48'** within centralized replicator **22.** The session description information of endpoints **42** and **44'** are exchanged, and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel.

[0053] Subject media gateway controller **26** acknowledges endpoint **46'** and responds with the session information of endpoint **48',** in order to facilitate the completion of the bearer channel configuration.

[0054] At this point a bearer channel is configured between end points **42** and **44', 44'** and **48'** and **48'** and **46'.** Subject **12** and second associate **20"** now enter the talking state with law enforcement agency **14** receiving the call content. Second associate **20"** terminates the call and subject **12** invokes a feature flash to return to first associate **20.** Subject media gateway controller **26** sends a message to break the connection between subject **12** and the message is intercepted and altered to only break the connection between end points **42** and **44'.** The connection with Law enforcement agency **14** is also broken, but the connections between endpoints **44'** and **48'** and **48'** and **46'** remain intact. Second associate media gateway controller **30'** (not shown) passes a clear forward message to subject media gateway controller **26** instructing connectivity to break the connection with second associate **20'.** Tandeming Connectivity software **74** (Figure 5) intercepts the message and, determining that the other external agent has been removed from,the bearer channel tandem, instructs a break of the connections between end points **44'** and **48',** and **48'** and **46'.**

[0055] Endpoints **44'** and **46'** are returned to resource manager **62** to be reentered into the free pool. Subject media gateway controller **26** (Figure 7) sends a message to reestablish a connection between subject **12** and first associate **20.** Tandeming Connectivity software **74** (Figure 5) Intercepts this message, determines the given communication is already associated with a tandemed connection, and retrieving the endpoints in use, issues connectivity messages to reestablish the connection between endpoints **42** and **44.**

[0056] The session information of end points **42** and **44** are exchanged as previously discussed completing the bearer channel tandem. Electronic Surveillance software **69** (Figure 5) requests notification of the endpoints being used to tandem the bearer channel through centralized replicator **22.** Endpoints **58** and **60** are then-connected to LEA media gateway **24** in order to provide capture of the call content. Subject **12** and associate **20** are again in a talking state through a bearer channel established via endpoints **42** and **44, 44** and **48** and **48** and **46.**

[0057] Referring to Figure 7 once again, a conference call feature is established in a manner similar to call waiting. A call is originated between subject **12** and first associate **20.** Subject media gateway controller **26** determines that the call is subject to monitoring and bearer channel tandeming is initiated connecting subject media gateway **16** and associate media gateway **18** via centralized replicator **22** as discussed above by LEA media gateway controller **26** associating respective end points within centralized replicator **22** with subject media gateway **16** and associate media gateway **18.** A connection is then initiated between end points within centralized replicator **22.**

[0058] Associate media gateway **18** acknowledges the associated endpoint within centralized replicator **22,** as if it were acknowledging subject media gateway **16,** as discussed above with reference to Figure 3, and responds with the session description information of associate media gateway **18** and a bearer channel is configured between endpoints **42, 44, 46** and **48** (Figure 4).

[0059] A connection between law enforcement agency gateway **24** and end points within centralized replicator **22** as discussed in Figure 4 above, is established. Subject **12** and associate **20** now enter a talking state and law enforcement agency **14** receives the replicated packet streams and monitors the call.

[0060] Referring again to Figure 8, subject **12** can invoke a flash feature and originate or receive a call with a second associate **20".** Subject media gateway controller **26** (Figure 7) receives a message from the call agent of subject **12** to break the connection with first associate **20,** which is intercepted due to the bearer channel tandeming, and media gateway controller **28** sends a modified message to centralized replicator **22** (rather than to associate media gateway **18)** to break the connectivity of endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA 14 be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** temporarily remain in tact.

[0061] With respect to the new caller, the media gateway determines that the call is subject to monitoring, and two more endpoints **44'** and **48'** within centralized replicator **22** are allocated by resource manager **62** and configured to tandem the call to second associate **20'.** A connection is then initiated between endpoints **42** and **44'** and media gateway controller **28** passes the endpoint of **48'** to the media gateway controller **30'** associated with second associate **20".** A connection is then initiated between **44'** and **48'** within centralized replicator **22.** The session description information of **42** and **44'** are exchanged and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel tandeming.

[0062] At this point a bearer channel is configured between **42** and **44', 44'** and **48',** and **48'** and **46'.** A connection is then initiated from centralized replicator **22** to LEA 14 via endpoints **44'** and **58'** and **48'** and **60'.** Subject **12** can now talk with second associate **20"** and LEA **14** can intercept the content. Subject **12** then invokes a feature flash to join first associate **20** in a three-way call. Connectivity software (Figure 5) requests that all connections associated with the previous legs be broken (shown in phantom) to enable the three-way call. Accord-

ingly, the connection of end points **44** and **48**, **48** and **46** and **44'** and **48'** and **48'** and **46'** are broken along with the corresponding LEA connection and all resources are returned to the resource pool. Media gateway controller **28** requests a connection between subject **12**, first associate **20** and second associate **20"** through conferenced ports **98**, **100** and **102**, as shown in Figure 9.

Claims

1. A method of intercepting a telecommunication signal transmitted between a first media gateway (16, 18) and a second media gateway (16, 18) in a network, the method comprising:

   (a) receiving a telecommunication packet from the first media gateway (16, 18) comprising a predetermined header and a payload;
   (b) removing the predetermined header from the packet;
   (c) replicating the payload;
   (d) adding a new header to the replicated payload; and
   (e) directing the replicated payload to the address associated with the new destination header and **characterised by**
   (f) adding an altered predetermined header or substitute header to the said telecommunication packet or the replicated payload, and directing that packet or payload to the second media gateway, the altered predetermined header or substitute header having address information such that it appears to the second media gateway (16, 18) that the message is coming from the first media gateway (16, 18).

2. The method of Claim 1 further comprising the step of determining that a telecommunication packet is to be monitored.

3. The method of claim 1 further comprising the step of determining that a telecommunication packet is to be intercepted.

4. The method of Claim 1 further comprising redirecting the telecommunication signal.

5. The method of claim 4 further comprising the step of determining that a telecommunication packet is to be redirected.

6. The method of claim 1 further comprising the step of associating the new destination header with an intended recipient or a law enforcement agency (14).

7. The method of claim 1 further comprising the step of replacing the predetermined header with a second new destination .

8. The method of claim 7 further comprising the step of associating the second new destination header with the other of the intended recipient or the law enforcement agency (14).

9. The method of claim 7 in which the step of replacing occurs after the step of replicating.

10. A system for intercepting a telecommunication signal transmitted between a first media gateway (16, 18) and a second media gateway (16, 18) within a network, the system comprising a replicator (22)including:

    (a) an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet from the first media gateway (16, 18), the telecommunication packet comprising a predetermined header and a payload; the replicator (22) **characterised by** further including:
    (b) a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to the replicated payload, (16, 18); and
    (c) a relay point for directing the replicated payload to the address associated with the new destination header and **characterised by**
    (d) the termination point being arranged to add an altered predetermined header or substitute header to the said telecommunication packet or the replicated payload, and the relay point being arranged to direct that packet or payload to the second media gateway, the altered predetermined header or substitute header having address information such that it appears to the second media gateway (16, 18) that the message is coming from the first media gateway (16, 18)

11. The system of claim 9 wherein the first media gateway (16, 18) is adapted to direct the telecommunication signal to the audio server.

12. The system of Claim 9 further comprising a second termination point for adding a second predetermined header to the payload.

13. The system of Claim 11 in which a second new destination header is added to the replicated payload, the second new destination header being associated with a law enforcement agency (14).

14. The system of Claims 11 or 13 further comprising a second relay point for directing the payload to the address associated with the second predetermined header.

15. The system of Claim 9 further comprising a media gateway controller (26, 30), responsive to a first or second media gateway (16, 18), for determining that a telecommunication packet is to be intercepted.

16. The system of Claim 13 in which the media gateway controller (26, 30) includes a call discriminator (32), responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception.

Patentansprüche

1. Verfahren zum Abfangen eines Telekommunikationssignals, das zwischen einer ersten Medien-Überleiteinrichtung (16, 18) und einer zweiten Medien-Überleiteinrichtung (16, 18) in einem Netzwerk übertragen wird, wobei das Verfahren Folgendes umfasst:

   (a) Empfangen eines Telekommunikations-Paketes von der ersten Medien-Überleiteinrichtung (16, 18), das ein vorgegebenes Kopffeld und eine Nutzinformation enthält;
   (b) Entfernen des vorgegebenen Kopffeldes von dem Paket;
   (c) Replizieren der Nutzinformation;
   (d) Hinzufügen eines neuen Kopffeldes zu der replizierten Nutzinformation; und
   (e) Lenken der replizierten Nutzinformation an die Adresse, die dem neuen Ziel-Kopffeld zugeordnet ist, und **gekennzeichnet durch**:
   (f) Hinzufügen eines geänderten vorgegebenen Kopffeldes oder Ersatz-Kopffeldes zu dem Telekommunikations-Paket oder der replizierten Nutzinformation, und Lenken des Paketes oder der Nutzinformation an die zweite Medien-Überleiteinrichtung, wobei das geänderte vorgegebene Kopffeld oder Ersatz-Kopffeld eine Adresseninformation derart hat, dass es der zweiten Medien-Überleiteinrichtung (16, 18) erscheint, dass die Mitteilung von der ersten Medien-Überleiteinrichtung (16, 18) kommt.

2. Verfahren nach Anspruch 1, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket zu überwachen ist, umfasst.

3. Verfahren nach Anspruch 1, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket abzufangen ist, umfasst.

4. Verfahren nach Anspruch 1, das weiterhin die Umlenkung des Telekommunikationssignals umfasst.

5. Verfahren nach Anspruch 4, das weiterhin den Schritt der Feststellung, dass ein Telekommunikations-Paket umzulenken ist, umfasst.

6. Verfahren nach Anspruch 1, das weiterhin den Schritt der Zuordnung des neuen Ziel-Kopffeldes zu einem beabsichtigen Empfänger oder einer Vollstreckungsbehörde (14) umfasst.

7. Verfahren nach Anspruch 1, das weiterhin den Schritt des Ersetzens des vorgegebenen Kopffeldes durch ein zweites neues Ziel umfasst.

8. Verfahren nach Anspruch 7, das weiterhin den Schritt der Zuordnung des zweiten neuen Ziel-Kopffeldes zu dem anderen von dem vorgesehenen Empfänger oder der Vollstreckungsbehörde (14) umfasst.

9. Verfahren nach Anspruch 7, bei dem der Schritt des Ersetzens nach dem Schritt des Replizierens erfolgt.

10. System zum Abfangen eines Telekommunikationssignals, das zwischen einer ersten Medien-Überleiteinrichtung (16, 18) und einer zweiten Medien-Überleiteinrichtung (16, 18) in einem Netzwerk übertragen wird, wobei das System einen Replikator (22) umfasst, der Folgendes einschließt:

    (a) einen Audio-Server, der auf ein Telekommunikationssignal anspricht, um ein Telekommunikations-Paket von der ersten Medien-Überleiteinrichtung (16, 18) zu empfangen, wobei das Telekommunikations-Paket ein vorgegebenes Kopffeld und eine Nutzinformation umfasst; wobei der Replikator (22) **dadurch gekennzeichnet ist, dass** er weiterhin Folgendes einschließt:
    (b) einen Abschluss-Punkt zum Entfernen des vorgegebenen Kopffeldes von dem Paket, zum Replizieren der Nutzinformation und zum Hinzufügen eines neuen Kopffeldes zu der replizierten Nutzinformation (16, 18); und
    (c) einen Relais-Punkt zum Lenken der replizierten Nutzinformation an die Adresse, die dem neuen Ziel-Kopffeld zugeordnet ist, und **dadurch gekennzeichnet, dass**:
    (d) der Abschluss-Punkt so angeordnet ist, dass er ein abgeändertes vorgegebenes Kopffeld oder ein Ersatz-Kopffeld zu dem Telekommunikations-Paket oder der replizierten Nutzinformation hinzufügt, und dass der Relais-Punkt so angeordnet ist, dass er dieses Paket oder die Nutzinformation an die zweite Medien-Überleiteinrichtung lenkt, wobei das geänderte vorgegebene Kopffeld oder das Ersatz-Kopffeld eine derartige Adresseninformation hat, dass es der zweiten Medien-Überleiteinrichtung (16, 18) erscheint, dass die Mitteilung von der ersten Medien-Überleiteinrichtung kommt.

11. System nach Anspruch 9, bei dem die erste Medien-Überleiteinrichtung (16, 18) so ausgebildet ist, dass sie das Telekommunikationssignal an den Audio-Server lenkt.

12. System nach Anspruch 9, das weiterhin einen zweiten Abschluss-Punkt zum Hinzufügen eines zweiten vorgegebenen Kopffeldes zu der Nutzinformation umfasst.

13. System nach Anspruch 11, bei dem ein neues Ziel-Kopffeld zu der replizierten Nutzinformation hinzugefügt wird, wobei das zweite neue Ziel-Kopffeld einer Vollstrekkungsbehörde (14) zugeordnet ist.

14. System nach Anspruch 11 oder 13, das weiterhin einen zweiten Relais-Punkt zum Lenken der Nutzinformation an die Adresse umfasst, die dem zweiten vorgegebenen Kopffeld zugeordnet ist.

15. System nach Anspruch 9, das weiterhin eine Medien-Überleiteinrichtungs-Steuerung (26, 30) umfasst, die auf die erste oder zweite Medien-Überleiteinrichtung (16, 18) anspricht, um festzustellen, dass ein Telekommunikations-Paket abzufangen ist.

16. System nach Anspruch 13, bei dem die Medien-Überleiteinrichtungs-Steuerung (26, 30) einen Anruf-Diskriminator (32) einschließt, der auf das Telekommunikationssignal anspricht, um festzustellen, dass das Telekommunikationssignal einem Abfangen unterworfen ist.

Revendications

1. Un procédé d'interception d'un signal de télécommunication transmis entre une première passerelle de médias (16, 18) et une seconde passerelle de médias (16, 18) dans un réseau, le procédé comprenant :

(a) la réception d'un paquet de télécommunication provenant de la première passerelle de médias (16, 18), comprenant un en-tête prédéterminé et une charge utile ;
(b) la suppression de l'en-tête prédéterminé du paquet ;
(c) la duplication de la charge utile ;
(d) l'ajout d'un nouvel en-tête à la charge utile dupliquée ; et
(e) la direction de la charge utile dupliquée vers l'adresse associée au nouvel en-tête de destination ; et **caractérisé par**
(f) l'ajout d'un en-tête prédéterminé modifié ou d'un en-tête de substitution audit paquet de télécommunication ou à la charge utile dupliquée, et la direction de ce paquet ou de cette charge utile vers la seconde passerelle de médias, l'en-tête prédéterminé modifié ou l'en-tête de substitution comprenant une information d'adresse modifiée de telle sorte qu'il apparaît à la seconde passerelle de médias (16, 18) que le message provient de la première passerelle de médias (16, 18).

2. Le procédé de la revendication 1, comprenant en outre l'étape consistant à déterminer qu'un paquet de télécommunication doit être surveillé.

3. Le procédé de la revendication 1, comprenant en outre l'étape consistant à déterminer qu'un paquet de télécommunication doit être intercepté.

4. Le procédé de la revendication 1, comprenant en outre l'étape consistant à rediriger le signal de télécommunication.

5. Le procédé de la revendication 4, comprenant en outre l'étape consistant à déterminer qu'un paquet de télécommunication doit être redirigé.

6. Le procédé de la revendication 1, comprenant en outre l'étape consistant à associer le second nouvel en-tête à un destinataire prévu ou à organisme chargé de l'application de la loi (14).

7. Le procédé de la revendication 1, comprenant en outre l'étape consistant à remplacer l'entête prédéterminé par une seconde nouvelle destination.

8. Le procédé de la revendication 7, comprenant en outre l'étape consistant à associer le second nouvel en-tête de destination à l'autre parmi le destinataire prévu ou l'organisme chargé de l'application de la loi (14).

9. Le procédé de la revendication 7, dans lequel l'étape de remplacement a lieu après l'étape de duplication.

10. Un système pour intercepter un signal de télécommunication transmis entre une première passerelle de médias (16, 18) et une seconde passerelle de médias (16, 18) dans un réseau, le système comprenant un duplicateur (22) incluant :

(a) un serveur audio, réagissant à un signal de télécommunication, pour recevoir un paquet de télécommunication provenant de la première passerelle de médias (16, 18), le paquet de télécommunication comprenant un en-tête prédéterminé et une charge utile ; le duplicateur étant **caractérisé en ce qu'**il comprend en outre :
(b) un point de terminaison pour supprimer l'en-tête prédéterminé du paquet, pour dupliquer la

charge utile et pour ajouter un nouvel en-tête à la charge utile dupliquée (16, 18) ; et
(c) un point de relais pour diriger la charge utile dupliquée vers l'adresse associée au nouvel en-tête de destination, et **caractérisé en ce que**
(d) le point de terminaison est agencé pour ajouter un en-tête prédéterminé modifié ou un en-tête de substitution audit paquet de télécommunication ou ladite charge utile dupliquée, et le point de relais est disposé pour diriger ce paquet ou cette charge utile à la seconde passerelle de médias, l'en-tête prédéterminé modifié ou l'en-tête de substitution ayant une information d'adresse de telle sorte qu'il apparaît à la seconde passerelle de médias (16, 18) que le message provient de la première passerelle de médias (16, 18).

11. Le système de la revendication 10, dans lequel la première passerelle de médias (16, 18) est adaptée pour diriger le signal de télécommunication vers le serveur audio.

12. Le système de la revendication 10, comprenant en outre un second point de terminaison pour ajouter un second en-tête prédéterminé à la charge utile.

13. Le système de la revendication 11, dans lequel un second nouvel en-tête de destination est ajouté à la charge utile dupliquée, le second nouvel en-tête de destination étant associé à un organisme chargé de l'application de la loi (14).

14. Le système des revendications 11 ou 13, comprenant en outre un second point de relais pour diriger la charge utile vers l'adresse associée au second en-tête prédéterminé.

15. Le système de la revendication 9, comprenant en outre une unité de commande de passerelle de médias (26, 30), réagissant à une première ou une seconde passerelle de médias (16, 18), pour déterminer qu'un paquet de télécommunication doit être intercepté.

16. Le système de la revendication 13, dans lequel l'unité de commande de passerelle de médias (26, 30) comprend un discriminateur d'appels (32), réagissant au signal de télécommunication, pour déterminer que le signal de télécommunication fait l'objet d'une interception.

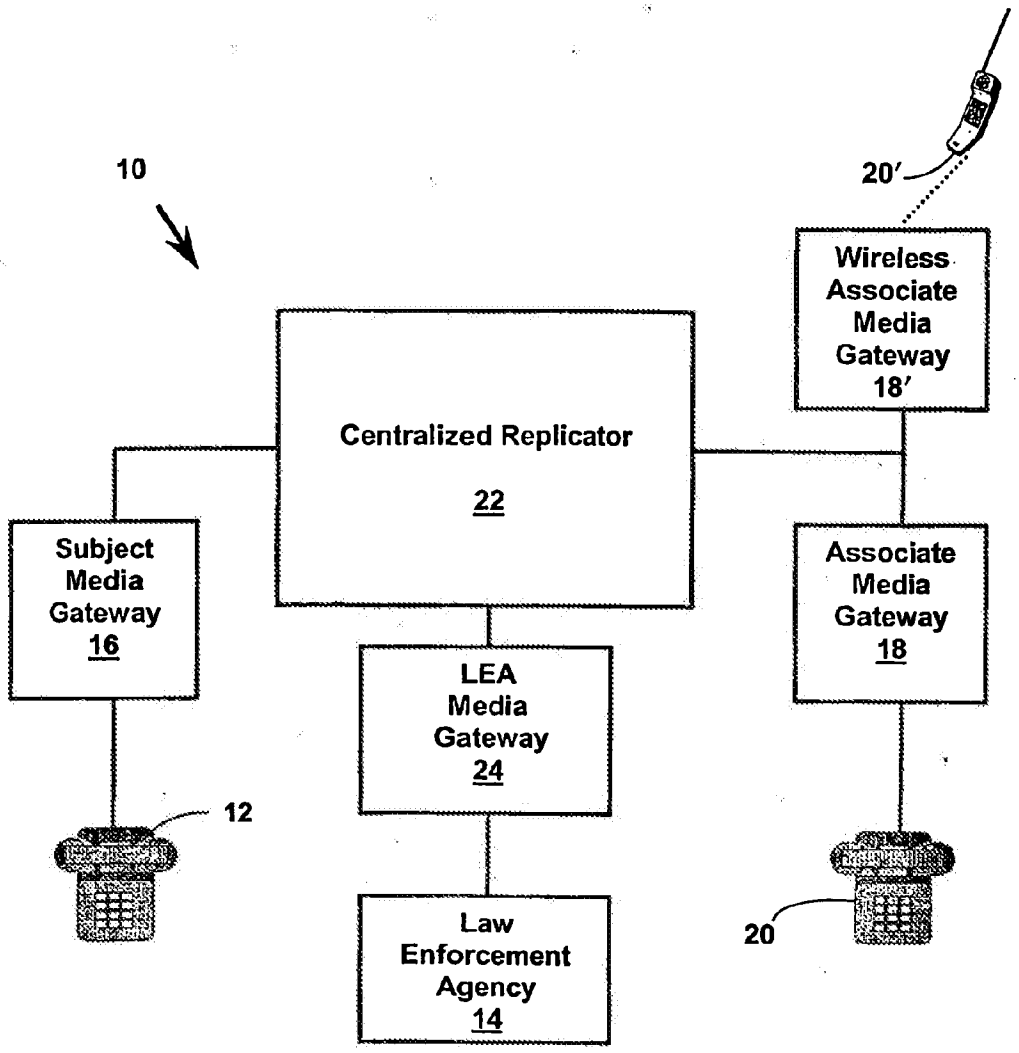


Figure 1

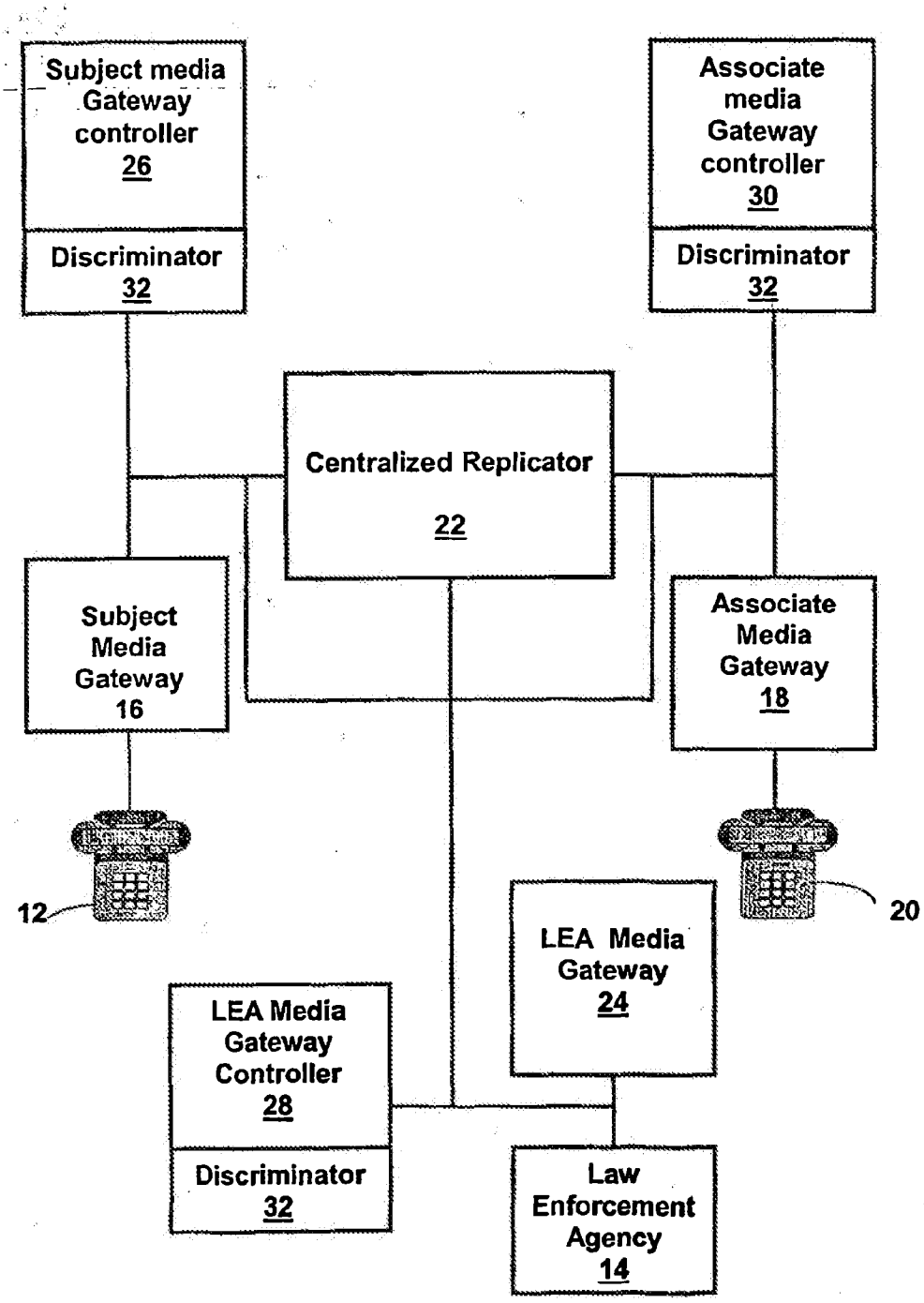


Figure 2

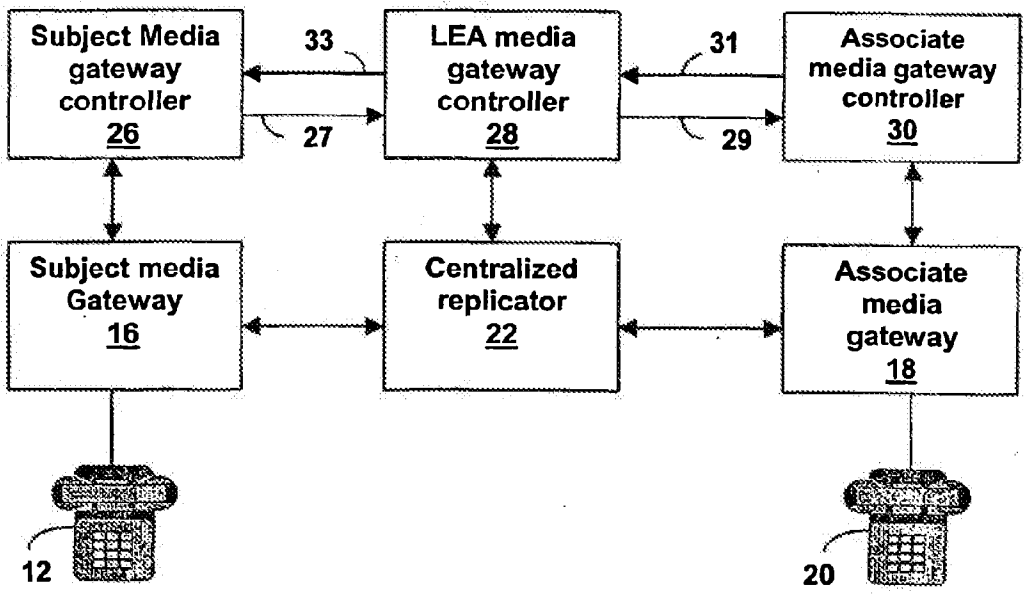


Figure 3

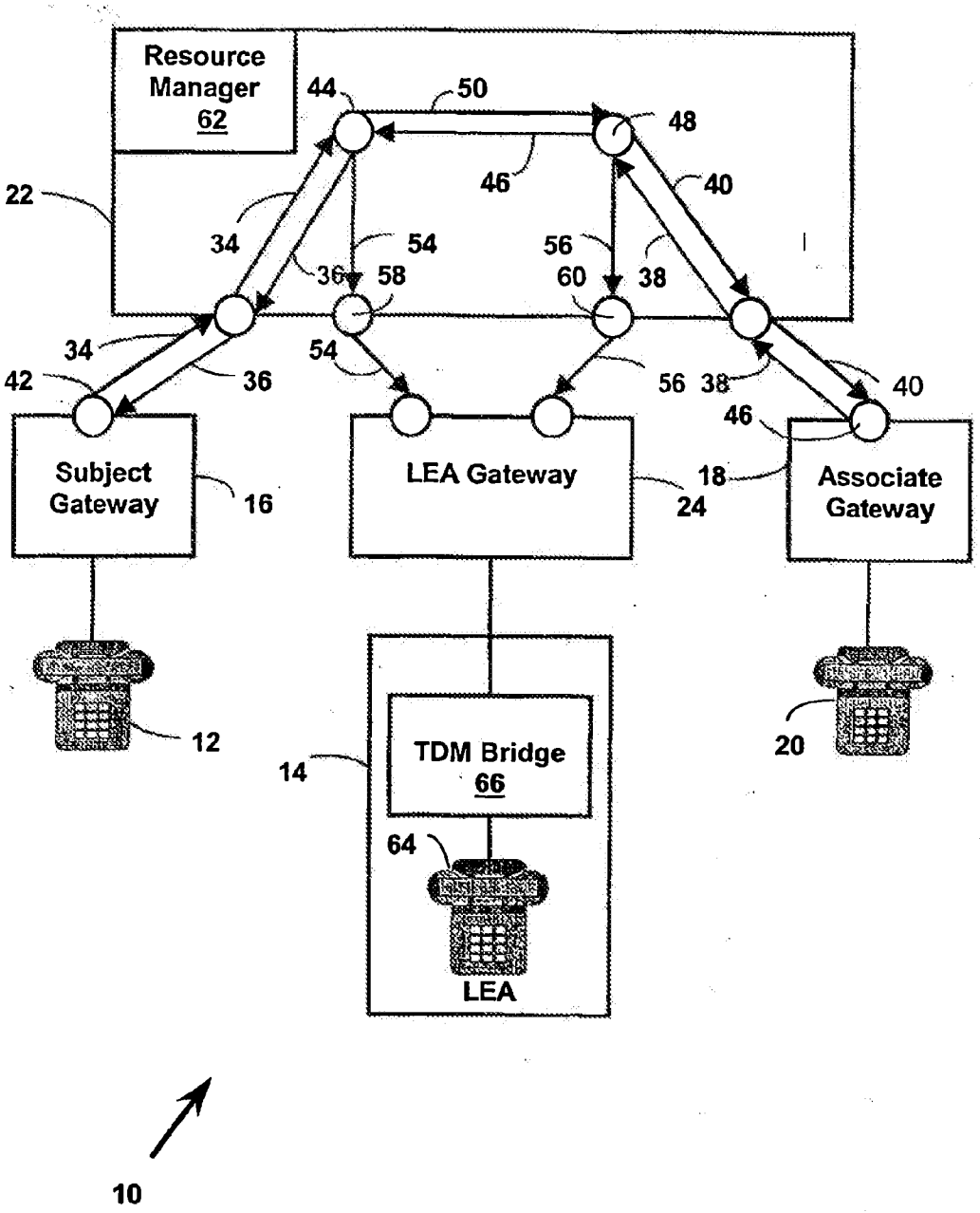


Figure 4

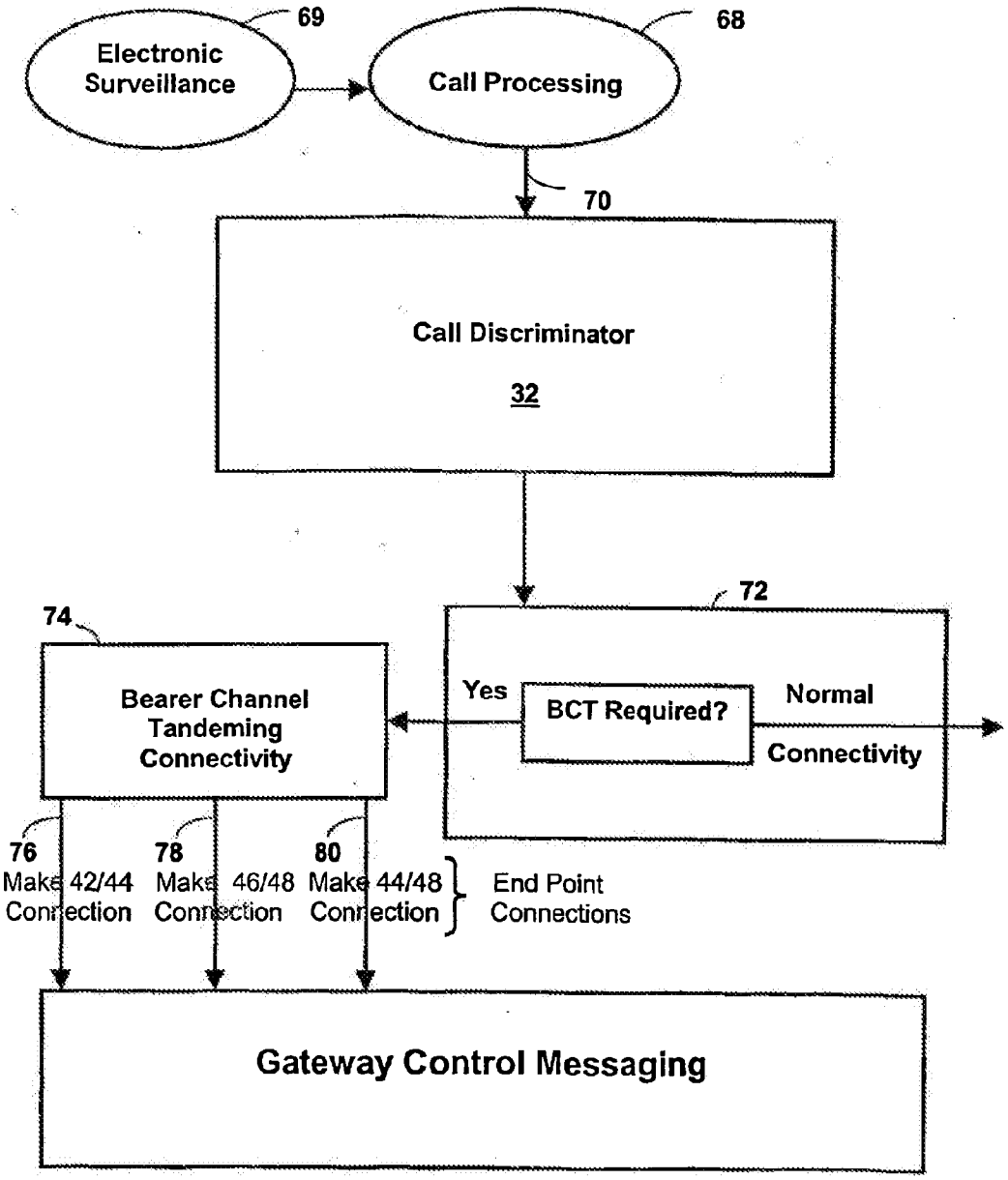


Figure 5

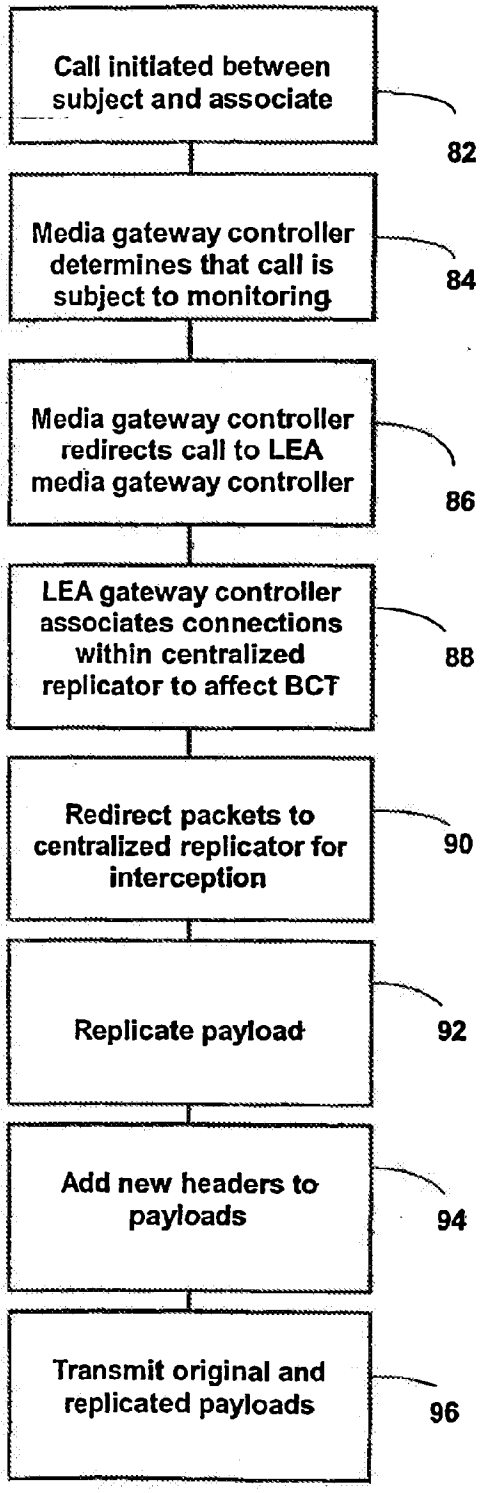


Figure 6

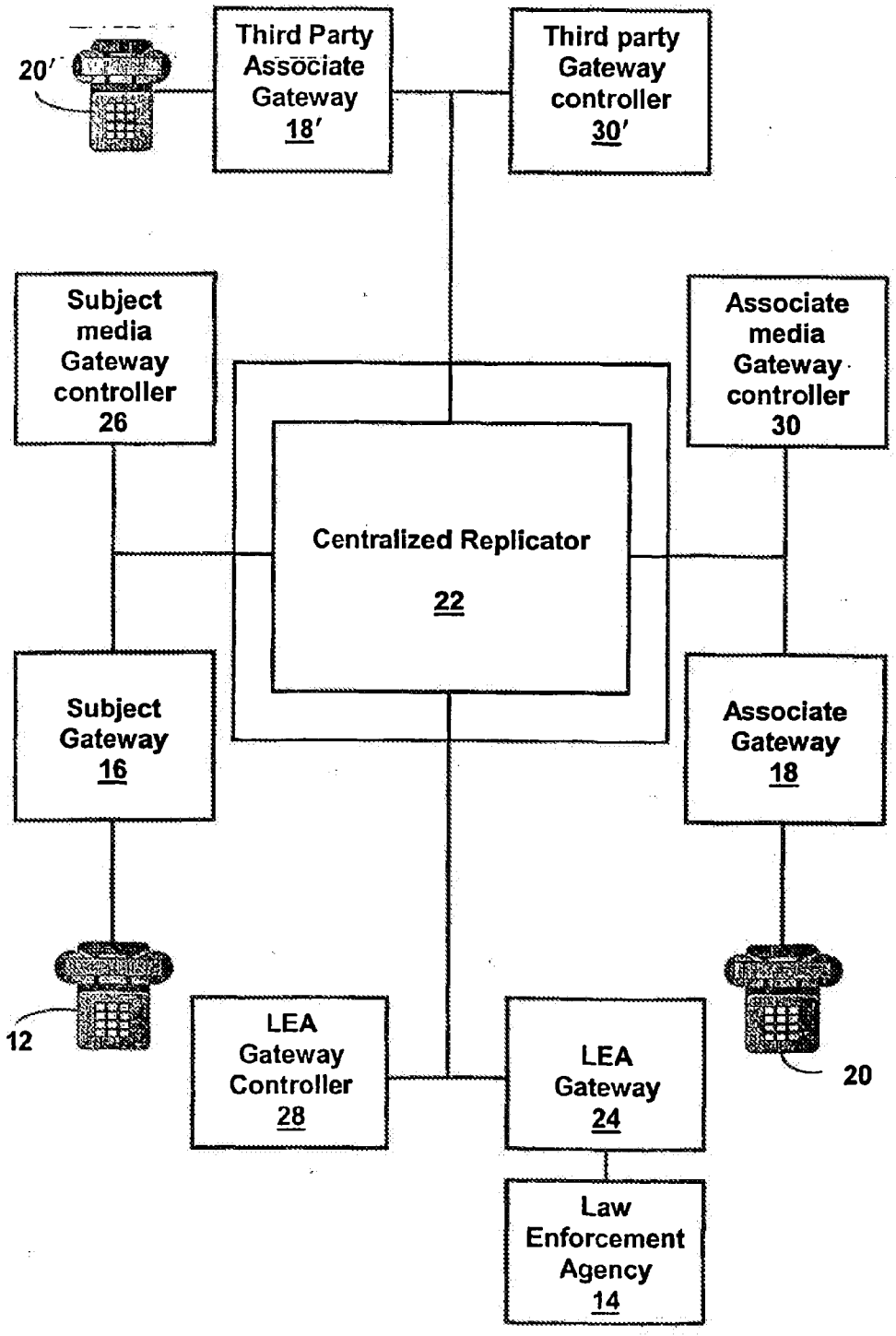


Figure 7

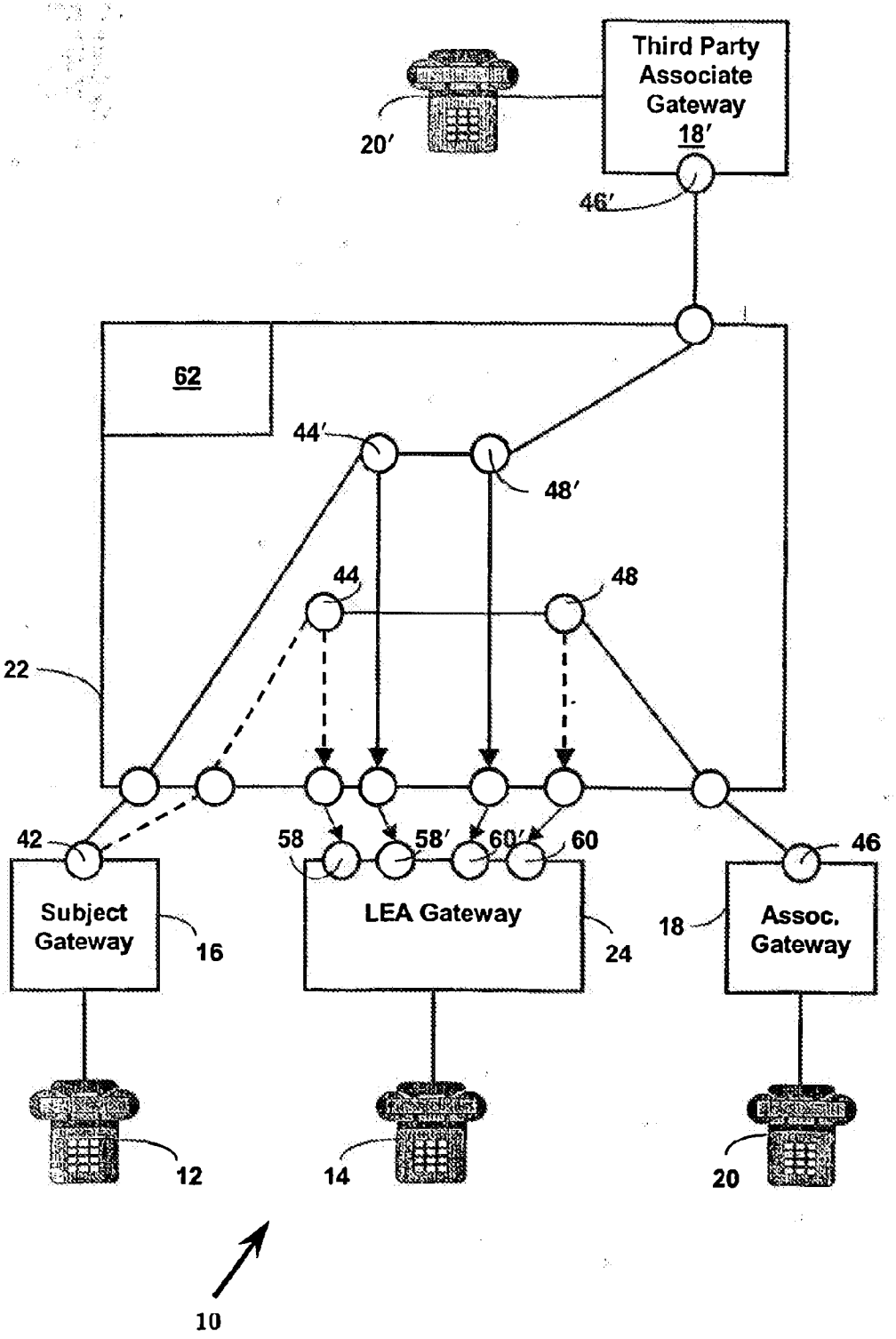


Figure 8

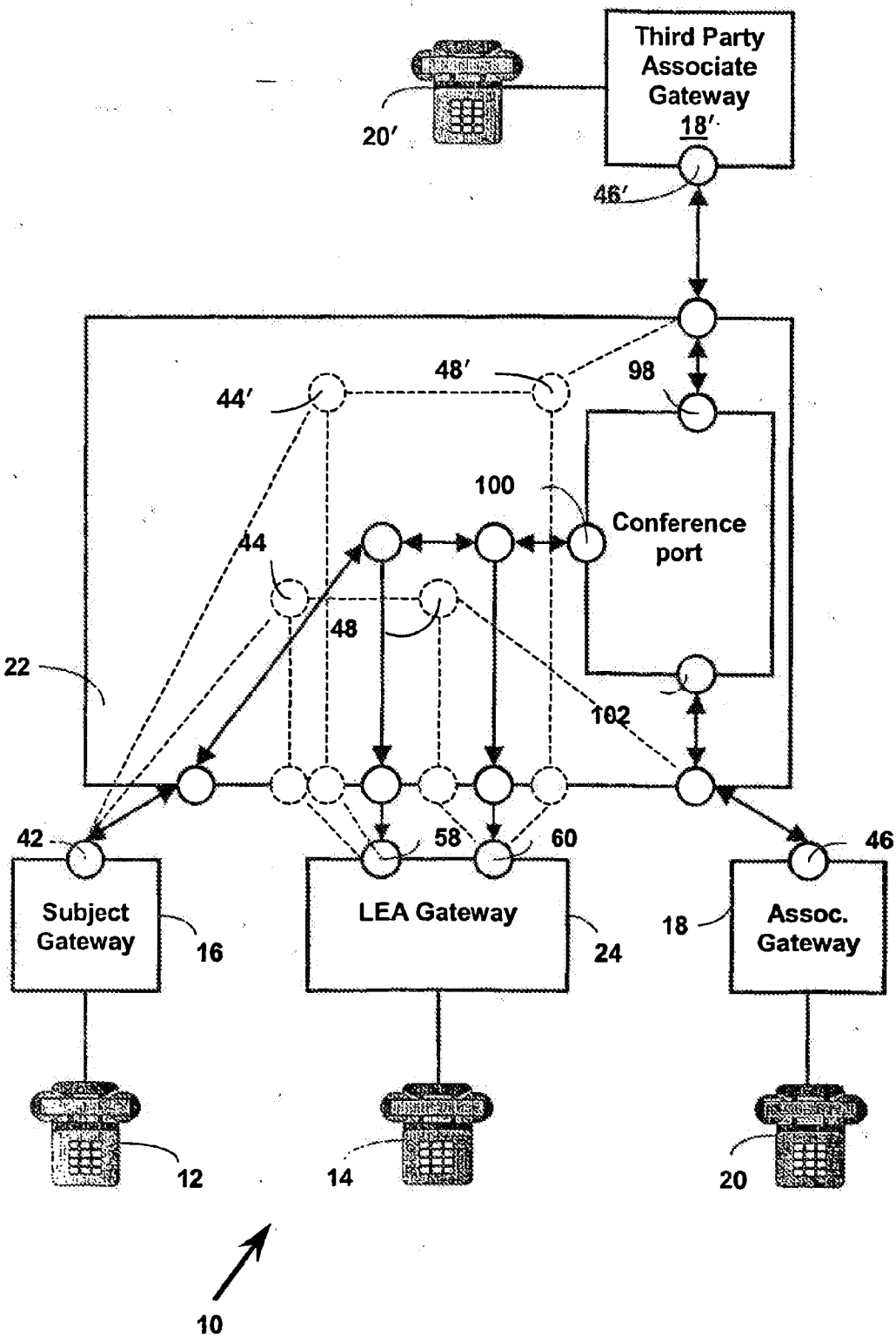


Figure 9

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 9917499 A **[0006]**
- WO 0056029 A **[0007]**
- WO 0042742 A **[0007]**

Espacenet

Bibliographic data: EP1974304 (A2) — 2008-10-01

SYSTEM AND METHOD FOR PROVIDING MEDICAL AND CONTACT INFORMATION DURING AN EMERGENCY CALL

Inventor(s): PATEL SUBODH M [US]; BROOKS ANTOINE P [US] ± (PATEL, SUBODH, M, ; BROOKS, ANTOINE, P)

Applicant(s): MEDICAL ENVELOPE L L C [US] ± (MEDICAL ENVELOPE L.L.C)

Classification: **- international:** ***A61B5/00; G06F19/00; H04M11/00;*** *H04W12/06; H04W4/22; H04W76/02; H04W8/20; H04W8/26*

- cooperative: **G06F21/6245;** G06F2221/2115; H04M2203/354; H04M2203/553; H04M2207/18; H04M2242/04; H04M3/42042; H04M3/42068; H04M3/42348; H04M3/5116; H04W12/06; H04W4/22; H04W76/007; H04W76/02; H04W8/20; H04W8/26

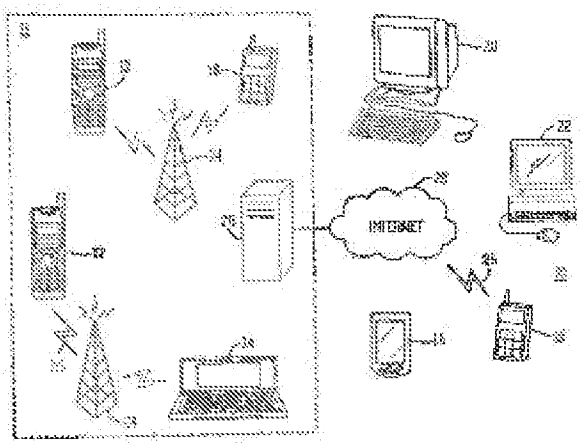
Application number: EP20060848356 20061228

Priority number(s): WO2006US49603 20061228 ; US20060759524P 20060117

Also published as: EP1974304 (A4) WO2007087077 (A2) WO2007087077 (A3) US2008188198 (A1) US2009214000 (A1)

Abstract not available for EP1974304 (A2)
Abstract of corresponding document: WO2007087077 (A2)

A system and method for providing medical and contact information of a subscriber initiating an emergency 911 call, directly to a response center at the time of the receipt of the emergency 911 call. Upon the initiation of an emergency 911 call, the existing infrastructure equipment of a communication service provider are able to access a central server containing the medical and contact information of a subscriber, and relay that information directly to a response center to speed response time and response



effectiveness. Alternatively, an agent resident on a communications device used by a subscriber can store and maintain medical and contact information of the subscriber, as well directly transmit the medical and contact information to the response center.; In addition, a subscriber has the ability to access, view, and modify his or her medical and contact information through an appropriate interface allowing interaction with either the central server or the agent.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 1 974 304 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2007/087077 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2007/087077 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2007/087077 (art. 153(3) CBE).

Espacenet

Bibliographic data: EP1974304 (A4) — 2009-08-26

SYSTEM AND METHOD FOR PROVIDING MEDICAL AND CONTACT INFORMATION DURING AN EMERGENCY CALL

Inventor(s): PATEL SUBODH M [US]; BROOKS ANTOINE P [US] ± (PATEL, SUBODH, M, ; BROOKS, ANTOINE, P)

Applicant(s): MEDICAL ENVELOPE L L C [US] ± (MEDICAL ENVELOPE L.L.C)

Classification: **- international:** ***A61B5/00; G06F19/00; H04M11/00;*** *H04W12/06; H04W4/22; H04W76/02; H04W8/20; H04W8/26*

- cooperative: **G06F21/6245;** G06F2221/2115; H04M2203/354; H04M2203/553; H04M2207/18; H04M2242/04; H04M3/42042; H04M3/42068; H04M3/42348; H04M3/5116; H04W12/06; H04W4/22; H04W76/007; H04W76/02; H04W8/20; H04W8/26

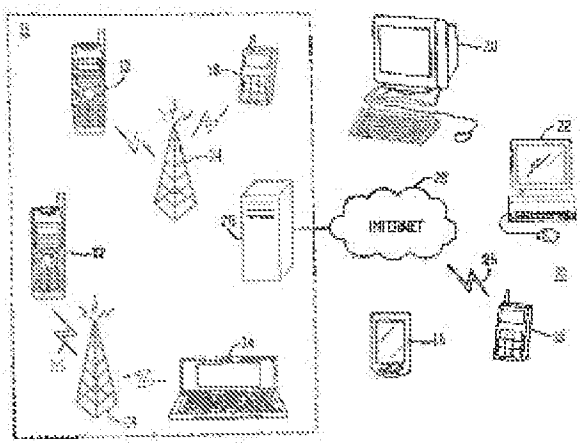
Application number: EP20060848356 20061228

Priority number(s): WO2006US49603 20061228 ; US20060759524P 20060117

Also published as: EP1974304 (A2) WO2007087077 (A2) WO2007087077 (A3) US2008188198 (A1) US2009214000 (A1)

Abstract not available for EP1974304 (A4)
Abstract of corresponding document: WO2007087077 (A2)

A system and method for providing medical and contact information of a subscriber initiating an emergency 911 call, directly to a response center at the time of the receipt of the emergency 911 call. Upon the initiation of an emergency 911 call, the existing infrastructure equipment of a communication service provider are able to access a central server containing the medical and contact information of a subscriber, and relay that information directly to a response center to speed response time and response



effectiveness. Alternatively, an agent resident on a communications device used by a subscriber can store and maintain medical and contact information of the subscriber, as well directly transmit the medical and contact information to the response center.; In addition, a subscriber has the ability to access, view, and modify his or her medical and contact information through an appropriate interface allowing interaction with either the central server or the agent.

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 06 84 8356

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 1 361 774 A (CIT ALCATEL [FR]) 12 November 2003 (2003-11-12) * paragraphs [0008], [0015] - [0017], [0019] - [0022], [0031], [0034] *	1-17	INV. G06F19/00 A61B5/00 H04M11/00
X	US 2002/057764 A1 (SALVUCCI ANGELO [US] ET AL) 16 May 2002 (2002-05-16) * paragraphs [0075], [0082], [0083], [0087], [0093], [0130] - [0147] *	1-5,12, 14,16	
X	WO 2004/051976 A (SONY ERICSSON MOBILE COMM AB [SE]; ESQUE BRIAN [US]; DERLER RAY [US];) 17 June 2004 (2004-06-17) * page 8, lines 6-17 * * page 12, lines 1-6 *	6-10,13, 15,17	
A	US 6 671 350 B1 (OXLEY L THOMAS [US]) 30 December 2003 (2003-12-30) * the whole document *	1-5,12, 14,16	

TECHNICAL FIELDS SEARCHED (IPC)

H04M
H04Q

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
The Hague	16 July 2009	Punte, Guus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 84 8356

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-07-2009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1361774 A	12-11-2003	NONE	
US 2002057764 A1	16-05-2002	NONE	
WO 2004051976 A	17-06-2004	AU 2003282265 A1	23-06-2004
		CN 1745567 A	08-03-2006
		DE 60316986 T2	24-07-2008
		EP 1568204 A2	31-08-2005
		JP 2006509395 T	16-03-2006
		US 2004203622 A1	14-10-2004
US 6671350 B1	30-12-2003	NONE	

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 610 583 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.08.2009 Bulletin 2009/35

(51) Int Cl.:
H04W 4/00 *(2009.01)*

(21) Application number: **05253822.0**

(22) Date of filing: **21.06.2005**

(54) **A method of providing a unique call back number for wireless 9-1-1 calls**

Verfahren zur Bereitstellung einer eindeutigen Rückrufnummer für schnurlose 9-1-1 Anrufe

Procédé pour fournir un numéro de rappel unique pour les appels sans fil au 9-1-1

(84) Designated Contracting States:
DE FR GB

(30) Priority: **24.06.2004 US 582615 P**
25.06.2004 US 877011

(43) Date of publication of application:
28.12.2005 Bulletin 2005/52

(73) Proprietor: **c/o LUCENT TECHNOLOGIES INC.**
Murray Hill NJ 07974-0636 (US)

(72) Inventor: **Rollender, Douglas Harold**
Bridgewater, NJ 08807 (US)

(74) Representative: **Sarup, David Alexander**
Alcatel-Lucent Telecom Limited
Unit 18, Core 3, Workzone
Innova Business Park
Electric Avenue
Enfield
EN3 7XU (GB)

(56) References cited:
US-A- 5 864 755 **US-A1- 2002 111 159**

- **JEFFREY M. PFAFF: "SPRINT PCS COMMENTS, Enhanced 911 Emergency Calling Systems" DA 00-1975, [Online] 18 September 2000 (2000-09-18), pages 1-17, XP002347969 Washington, D.C. 20554 Retrieved from the Internet: URL:http://www.wutc.wa.gov/webdocs.nsf/0/c551ce36f524ed198825696d007f35a0/$FILE/Comm ents.pdf> [retrieved on 2005-10-05]**

EP 1 610 583 B1

Description

BACKGROUND OF THE INVENTION

I. FIELD OF THE INVENTION

[0001] The present invention relates to telecommunications, and more particularly, to wireless communications.

II. DESCRIPTION OF THE RELATED ART

[0002] Emergency service calls in North America may be originated by dialing "9-1-1." Other parts of the world may use another abbreviated string of dialable digits, such as "6-1-1" in Mexico, for example. These abbreviated string of digits are intended to simplify an emergency call for help with an easy to remember number. These emergency calls may be routed to a local Public Service Answering Point ("PSAP") call center to enable the initiation of an emergency response (e.g., police, fire department, road repair, and/or ambulance) while the caller is kept on the phone. If, however, the call is somehow disconnected or dropped before the emergency is completely reported or the responder arrives, the PSAP call center may be required to call back the originator.

[0003] Presently, a record for a "9-1-1" call originated through a wired network may include Automatic Line Identification ("ALI") or the telephone number of the access line from which the call originated. The directory number ("DN") or telephone number of a wireless subscriber may not, however, be associated with a physical line or wireless unit. Calls to a roaming wireless subscriber are routed to the wireless unit by way of the mobile station identification ("MSID"), as opposed to the mobile DN ("MDN"). U.S. Patent 5,864,755 to N.J. King et al. discloses a system in which a pool of inward dialing numbers are shared between unregistered mobile units, each inward dialing number being assigned for a limited amount of time only. U.S. Patent 5,689,548 to Maupin et al. discloses a method for establishing an emergency call connection towards a Public Safety Answering Point (PSAP) terminal for a mobile subscriber, where instead of transmitting the Mobile Station Integrated Service Directory Number (MSISDN) assigned to the mobile station, a directory number assigned to the serving mobile switching center/visitor location register (MSC/VLR) is transmitted as the Calling Party Number.

[0004] Accordingly, performing an emergency call back to a wireless unit poses hurdles not encountered with landline devices, for example.

[0005] The MSID may typically be characterized as either a 10-digit mobile identification number ("MIN") or a 15-digit International Mobile Subscriber Identifier ("IMSI"). The IMSI may be programmed into a wireless unit or a Subscriber Identity Module ("SIM") card by the service provider with whom the wireless unit user has entered into a service agreement. Accordingly, the MSID may not necessarily be a dialable number.

[0006] The DN of a wireless unit is a dialable number. The DN is dialed by a caller and used to route a call through the network to the wireless subscriber's home system. At the subscriber's home system, the home location register ("HLR") contains the MSID associated with the subscriber's DN. The MSID, as opposed to the DN, may then be used to route the call through the network to the serving wireless system and page the subscriber. The subscriber's DN may be provided to the serving system from the SIM card through the wireless unit or by the home system to the serving system in a separate data file called the subscriber profile.

[0007] The rollout of systems employing a separate number for DN and MSID is a relatively recent occurrence for some wireless systems. Others have used this technique since their inception. Historically, the mobile identification number of a wireless unit was the same as the DN for some systems, particularly in systems supportive of TIA/EIA-41 standards, prior to implementing wireless number portability ("WNP") or thousands block number pooling ("TBNP") based on the Local Routing Number ("LRN") method and international roaming ("IR"). However, with WNP and TBNP, the MDN became "portable" or "poolable" from one service provider to another service provider. Since MSID may not be portable or poolable, the recipient service provider may assign a new MSID for a subscriber with a ported-in or pooled MDN.

[0008] International roaming has also forced the separation of MSID and MDN. While the MIN is a 10-digit number modeled after the North American Numbering Plan's 10-digit MDN, other nation's carriers using a different directory numbering plan may not allow their subscriber's DN to be equivalent to the internationally recognized MIN format. Another standard MSID is the IMSI. It may be used in TIA/EIA-41 and GSM systems around the world. IMSI is a 15-digit non-dialable number based on ITU-T Recommendation E.212, and therefore, may not serve as a 10 digit MDN.

[0009] Historically, when the MDN was the same as the MIN, the MIN would be delivered to a PSAP call center and would be used as a call back number. With the separation of MIN and MDN as described above, it became necessary to deliver the MDN as a separate call back number to the PSAP call center, as well as the caller's MSID. There are certain problems, however, associated with implementing this solution. One issue is that the serving system may not have the caller's MDN, only the MSID, to present to the PSAP call center with the call. Some of the reasons for this relate to the way MSID-MDN separation has been implemented according to standards. Another reason is that the network interface used to deliver the call to the PSAP call center may not have the capacity to signal both the DN and MSID or, in some cases, even a full DN.

[0010] An old serving TIA/EIA-41 system may not support WNP, TBNP or IR. This means that the older serving system may be expecting the MIN and the MDN to be

the same. The older system would not even know to look for a separate MDN in the subscriber's service profile (e.g., keyed on MIN, not MDN). With this limitation, these subscribers may not be allowed to use basic services, but they must be allowed to call for emergency services. As a result, a roamer who dials "9-1-1" while on an old system will have his or her call delivered to the PSAP call center with an MSID but no MDN. Accordingly, no call back is possible.

[0011] A newer serving system that is WNP and IR capable may not be able to deliver MDN to the PSAP call center. This could happen if the calling wireless unit is not registered with any service provider (e.g., there are mobile phones used for emergency calls only). These wireless units may be referred to as non-subscriber initialized ("NSI") phones. It is also possible for a subscriber to place an emergency call before the HLR has responded to the serving system with the subscriber's service profile containing the DN. Even if the PSAP call center has been provided with a working DN for callback, the callback to the DN will not go through if the subscriber has call forwarding service for all inbound calls or if the subscriber has a limited, pre-paid service and there is no remaining balance available to pay for the inbound callback from the PSAP call center. Further, if the callback number is to a visiting international roamer, the PSAP call center may need to place an international call. Some PSAP call center may not have the ability to callback an international number. There is also the risk of network congestion or delay in completing an international call that would be detrimental to handling an emergency in a timely manner. Some PSAP call centers may not even be equipped to place any outbound calls through separate, outbound administrative lines.

[0012] The call back DN for an international roamer would require the PSAP call center to place an international call to reach a subscriber in their local Emergency Service Zone ("ESZ"). This is not a practical, timely or sufficiently reliable solution for a PSAP call center that normally does not place international calls and for applications that may require immediate call back information for emergency purposes. In addition, the entire international MDN (up to 15 digits including a country code) may not be presented to the PSAP call center for call back if the PSAP call center only supports 10 digits.

[0013] It is also possible that the calling wireless unit is not registered with any service provider. As a result, there may be no DN associated with the wireless unit or no permanent MSID encoded in the wireless unit - such wireless units are referred to as NSI mobile phones, for example. This could be because (a) the NSI phone was never intended to be registered (there are such phones to use for emergency calls only), (b) the phone is new and has not yet been initialized by a service provider, (c) the subscription has expired and the NSI phone is no longer registered with a service provider or (d) the SIM card is lost, stolen, or simply never been inserted or been removed either advertently or inadvertently.

[0014] Some wireless units also support a removable User Identity Module ("R-UIM") or SIM that may contain the MSID and the DN. If the R-UIM or SIM are not in the phone, then it can still be used to place an emergency call. However, there is no DN or MSID known to the phone or the serving system to provide the PSAP call center as a call back number.

[0015] Every MS contains a unique mobile equipment identification number ("MEIN") encoded in the phone by the manufacturer. The MEIN may be, for example, an electronic serial number ("ESN"), as used in ANSI/TIA/EIA-41 systems or an International Mobile Equipment Identity ("IMEI") used in GSM systems. The MEIN is independent of the MSID and DN. The MEIN is signaled over the air between the wireless unit and the base station of a wireless system with a call origination attempt or soon thereafter. For example, if not supplied with the call origination attempt, the MEIN may be requested by the serving system.

[0016] Current standards for wireless emergency services call for delivering "9-1-1 + the last seven digits of the MEIN" to the PSAP call center as the form call back number when the directory number assigned to the wireless subscriber is not available. While this may serve to notify the PSAP call center that no working callback number is available with the call, the string of "9-1-1 + the last seven digits of the MEIN (MEIN7)" do not uniquely identify the call (i.e., many emergency calls may be identified by the same "9-1-1+MEIN7) and is not a routable number through the network. This is because the "9-1-1 + the last seven digits of the MEID" do not contain a complete MEID, and therefore is not unique.

[0017] While the hereinabove approach provides the PSAP call center with some measure for performing an emergency call back of a wireless unit, several hurdles still exist. For example, the callback number for a wireless unit in certain circumstances may be nothing more than a dummy number with user location data. Consequently, a need exists for a method and system architecture for uniquely identifying each wireless unit originating a "9-1-1" call. Furthermore, there is a demand for a unique identifier that may be used to enable the PSAP call center to launch a call back of the wireless unit originating a "9-1-1" call.

SUMMARY OF THE INVENTION

[0018] Methods according to the present invention are set out in the independent claims, to which the reader is now referred. Preferred features are laid out in the dependent claims.

[0019] The present invention provides for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, the present invention provides for enabling the call back of a wireless unit originating a "9-1-1" call using a unique identifier. For the purposes of the present disclosure, a unique identifier may correspond with a unique call back number for enabling an

emergency call center (e.g., a local public service answering point) to launch a call back of the wireless unit (s) that originated the "9-1-1" call. This unique call back number may be generated from a string of numbers corresponding with a local public safety number ("LPN") associated with wireless network infrastructure element(s), such as a mobile switching center ("MSC"), for example.

[0020] In an embodiment of the present invention, a method includes the step of receiving one or more routing tags associated with a wireless unit originating a "9-1-1" call. A routing tag may comprise, for example, a string of numbers corresponding with Emergency Service Routing Digits ("ESRD") and/or an Emergency Service Routing Key ("ESRK"). In addition to the routing tag, a mobile equipment identification number ("MEIN") and/or a paging identity ("PGID") may also be received by a database accessible by wireless network infrastructure elements, such as an MSC, as well as the emergency call center, including the local public service answering point, for example. In response to this receiving step, at least one unique identifier (e.g., unique call back number) may be generated. This unique identifier may be a dialable number to enable the emergency call center to call back the wireless unit originating the "9-1-1" call. Thereafter, the unique identifier may be transmitted back to the MSC, along with the emergency call center, for example. Consequently, an emergency call back may be launched by the emergency call center using the unique identifier to reach the MSC generally, and more particularly, the wireless unit originating the "9-1-1" call.

These and other embodiments will become apparent to those skilled in the art from the following detailed description read in conjunction with the appended claims and the drawings attached hereto.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The present invention will be better understood from reading the following description of non-limiting embodiments, with reference to the attached drawings, wherein below:

> **FIGS. 1** and **2** depict an architecture and flow chart of an embodiment of the present invention; and
> **FIGS. 3** and **4** depict alternate embodiments of the present invention.

[0022] It should be emphasized that the drawings of the instant application are not to scale but are merely schematic representations, and thus are not intended to portray the specific dimensions of the invention, which may be determined by skilled artisans through examination of the disclosure herein.

DETAILED DESCRIPTION

[0023] The present invention provides for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, the present invention provides for enabling the call back of a wireless unit originating a "9-1-1" call using a unique identifier. For the purposes of the present disclosure, a unique identifier may correspond with a unique call back number for enabling an emergency call center (e.g., a local public service answering point) to launch a call back of the wireless unit (s) that originated the "9-1-1" call. This unique call back number may be generated from a string of numbers corresponding with a local public safety number ("LPN") associated with wireless network infrastructure element(s), such as a mobile switching center ("MSC"), for example.

[0024] Referring to **FIG. 1,** an embodiment of the present invention is illustrated. **FIG. 1** is reflective of an architecture **10** of a network reference model ("NRM") supporting mobile emergency service is shown. Architecture **10** supports the unique identification of a wireless unit originating an emergency "9-1-1" call and for enabling the call back of the wireless unit originating the emergency "9-1-1" call using a unique identifier.

[0025] As shown in **FIG. 1,** a wireless unit **20** is shown for communicating an emergency "9-1-1" call to architecture **10.** For the purposes of the present disclosure, an emergency "9-1-1" call corresponds with a call and/or a request for emergency services (e.g., police, fire department, road repair, and/or ambulance). The communication, as originated by wireless unit **20,** is conveyed to a mobile switching center **40** ("MSC") through a base station (not shown).

[0026] Once the emergency "9-1-1" call is received by MSC **40,** identification information associated with wireless unit **20** may be communicated to a serving system emergency call register **50** ("SS-ECR"). More particularly, the information associated with wireless unit **20** includes, for example, a mobile equipment identification number ("MEIN"). The transfer of the MEIN to ECR-SS **50** is performed by MSC **40** over a first NRM interface, E_x. It should be noted that the MEIN, as transferred to SS-ECR **50**, might be realized by an International Mobile Equipment Identity ("IMEI"), electronic serial number ("ESN"), pseudo ESN ("pESN") and/or mobile equipment identity ("MEID").

[0027] Along with transferring the MEIN, MSC **40** may also communicate a paging identity ("PGID") to SS-ECR **50.** In the event that the emergency "9-1-1" call from wireless unit **20** is dropped or disconnected from the base station and MSC **40,** the PGID may be used to page wireless unit **20.** To page wireless unit **20** in the circumstance of a call drop or disconnect, a local public safety number ("LPN") of MSC **40** may be needed to uniquely identify the switch serving "9-1-1" caller (e.g., wireless unit **20).** The LPN may be realized by a dialable number from a native or non-portable number block assigned to MSC **40.** The LPN may assist in identifying SS-ECR **50** and for originating a call back to the wireless unit originating the emergency "9-1-1" call in the event of a call drop or disconnect occurs.

[0028] In addition to the LPN, Emergency Service

Routing Digits ("ESRD") or Emergency Service Routing Key ("ESRK") may also be employed for uniquely identifying the emergency "9-1-1" call. ESRD may not uniquely identify the emergency "9-1-1" call, while ESRK may support the communication of location information of wireless unit **20,** as associated with the emergency "9-1-1" call. The network elements and interfaces involved in providing an ESRK may be realized, in one embodiment, using existing communication standards. It should be noted that the Emergency Service Routing Digits may include, in one example, a string of numbers associated with a cell sector of the mobile switching center in which the emergency call originates, while the Emergency Service Routing Key may include a string of numbers associated with at least one of a mobile positioning center and/or geographical mobile location center **90.**

[0029] From the hereinabove, the PGID may be one of a number of communication standards-based identifiers supporting paging wireless unit **20** to deliver an inbound call if the emergency "9-1-1" call is dropped or disconnected. With respect to a GSM-based system, wireless unit **20** may be paged via an international mobile station identity ("IMSI") provided by wireless unit **20**, a temporary mobile station identity ("TMSI") associated with the IMSI and/or an IMEI from wireless unit **20.** In a CDMA2000 system, this paging step may be realized using a mobile identification number ("MIN"), an IMSI, a default mobile station identity ("dMSID") from a non-subscriber initiated ("NSI") wireless unit(s), an ESN from wireless unit **20** and/or a pESN generated from an MEID within wireless unit **20.**

[0030] With identification information associated with wireless unit **20** received from MSC **40,** ECR-SS **50** may then redirect this information over a network interface, E_y, to another emergency call register ("ECR") **60** associated with a public service answering point ("PSAP") **70**. Consequently, the MEIN, LPN, dMSID, ESRK and/or a unique identifier (e.g., unique call back number or "UCBN") may be re-transmitted from SS-ECR **50** to ECR **60.** It should be noted that ECR **60** might be realized by a database. Other associated databases in, however, may be keyed on the ESRK, the MEIN, the mobile station identity (e.g., MIN or IMSI) and/or the directory number of the caller.

[0031] The E interfaces depicted support signaling of emergency data and service requests through architecture **10** between MSC **40** and PSAP **70.** Call handling instructions from PSAP **70,** such as to establish a call-back through MSC **40**, may be communicated from PSAP **70** to ECR **60** over an E_d interface, on to SS-ECR **50** through an E_y interface and from SS-ECR **50** to MSC **40** through an E_x interface. Here, PSAP **70** may communicate with ECR **60** directly over the E_d interface using a unique identifier (e.g., a unique call back number) as a key. Alternatively, PSAP **70** may communicate with ECR **60** indirectly through an automatic line identifier ("ALI") database **80** over the D and E_z interfaces using ESRK or the unique identifier (e.g., a unique call back number) as key.

[0032] SS-ECR **50** and ECR **60** may be implemented as a single entity. As shown, however, SS-ECR **50** and ECR **60** are individual elements to allow consideration for one SS-ECR to serve one MSC and one SS-ECR to interface with many ECRs associated with PSAP **70.** In addition, while one ECR may serve many PSAPs, one PSAP need only interface with one ECR. Moreover, PSAP **70** may have access to information in many ECRs through ECR networking over the E_w interface.

[0033] Referring to **FIG. 2,** a flow chart depicting another embodiment of the present invention is illustrated. More particularly, an algorithmic method **(100)** is shown for uniquely identifying one or more wireless units originating a "9-1-1" call. More particularly, algorithmic method **(100)** enables the call back of a wireless unit originating a "9-1-1" call using a unique identifier. This is of particularly relevance if the originating emergency "9-1-1" call was terminated.

[0034] The algorithmic method **(100)** of **FIG. 2** may initially include the step of receiving a routing tag (step **110).** A routing tag is associated with a wireless unit originating a "9-1-1" call and may, for example be transmitted by mobile switching center **40** and received by emergency call register **50** of **FIG. 1.** For the purposes of the present disclosure, a routing tag may comprise, for example, a string of numbers corresponding with Emergency Service Routing Digits ("ESRD") and/or an Emergency Service Routing Key ("ESRK"). Consequently, while the routing tag may identify the originating system and destination PSAP, the routing tag may not uniquely identify the emergency "9-1-1" call if it is an ESRD or may be unable to uniquely identify the emergency "9-1-1" call once the originating call is no longer in progress. It should be noted that in practice, this step of receiving may also include receiving the mobile equipment identification number ("MEIN"), as well as the paging identifier ("PGID") along routing tag. It should be also noted that, in practice, the MEIN and PGID may be received prior to the receiving of the routing tag.

[0035] Once the step of receiving a routing tag has been achieved, the algorithmic method **(100)** then includes the step of generating a unique identifier (step **120).** Unlike the routing tag, the unique identifier identify the emergency "9-1-1" call even if the originating call is no longer in progress. In one embodiment, the unique identifier may be a ten (10) digit, unique call back number associated with at least one serving mobile switching center. In one embodiment, the unique call back number comprises a string of numbers corresponding with a local public safety number ("LPN") associated with the serving mobile switching center. In one scenario, the unique call back number may comprise six (6) fixed digits associated with the LPN (e.g., NPA+NXX) and four unassigned digits (XXX). In this scenario, the four unassigned digits may translate into 10,000 unique number sequences to be assigned as a result of this generating step.

[0036] Thereafter, the algorithmic method **(100)** may

store the generated unique identifier in a database (step **130**). The database is accessible to a local emergency center. In one example, the database is realized by emergency call register **60** accessible to PSAP **70** in FIG. **1**.

[0037] Once generated, the algorithmic method **(100)** may then transmit the unique identifier (step **140).** Here, the unique identifier (e.g., unique call back number) may, for example be transmitted by emergency call register **50** and received by mobile switching center **40** of **FIG. 1.** As a result, mobile switching center **40** may identifying the emergency "9-1-1" call even if the originating call is no longer in progress. Moreover, the local emergency center, such as PSAP **70,** may also identify the emergency "9-1-1" call even if the originating call is no longer in progress, by accessing emergency call register **60.**

[0038] With the unique call back number accessible to the local emergency center, such as PSAP **70,** and mobile switching center **40,** the algorithmic method **(100)** may then form a traffic channel (step **150).** This scenario arises in the event the originating emergency "9-1-1" call from the wireless unit is no longer in progress - e.g., disconnected or terminated. After the traffic channel is formed, the local emergency center (e.g., PSAP **70**) may call back the wireless unit originated the emergency "9-1-1" call using the unique identifier (e.g., unique call back number).

EXEMPLARY EMBODIMENT

[0039] Mobile Emergency Service (E911M) requires the following items to be incorporated into wireless and Emergency Service Network standard protocols and procedures: Local Public Safety Number (LPN); Mobile Equipment Identification Number (MEIN); Mobile Equipment Paging Identity (PGID); Unique Call Back Number (UCBN); Emergency Call Register (ECR); and Mobile E9-1-1 Network.

[0040] A Local Public Safety Number (LPN) is a dialable number where the NPA-NXX uniquely identifies the MSC in the originating network. In order to avoid number portability and pooling complexities, the LPN may be taken from the native number block of the MSC.

[0041] The Mobile Equipment Identity Number (MEIN) is a unique serial number programmed into a wireless unit by the manufacturer. In CMRS phones, it may take the form of a 32-bit Electronic Serial Number (ESN) in TDMA, CDMA or Analog phones, a 15-digit International Mobile Equipment Identity (IMEI) in GSM, UMTS or PCS1900 phones or a 56-bit Mobile Equipment Identity (MEID) in CDMA2000 phones. Every phone has a MEIN but not every wireless system uses MEIN to page the phone. However, this may be modified as needed to allow a mobile phone that is used to originate an emergency 9-1-1 call to be paged for a call back with its MEIN. The alternative is to create a data field in the ECR called the Paging Identity (PGID) to store one of many possible identifiers that may be used by the serving system to page a mobile phone.

[0042] PGID may be the Mobile Subscription Identity (MSID) if it is available from the phone with the emergency 9-1-1 call origination. The MSID may be a 15-digit International Mobile Subscription Identity (IMSI) or a 10-digit Mobile Identification Number (MIN). MSID is not available with an emergency 9-1-1 call origination if a Non-Subscription Initialized (NSI) phone is used to place the call. There is no MSID programmed into a NSI phone by a service provider or in a phone without a Subscriber Identity Module (SIM card). PGID may be a Temporary Mobile Station Identity (TMSI), a default MSID (dMSID) provided by the phone manufacturer and used for Over-The-Air Activation (OTA) of a new phone, a new 56 bit MEID or a pseudo-ESN (pESN) derived from the MEID. The PGID is whatever identity a wireless phone provides for itself when it enters a system and is acceptable by that system to page that phone for a call back.

[0043] The Unique Callback Number (UCBN) is dynamically assigned at the serving system when a 9-1-1 call is originated. It is stored in the ECR as a key to the database. The UCBN is signaled with every emergency 9-1-1 call to uniquely identify the emergency 9-1-1 call, retrieve call back information from the PSAP-ECR and originate a call back. The UCBN is a unique10-digit dialable number based on the NPA-NXX from the LPN of the serving system. The last four digits are uniquely assigned to each call at the serving system. The UCBN is not a Mobile Directory Number (MDN) or Mobile Station ISDN Number (MSISDN) assigned to the calling subscriber by the home service provider. If the UCBN is used for call back, it is signaled to the serving system MSC as the Called Party Number (CPN). The MSC uses the UCBN to request a PGID from the SS-ECR. The PGID is then used to page the phone and complete the call-back.

[0044] Based on existing guidelines, the UCBN may be signaled from the MSC to the Selective Router and on to the PSAP as the Call Back Number (CBN) in the Calling Party Number (CPN) or the Charge Number (CHGN) when the ESRD is populated in either the Generic Digits Parameter (GDP) or the Called Party Number (CdPN). When the ESRK is populated as the either the CPN or CHGN, the UCBN may be populated in the other field or in the GDP.

[0045] If the UCBN is not signaled with a call routed by the ESRK, then the PSAP may use the ESRK while the call is still in progress to obtain the UCBN from the PSAP-ECR or the ALI. ALI may get the UCBN from the PSAP-ECR or the MPC. MPC may have the UCBN if it is provided by the MSC.

[0046] The Emergency Call Register (ECR) is a database holding emergency call detail information and call handling instructions for the MSC. The ECR database is keyed on the UCBN and contains the MEIN, PGID. ESRK or ESRD for the emergency 9-1-1 call, as well as the LPN of the serving system. The LPN may be updated automatically as the wireless unit originating the emergency 9-1-1 caller roams and is handed off (or over) from one

serving system to another.

[0047] ECR entries may be created in different ways. An entry may be created at the originating network with the origination of a 911 call, through a download of entries from other ECRs or by manual entry. Manual entry of a MEIN and any local LPN into a ECR associated with the PSAP allows the PSAP to call any wireless unit through the MSC even if the wireless unit was not used to originate an emergency 9-1-1 call. LPN Update procedures allow for the LPN of the serving system to be automatically entered into the SS-ECR after the wireless unit is located in the true serving system. The LPN is updated in other PSAP-ECRs and SS-ECRs through the Mobile E-9-1-1 Network.

[0048] The Mobile E9-1-1 Network may be used to exchange data between ECRs and trigger events in other network elements. An ECR is located with an MSC at the serving system (SS-ECR), a PSAP in the Emergency Services Network (PSAP-ECR), and any other call center handling emergency calls. For example, a secondary PSAP or a Telematics Call Center may have an ECR to track 9-1-1 calls and other outbound calls placed for their clients, to track inbound calls from clients or to remotely request service for clients through the serving system.

[0049] The ECR Network is used for more than exchanging emergency call information and tracking individual phones. The ECR network is also used to manage mobility for mobile phones used to place an emergency 9-1-1 call and request services through the MSC. Messages are signaled through the network to support intersystem operations for Intersystem Roaming and Emergency Short Message Service for NSI Phones and International Roamers, Emergency Call Origination through the MSC for Telematics Call Centers, PSAP-to-PSAP Call Forwarding or Conference Calling through the MSC, LPN Update, Intersystem Paging for Emergency Call Back and possibly many other services. The PSAP-ECR acts like a Home Location Register (HLR) and the SS-ECR acts like a Visitor Location Register (VLR).

[0050] Referring to **FIG. 3,** a signal flow diagram **200** according to an exemplary embodiment of the present invention is illustrated. **FIG. 3** depicts the process in the origination of an emergency "9-1-1" call by a wireless unit. Here, an emergency "9-1-1" call is originated by a wireless unit through a serving MSC using a routing tag, such as an ESRD ("Emergency Service Routing Digits") or an ESRK ("Emergency Service Routing Key"). The emergency "9-1-1" call may be routed to a geographically designated PSAP call center based on the routing tag - e.g., the corresponding ESRD or ESRK. An emergency call register ("ECR") coupled with the serving MSC and the PSAP call center may then be updated with call back information. Thereafter, a unique identifier may be generated for uniquely identifying the emergency "9-1-1" call. This unique identifier may be realized by a unique call back number derived from a local public safety number. Moreover, the routing tag - the corresponding ESRD or ESRK - may identify the originating system and destination PSAP. It should be noted that an ESRD does not uniquely identify the call, while an ESRK may be used to uniquely identify the call so long as the call is in progress.

[0051] Referring to **FIG. 4,** a signal flow diagram **300** according to another exemplary embodiment of the present invention is illustrated. **FIG. 3** depicts the process of calling back the wireless unit, which originated the emergency "9-1-1" call. After the original emergency "9-1-1" call was terminated, the PSAP may dial the unique identifier (e.g., unique call back number) derived from a local public safety number to reach the wireless unit originating the emergency "9-1-1" call. Here, the MSC uses the unique identifier to retrieve an associated paging identifier ("PGID") from a serving system emergency call register ("SS-ECR"), page the wireless unit and then complete the call back to the wireless unit. Alternatively, the PSAP may use the unique identifier or the mobile equipment identification number to request a call back from through the MSC from the PSAP emergency call register ("PSAP-ECR").

[0052] While the particular invention has been described with reference to illustrative embodiments, this description is not meant to be construed in a limiting sense. It is understood that although the present invention has been described, various modifications of the illustrative embodiments, as well as additional embodiments of the invention, will be apparent to one of ordinary skill in the art upon reference to this description without departing from the spirit of the invention, as recited in the claims appended hereto.

[0053] Consequently, the method, system and portions thereof and of the described method and system may be implemented in different locations, such as the wireless unit, the base station, a base station controller and/or mobile switching center, for example. Moreover, processing circuitry required to implement and use the described system may be implemented in application specific integrated circuits, software-driven processing circuitry, firmware, programmable logic devices, hardware, discrete components or arrangements of the above components as would be understood by one of ordinary skill in the art with the benefit of this disclosure. Those skilled in the art will readily recognize that these and various other modifications, arrangements and methods can be made to the present invention without strictly following the exemplary applications illustrated and described herein. It is therefore contemplated that the appended claims will cover any such modifications or embodiments as fall within the true scope of the invention.

Claims

1. A method of communication with at least one wireless unit (20) originating an emergency call, the method comprising:

receiving (110), at a wireless communication

system, at least one routing tag associated with the at least one wireless unit from which an emergency call has been received;
generating (120), at the wireless communication system, a unique call back number in response to receiving the at least one routing tag, the unique call-back number being associated with at least one mobile switching center (40) serving the at least one wireless unit (20);
storing (130), at the wireless communication system, the unique call back number in an emergency database (60) directly accessible by a local emergency center; and
transmitting (140), from the emergency database (60) to a mobile switching center (40), the unique call-back number to uniquely identify the at least one wireless unit in response to the step of receiving at least one routing tag.

2. The method of claim 1, further comprising:

storing the unique call back number in association with the at least one routing tag.

3. The method of claim 2, further comprising:

storing a paging identity other than a mobile directory number in association with the unique call back number and the routing tag, the paging identity being an identifier of the wireless unit used to page the wireless unit.

4. The method of claim 3, wherein the paging identity is one of a mobile station
subscriber identification, an international mobile subscription identity, a mobile identification number, a temporary mobile station identity, a mobile equipment identification number, and a pseudo electronic serial number.

5. The method of claim 3, further comprising:

receiving the unique call back number in an emergency call back;
accessing the paging identity using the unique call back number; and
launching an emergency call back to the mobile station using the accessed paging identity.

6. The method of claim 1, further comprising:

transmitting the at least one routing tag associated with the at least one wireless unit to a system database (50);
receiving, from the system database (50), the unique call-back number in response to the step of transmitting the at least one routing tag; and
sending the emergency call to a public service answering point using the unique call back number as the calling party number.

7. The method of claim 6, wherein the transmitting step transmits the routing tag and a paging identity, the paging identity being an identifier of the wireless unit used to page the wireless unit.

8. The method of claim 7, comprising:

receiving the unique call back number in an emergency call back;
sending the unique call back number to the database; and
launching the emergency call back to the mobile station using the paging identity.

9. The method of claim 7, wherein the paging identity is one of a mobile station
subscriber identification, an international mobile subscription identity, a mobile identification number, a temporary mobile station identity, a mobile equipment identification number, and a pseudo electronic serial number.

10. The method of claims 1 or 6, wherein the at least one routing tag comprises a string of numbers corresponding with at least one of a Emergency Service Routing Digits and a Emergency Service Routing Key.

11. The method of claim 10, wherein the Emergency Service Routing Digits comprises a string of numbers associated with a cell sector of the mobile switching center in which the emergency call originates, and the Emergency Service Routing Key comprises a string of numbers associated with at least one of a mobile positioning center and geographical mobile location center.

Patentansprüche

1. Ein Verfahren zur Kommunikation mit mindestens einem Mobilfunkendgerät (20), welches einen Notruf erzeugt, wobei das Verfahren umfasst:

Empfangen (110), an einem drahtlosen Kommunikationssystem, von mindestens einem Routing-Tag, welcher mit dem mindestens einem Mobilfunkendgerät, von welchem der Notruf empfangen wurde, assoziiert ist;
Erzeugen (120), an dem drahtlosen Kommunikationssystem, einer eindeutigen Rückrufnummer in Reaktion auf den Empfang des mindestens einen Routing-Tags, wobei die eindeutige Rückrufnummer mit mindestens einer Mobilfunkvermittlungsstelle (40), welche mindestens

ein Mobilfunkendgerät (20) bedient, assoziiert ist;
Speichern (130), an dem drahtlosen Kommunikationssystem, der eindeutigen Rückrufnummer in einer Notfall-Datenbank (60), welche direkt für eine lokale Notfallzentrale zugänglich ist; und
Übertragen (140) der eindeutigen Rückrufnummer von der Notfall-Datenbank (60) an eine Mobilfunkvermittlungsstelle (40), um das mindestens eine Mobilfunkendgerät in Reaktion auf den Schritt des Empfangens von mindestens einem Routing-Tag eindeutig zu identifizieren.

2. Das Verfahren nach Anspruch 1, weiterhin umfassend:

Speichern der eindeutigen Rückrufnummer in Verbindung mit dem mindestens einen Routing-Tag.

3. Das Verfahren nach Anspruch 2, weiterhin umfassend:

Speichern einer Funkrufkennung, welche sich von der Funkrufverzeichnis-Nummer unterscheidet, in Verbindung mit der eindeutigen Rückrufnummer und dem Routing-Tag, wobei die Funkrufkennung eine Kennung des Mobilfunkendgeräts ist, welche benutzt wird, um das Mobilfunkendgerät zu rufen.

4. Das Verfahren nach Anspruch 3, wobei die Funkrufkennung entweder eine Mobilstation-Teilnehmerkennung, eine internationale Mobilfunk-Teilnehmerkennung, eine Mobilfunkkennungsnummer, eine temporäre Mobilstation-Identität, eine eindeutige Kennnummer zur Identifizierung des einzelnen Mobilendgeräts oder eine pseudoelektronische Seriennummer ist.

5. Das Verfahren nach Anspruch 3, weiterhin umfassend:

Empfangen der eindeutigen Rückrufnummer in einem Notrückruf;
Abrufen der Funkrufkennung unter Verwendung der eindeutigen Rückrufnummer; und
Aussenden eines Notrückrufs an die Mobilstation unter Verwendung der abgerufenen Funkrufkennung.

6. Das Verfahren nach Anspruch 1, weiterhin umfassend:

Übertragen des mindestens einen Routing-Tags, welcher mit dem mindestens einen Mobilfunkendgerät assoziiert ist, an eine Systemdatenbank (50);
Empfangen, von der Systemdatenbank (50), der eindeutigen Rückrufnummer in Reaktion auf den Schritt des Übertragens des mindestens einen Routing-Tags; und
Senden des Notrufs an eine Notrufzentrale unter Verwendung der eindeutigen Rückrufnumer als die Nummer des rufenden Teilnehmers.

7. Das Verfahren nach Anspruch 6, wobei der Schritt des Übertragens das Routing-Tag und eine Funkrufkennung überträgt, wobei die Funkrufkennung eine Kennung des Mobilfunkendgeräts ist, welche verwendet wird, um das Mobilfunkendgerät zu rufen .

8. Das Verfahren nach Anspruch 7, umfassend:

Empfangen der eindeutigen Rückrufnummer in einem Notrückruf;
Senden der eindeutigen Rückrufnummer an die Datenbank; und
Aussenden des Notrückrufs an die Mobilstation unter Verwendung der Funkrufkennung.

9. Das Verfahren nach Anspruch 7, wobei die Funkrufkennung entweder eine Mobilstation-Teilnehmerkennung, eine internationale Mobilfunk-Teilnehmerkennung, eine Mobilfunkkennungsnummer, eine temporäre Mobilstation-Identität, eine eindeutige Kennnummer zur Identifizierung des einzelnen Mobilendgeräts oder eine pseudoelektronische Seriennummer ist.

10. Das Verfahren nach den Ansprüchen 1 oder 6, wobei der mindestens eine Routing-Tag eine Kette von Zahlen, welche mindestens entweder einer Notdienst-Routingnummer oder einem Notdienst-Routingschlüssel entspricht, umfasst.

11. Das Verfahren nach Anspruch 10, wobei die Notdienst-Routingnummer eine mit einem Zellbereich der Mobilfunkvermittlungsstelle, in welcher der Notruf erzeugt wird, assoziierte Kette von Zahlen umfasst, und der Notdienst-Routingschlüssel eine mit mindestens entweder einer Zentrale zur Positionsbestimmung des Mobilendgeräts oder einer Zentrale zur geografischen Lokalisierung des Mobilendgeräts assoziierte Kette von Zahlen umfasst.

Revendications

1. Procédé de communication avec au moins une unité sans fil (20) d'où provient un appel d'urgence, le procédé comprenant les étapes de :

recevoir (110), dans un système de communication sans fil, au moins une étiquette d'ache-

minement associée à l'au moins une unité sans fil à partir de laquelle un appel d'urgence a été reçu ;
générer (120), dans le système de communication sans fil, un numéro de rappel unique en réponse à la réception de l'au moins une étiquette d'acheminement, le numéro de rappel unique étant associé à au moins un centre de commutation mobile (40) desservant l'au moins une unité sans fil (20) ;
enregistrer (130), dans le système de communication sans fil, le numéro de rappel unique dans une base de données de secours (60) directement accessible par un centre de secours local ; et
transmettre (140), à partir de la base données de secours (60) à un centre de commutation mobile (40), le numéro de rappel unique pour identifier de manière unique l'au moins une unité sans fil en réponse à l'étape de réception d'au moins une étiquette d'acheminement.

2. Procédé selon la revendication 1, comprenant en outre les étapes de :

enregistrer le numéro de rappel unique en association avec l'au moins une étiquette d'acheminement.

3. Procédé selon la revendication 2, comprenant en outre les étapes de :

enregistrer une identité de radiomessagerie différente d'un numéro de répertoire mobile en association avec le numéro de rappel unique et l'étiquette d'acheminement, l'identité de radiomessagerie étant un identifiant de l'unité sans fil utilisé pour communiquer par radiomessagerie avec l'unité sans fil.

4. Procédé selon la revendication 3, dans lequel l'identité de radiomessagerie est une identification d'abonné de station mobile, une identité internationale d'abonné mobile, un numéro d'identification mobile, une identité provisoire de station mobile, un numéro d'identification d'équipement mobile ou un pseudo numéro de série électronique.

5. Procédé selon la revendication 3, comprenant en outre les étapes de :

recevoir le numéro de rappel unique dans un rappel d'urgence ;
accéder à l'identité de radiomessagerie en utilisant le numéro de rappel unique ; et
lancer un rappel d'urgence à la station mobile en utilisant l'identité de radiomessagerie ayant fait l'objet d'un accès.

6. Procédé selon la revendication 1, comprenant en outre les étapes de :

transmettre l'au moins une étiquette d'acheminement associée à l'au moins une unité sans fil à une base de données de système (50) ;
recevoir, à partir de la base de données de système (50), le numéro de rappel unique en réponse à l'étape de transmission de l'au moins une étiquette d'acheminement ; et
envoyer l'appel d'urgence à un service public d'appel d'urgence en utilisant le numéro de rappel unique comme numéro d'appelant.

7. Procédé selon la revendication 6, dans lequel l'étape de transmission transmet l'étiquette d'acheminement et une identité de radiomessagerie, l'identité de radiomessagerie étant un identifiant de l'unité sans fil utilisé pour communiquer par radiomessagerie avec l'unité sans fil.

8. Procédé selon la revendication 7, comprenant les étapes de :

recevoir le numéro de rappel unique dans un rappel d'urgence ;
envoyer le numéro de rappel unique à la base de données ; et
lancer le rappel d'urgence à la station mobile en utilisant l'identité de radiomessagerie.

9. Procédé selon la revendication 7, dans lequel l'identité de radiomessagerie est une identification d'abonné de station mobile, une identité internationale d'abonné mobile, un numéro d'identification mobile, une identité provisoire de station mobile, un numéro d'identification d'équipement mobile ou un pseudo numéro de série électronique.

10. Procédé selon la revendication 1 ou 6, dans lequel l'au moins une étiquette d'acheminement comprend une chaîne de nombres correspondant aux chiffres d'acheminement de service d'urgence et/ou à une clé d'acheminement de service d'urgence.

11. Procédé selon la revendication 10, dans lequel les chiffres d'acheminement de service d'urgence comprennent une chaîne de nombres associés à un secteur de cellule du centre de commutation mobile d'où provient l'appel d'urgence et la clé d'acheminement de service d'urgence comprend une chaîne de nombres associés à un centre de positionnement mobile et/ou à un centre de géolocalisation.

FIG. 1

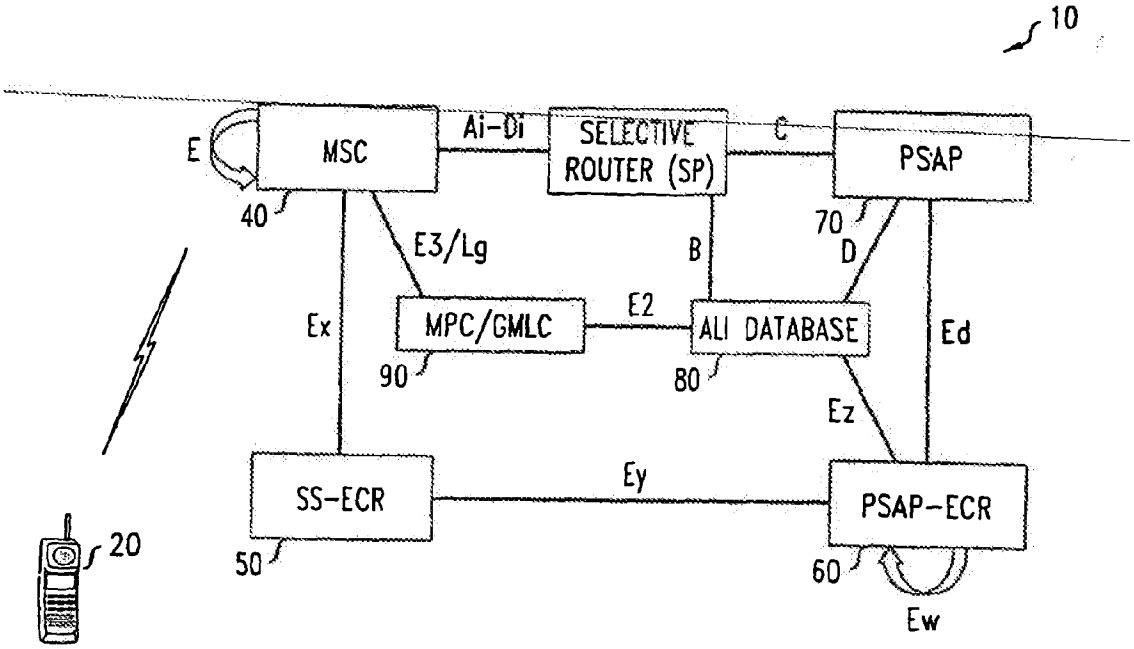
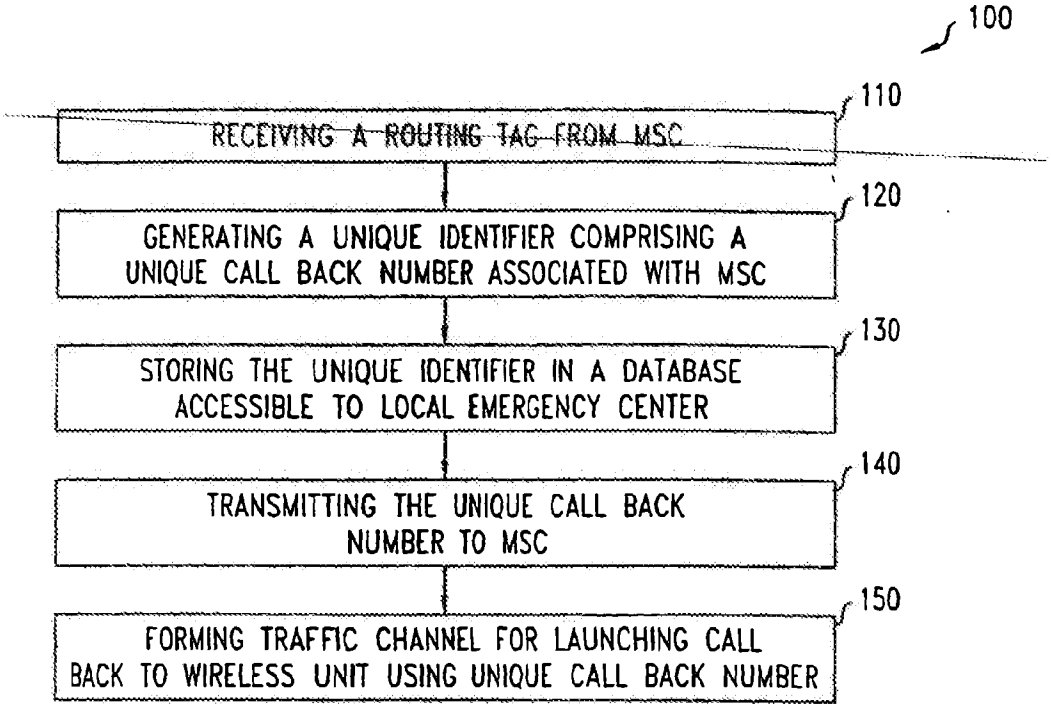

10
E
MSC
40
Ai-Di
SELECTIVE ROUTER (SP)
C
PSAP
70
E3/Lg
B
D
Ex
MPC/GMLC
90
E2
ALI DATABASE
80
Ed
Ez
SS-ECR
50
Ey
PSAP-ECR
60
Ew
20

FIG. 2



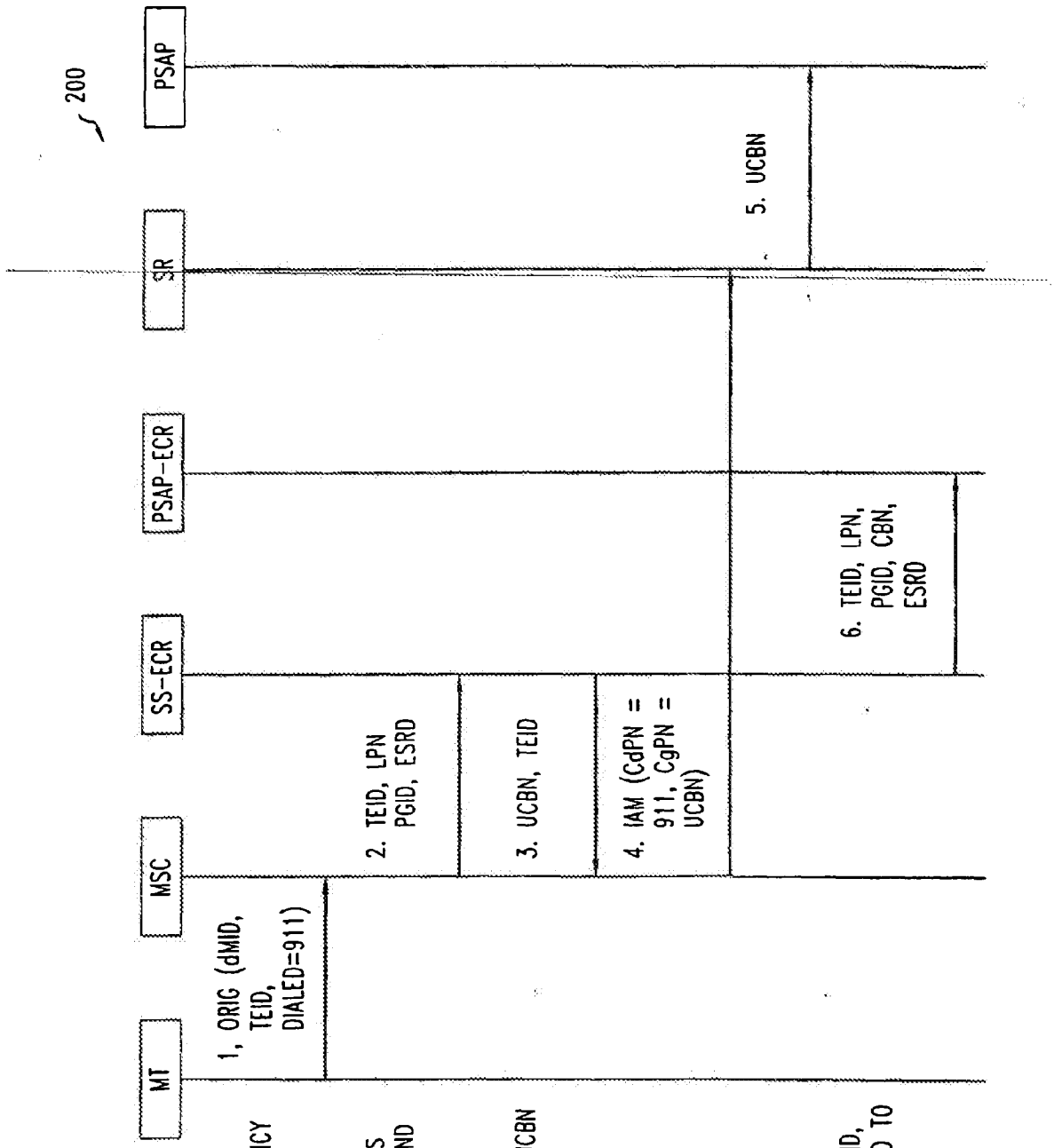
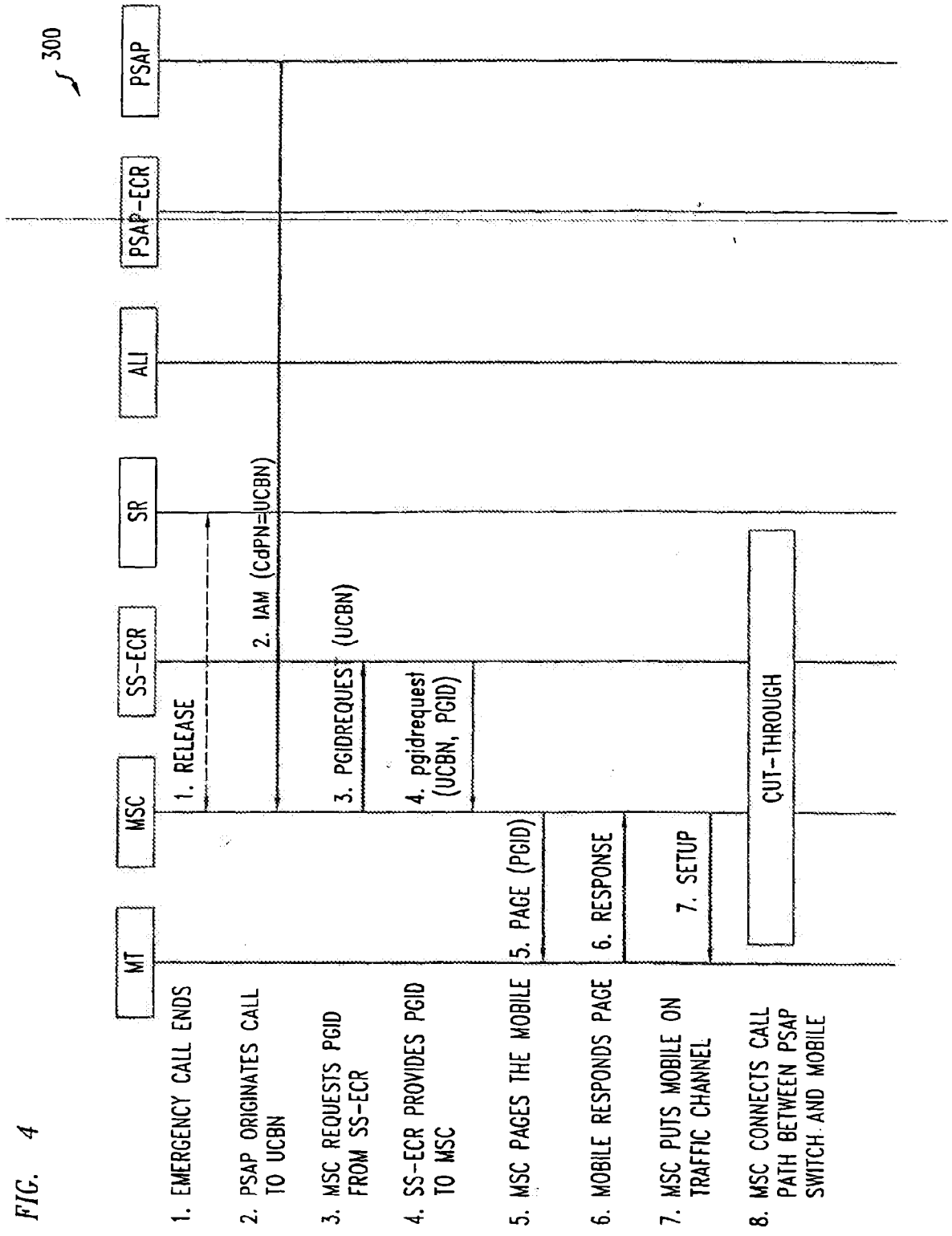

200
MT
MSC
SS-ECR
PSAP-ECR
SR
PSAP
1. ORIG (dMID, TEID, DIALED=911)
2. TEID, LPN PGID, ESRD
3. UCBN, TEID
4. IAM (CdPN = 911, CgPN = UCBN)
5. UCBN
6. TEID, LPN, PGID, CBN, ESRD
1. MOBILE TERMINAL ORIGINATES EMERGENCY CALL
2. SERVING MSC ENTERS TEID, LPN, dMSID, AND ESRD IN SS-ECR
3. SS-ECR PROVIDES UCBN TO MSC
4. MSC SIGNALS CBN TO PSAP
5. SR SIGNALS CBN TO PSAP
6. SS-ECR SIGNALS TEID, LPN, UCBN AND PGID TO PSAP-ECR

FIG. 3

FIG. 4



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5864755 A, N.J. King **[0003]**
- US 5689548 A, Maupin **[0003]**

Espacenet

Bibliographic data: EP2127232 (A1) — 2009-12-02

SYSTEM AND METHOD FOR RECORDING AND MONITORING COMMUNICATIONS USING A MEDIA SERVER

Inventor(s): WYSS FELIX IMMANUEL [US]; SNYDER MICHAEL D [US]; O'CONNOR KEVIN [US] ± (WYSS, FELIX, IMMANUEL, ; SNYDER, MICHAEL, D, ; O'CONNOR, KEVIN)

Applicant(s): INTERACTIVE INTELLIGENCE INC [US] ± (INTERACTIVE INTELLIGENCE, INC)

Classification: **- international:*H04L12/28; H04L29/06; H04M3/51***
- cooperative: H04L63/00; H04L63/1425; H04L63/30; H04L65/605; H04M3/2281; H04M3/42221; H04M3/51; H04L65/1006; H04L65/104

Application number: EP20080730132 20080219

Priority number (s): WO2008US54271 20080219 ; US20070678315 20070223

Also published as: EP2127232 (A4) WO2008103652 (A1) US2012195415 (A1) US2008205378 (A1) US8427981 (B2)

Abstract not available for EP2127232 (A1)
Abstract of corresponding document: WO2008103652 (A1)

A communication system including a media server through which communication packets are exchanged for recording and monitoring purposes is disclosed. A tap is associated with each communication endpoint allowing for cradle to grave recording of communications despite their subsequent routing or branching. An incoming communication is routed to a first tap and upon selection of a receiving party; the first tap is routed to a second tap which forwards communication packets on to the receiving party. The taps may be used to forward communication packets to any number of other taps or destinations, such as a recording device, monitoring user, or other user in the form of a conference.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 127 232 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2008/103652 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2008/103652 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2008/103652 (art. 153(3) CBE).

Espacenet

Bibliographic data: EP2165489 (A1) — 2010-03-24

SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

Inventor(s): PURNADI RENE W [US]; ISLAM M KHALEDUL [CA] + (PURNADI, RENE W, ; ISLAM, M. KHALEDUL)

Applicant(s): RESEARCH IN MOTION LTD [CA] + (RESEARCH IN MOTION LIMITED)

Classification: **- international:*H04L12/66; H04M11/06; H04Q3/64***
- cooperative: **H04M3/5116**; **H04Q3/64**; H04L65/1016; H04M1/72538; H04Q2213/13152; H04Q2213/13176; H04Q2213/13204; H04Q2213/13248; H04Q2213/13348; H04Q2213/1337; H04Q2213/13389

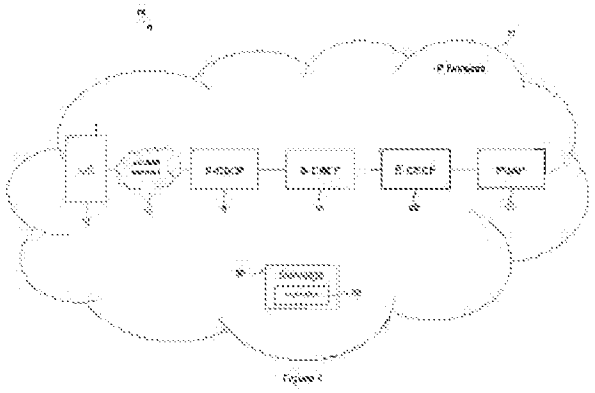
Application number: EP20070855458 20071204

Priority number(s): WO2007CA02176 20071204 ; US20070944258P 20070615

Also published as: EP2165489 (A4) WO2008151406 (A1) WO2008151406 (A8) US2008310599 (A1) MX2009013633 (A) KR20120051078 (A) KR101162903 (B1) KR20100029124 (A) KR101162847 (B1) CN101772929 (A) CN101772929 (B) CA2690236 (A1) less

Abstract not available for EP2165489 (A1)
Abstract of corresponding document: WO2008151406 (A1)

A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 165 489 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2008/151406 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2008/151406 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2008/151406 (art. 153(3) CBE).

Espacenet

Bibliographic data: EP2215755 (A1) — 2010-08-11

IP-BASED CALL CONTENT INTERCEPT USING REPEATERS

Inventor(s): BASTIEN STEPHANE [CA] ± (BASTIEN, STEPHANE)

Applicant(s): BROADSOFT INC [US] ± (BROADSOFT, INC)

Classification: **- international:*H04J3/26***
- cooperative: H04L63/00; H04L63/30; H04L65/1083; H04M3/2281; H04M7/006

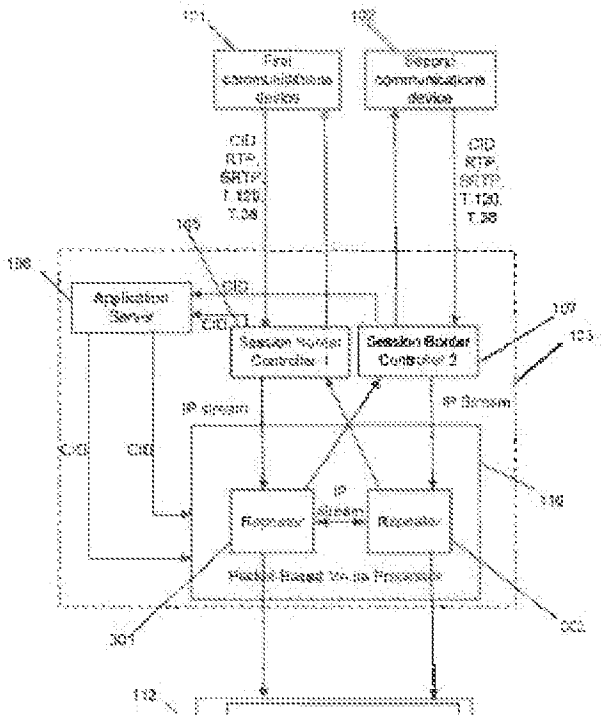
Application number: EP20080854264 20081125

Priority number (s): WO2008US13100 20081125 ; US20070987486 20071130

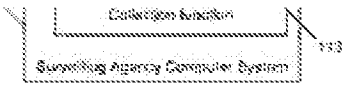
Also published as: EP2215755 (A4) US2009141883 (A1) US8514841 (B2) WO2009070278 (A1)

Abstract not available for EP2215755 (A1)
Abstract of corresponding document: US2009141883 (A1)

A computer-readable medium for performing IP-based call intercept includes instructions for receiving call initiation data, a first IP packet from the first communications device, and a second IP packet from a second communications device, generating copies of the first IP packet and the second IP packet, and transmitting one of the first IP packets to the second communications device according to the call initiation data, another of the first IP packets to a surveilling agency computer system without encoding a decoding the IP packet, one of the second IP packets to the first communications device according to the call initiation data, and another of the second IP packets to the surveilling agency computer system



without encoding or decoding the IP packet.



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 215 755 A0**
(11) Numéro de publication:

Internationale Anmeldung veröffentlicht durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2009/070278 (Art. 153(3) EPÜ).

International application published by the World Intellectual Property Organization under number:

WO 2009/070278 (Art. 153(3) EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété Intellectuelle sous le numéro:

WO 2009/070278 (art. 153(3) CBE).

Espacenet

Bibliographic data: EP2165489 (A4) — 2011-03-02

SYSTEM AND METHOD FOR INDICATING EMERGENCY CALL BACK TO USER EQUIPMENT

Inventor(s): PURNADI RENE W [US]; ISLAM M KHALEDUL [CA] + (PURNADI, RENE W, ; ISLAM, M. KHALEDUL)

Applicant(s): RESEARCH IN MOTION LTD [CA] + (RESEARCH IN MOTION LIMITED)

Classification: **- international:*H04L12/66; H04M11/06; H04Q3/64***
- cooperative: **H04M3/5116**; **H04Q3/64**; H04L65/1016; H04M1/72538; H04Q2213/13152; H04Q2213/13176; H04Q2213/13204; H04Q2213/13248; H04Q2213/13348; H04Q2213/1337; H04Q2213/13389

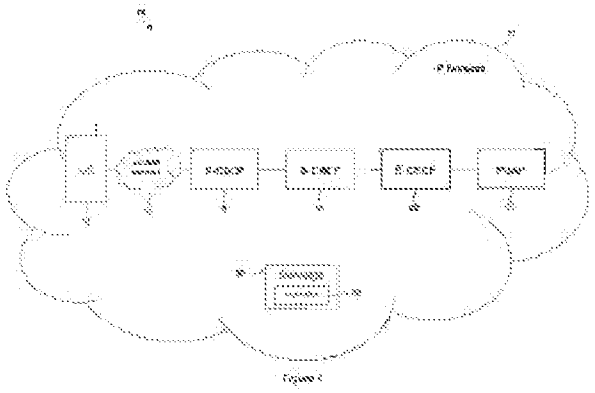
Application number: EP20070855458 20071204

Priority number(s): WO2007CA02176 20071204 ; US20070944258P 20070615

Also published as: EP2165489 (A1) WO2008151406 (A1) WO2008151406 (A8) US2008310599 (A1) MX2009013633 (A) KR20120051078 (A) KR101162903 (B1) KR20100029124 (A) KR101162847 (B1) CN101772929 (A) CN101772929 (B) CA2690236 (A1) less

Abstract not available for EP2165489 (A4)
Abstract of corresponding document: WO2008151406 (A1)

A method is provided for indicating an IMS (Internet Protocol Multimedia Subsystem) emergency call back to a user equipment 14 and an access network 15. The method comprises including in a message 30 from a PSAP (Public Safety Answering Point) 22 to the user equipment 14 and the access network 15 an indication 32 that the emergency call back is from the PSAP 22.



Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 07 85 5458

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2007/016695 A2 (QUALCOMM INC [US]; NASIELSKI JOHN [US]; EDGE STEPHEN [US]; BURROUGHS K) 8 February 2007 (2007-02-08) * abstract; claims 1-19; figure 11 * * paragraphs [0064], [0084] * * paragraph [00147] - paragraph [00157] * * paragraph [0180] *	1-15	INV. H04L12/66 H04M11/06 H04Q3/64
A	US 2007/066277 A1 (BHARATIA JAYSHREE [US] ET AL) 22 March 2007 (2007-03-22) * abstract; claims 1-8; figure 4 * * paragraphs [0032], [0033], [0037] *	1-15	
A	ROSENBERG CISCO J: "Applying Loose Routing to Session Initiation Protocol (SIP) User Agents (UA); draft-rosenberg-sip-ua-loose-route-01.txt", IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 1, 12 June 2007 (2007-06-12), XP015052124, ISSN: 0000-0004 * paragraphs [02.6], [04.1] *	1-15	TECHNICAL FIELDS SEARCHED (IPC) H04M H04L H04Q

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	21 January 2011	Ohanovici, Z

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 85 5458

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-01-2011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007016695 A2	08-02-2007	CA 2617783 A1	08-02-2007
		EP 1911257 A2	16-04-2008
		JP 2009505455 T	05-02-2009
		KR 20080054380 A	17-06-2008
US 2007066277 A1	22-03-2007	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP2127232 (A4) — 2011-03-16

SYSTEM AND METHOD FOR RECORDING AND MONITORING COMMUNICATIONS USING A MEDIA SERVER

Inventor(s): WYSS FELIX IMMANUEL [US]; SNYDER MICHAEL D [US]; O'CONNOR KEVIN [US] ± (WYSS, FELIX, IMMANUEL, ; SNYDER, MICHAEL, D, ; O'CONNOR, KEVIN)

Applicant(s): INTERACTIVE INTELLIGENCE INC [US] ± (INTERACTIVE INTELLIGENCE, INC)

Classification: **- international:*H04L12/28; H04L29/06; H04M3/51***
- cooperative: H04L63/00; H04L63/1425; H04L63/30; H04L65/605; H04M3/2281; H04M3/42221; H04M3/51; H04L65/1006; H04L65/104

Application number: EP20080730132 20080219

Priority number (s): WO2008US54271 20080219 ; US20070678315 20070223

Also published as: EP2127232 (A1) WO2008103652 (A1) US2012195415 (A1) US2008205378 (A1) US8427981 (B2)

Abstract not available for EP2127232 (A4)
Abstract of corresponding document: WO2008103652 (A1)

A communication system including a media server through which communication packets are exchanged for recording and monitoring purposes is disclosed. A tap is associated with each communication endpoint allowing for cradle to grave recording of communications despite their subsequent routing or branching. An incoming communication is routed to a first tap and upon selection of a receiving party; the first tap is routed to a second tap which forwards communication packets on to the receiving party. The taps may be used to forward communication packets to any number of other taps or destinations, such as a recording device, monitoring user, or other user in the form of a conference.

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 08 73 0132

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 7 055 174 B1 (COPE WARREN B [US] ET AL) 30 May 2006 (2006-05-30) * abstract * * figure 4 * * column 1, line 8 - line 11 * * column 1, line 49 - column 3, line 21 * * column 3, line 44 - line 45 * * column 7, line 23 - column 10, line 34 *	1-15	INV. H04L29/06 H04L12/28 H04M3/51
X	EP 1 389 862 A1 (CIT ALCATEL [FR]) 18 February 2004 (2004-02-18) * abstract * * paragraph [0004] - paragraph [0011] * * paragraph [0017] - paragraph [0027] * * paragraph [0047] - paragraph [0055] * * claims 1,2,3,4,7 * * figure 2 *	1-15	
X	WO 2004/091250 A1 (ERICSSON TELEFON AB L M [SE]; LAIHO KEIJO [FI]; VALASSI PAOLO [IT]) 21 October 2004 (2004-10-21) * abstract * * page 1, line 15 - line 28 * * page 2, line 19 - page 3, line 31 * * page 4, line 3 - line 10 * * page 4, line 20 - line 22 * * page 5, line 5 - line 10 * * page 6, line 7 - page 9, line 16 * * claims 1,11 * * figures 3,5,6 *	1-15	TECHNICAL FIELDS SEARCHED (IPC) H04L H04M
X	WO 2006/124945 A1 (ELOYALTY CORP [US]; CONWAY KELLY [US]; CAPERS KEENE HEDGES [US]; DANSO) 23 November 2006 (2006-11-23) * abstract * * paragraph [0003] - paragraph [0006] * * paragraph [0010] - paragraph [0038] *	1,7,15	

-/--

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	1 February 2011	Kopp, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 08 73 0132

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 02/075559 A1 (WORLDCOM INC [US]) 26 September 2002 (2002-09-26) * abstract * * page 1, line 25 - line 28 * * page 2, line 2 - page 5, line 21 * -----	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	1 February 2011	Kopp, Klaus

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 73 0132

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-02-2011

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7055174 B1	30-05-2006	NONE	
EP 1389862 A1	18-02-2004	AT 281734 T	15-11-2004
		DE 60201827 D1	09-12-2004
		DE 60201827 T2	10-11-2005
		ES 2229073 T3	16-04-2005
		US 2004202295 A1	14-10-2004
WO 2004091250 A1	21-10-2004	AU 2003271736 A1	01-11-2004
		US 2006264200 A1	23-11-2006
WO 2006124945 A1	23-11-2006	EP 1889254 A1	20-02-2008
		US 2006262920 A1	23-11-2006
WO 02075559 A1	26-09-2002	BR 0208225 A	02-03-2004
		CA 2441716 A1	26-09-2002
		CN 1498373 A	19-05-2004
		EP 1374071 A1	02-01-2004
		JP 2004533743 T	04-11-2004
		MX PA03008474 A	30-06-2004

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP1829300 (A4) — 2012-05-02

METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM

Inventor(s): KALLIO JUHA [FI] ± (KALLIO, JUHA)

Applicant(s): NOKIA CORP [FI] ± (NOKIA CORPORATION)

Classification: - international: ***H04L12/28; H04L12/56; H04W76/02;*** *H04W8/26;* ***H04L***
- cooperative: **H04W76/021**; **H04W8/10**; H04W8/26

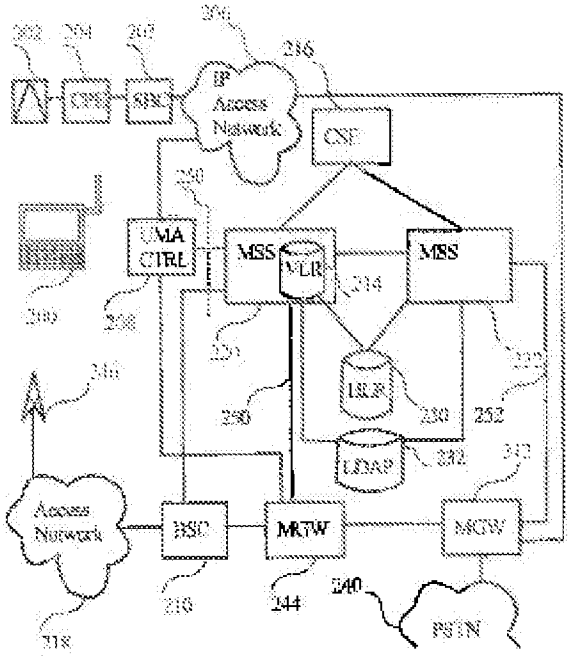
Application number: EP20050821728 20051220

Priority number (s): WO2005FI00540 20051220 ; FI20040001659 20041223

Also published as: EP1829300 (A1) EP1829300 (B1) WO2006067269 (A1) US2006142011 (A1) US7400881 (B2) KR20070097526 (A) KR100886165 (B1) CN101069390 (A) CN101069390 (B) less

Abstract not available for EP1829300 (A4)
Abstract of corresponding document: WO2006067269 (A1)

The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile



station. The call control node translates the called party number to the logical name using the directory.

Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 05 82 1728

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2004/229608 A1 (ISUKAPALLI RAMANA [US] ET AL ALEXIOU TRIANTAFYLLOS [US] ET AL) 18 November 2004 (2004-11-18) * abstract * * paragraph [0001] - paragraph [0065] * -----	1-24	INV. H04L12/56 H04L12/28 H04Q7/38
A	US 2004/228324 A1 (ALEXIOU TRIANTAFYLLOS [US] ET AL) 18 November 2004 (2004-11-18) * abstract * * paragraph [0001] - paragraph [0054] * * figures 1-3 * -----	1-24	

TECHNICAL FIELDS SEARCHED (IPC)

H04W

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

1

Place of search	Date of completion of the search	Examiner
Munich	22 March 2012	Körbler, Günther

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 82 1728

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-03-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004229608 A1	18-11-2004	NONE	
US 2004228324 A1	18-11-2004	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP2449749 (A1) — 2012-05-09

METHOD AND APPARATUS FOR RELAYING PACKETS

Inventor(s): KERAENEN ARI [FI]; HAUTAKORPI JANI [FI]; MAEENPAEAE JOUNI [FI] + (KERAENEN, ARI, ; HAUTAKORPI, JANI, ; MAEENPAEAE, JOUNI)

Applicant(s): ERICSSON TELEFON AB L M [SE] + (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL))

Classification: - international: ***H04L29/12***
- cooperative: **H04L29/12537**; **H04L61/2578**; **H04L61/2589**

Application number: EP20090780010 20090629

Priority number (s): WO2009EP58129 20090629

Also published as: EP2449749 (B1) WO2011000405 (A1) US2012099599 (A1) US8611354 (B2) RU2012102911 (A) CN102484656 (A) less

Abstract not available for EP2449749 (A1)
Abstract of corresponding document: WO2011000405 (A1)

Apparatus for relaying packets between a first host and a second host. The apparatus comprises a memory for registering for said first host; an address of the first host, a relayed address of the first host, an address of the second host, and an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier. The apparatus further comprises and one or both of : an outbound packet inspector for inspecting packets received from said first host and addressed to an address of the apparatus to determine whether or not they contain a registered outbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the second host; and an inbound packet inspector for inspecting packets received from said second host and addressed to said relayed address to determine whether or not they contain a registered inbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the first host.

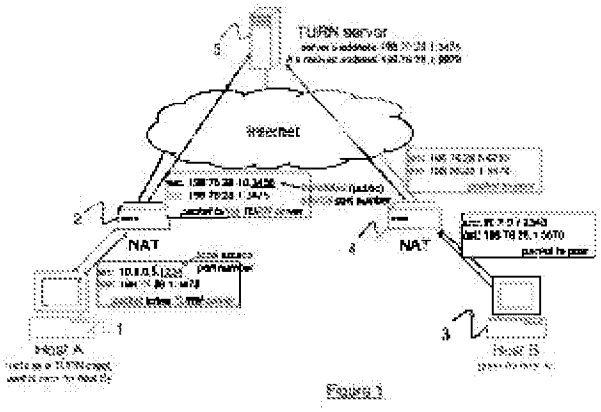


Figure 1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer:
(11) Publication number: **EP 2 449 749 A0**
(11) Muméro de publication:

Internationale Anmeldung veröffentlich durch die Weltorganisation für geistiges Eigentum unter der Nummer:

WO 2011/000405 (art. 158 des EPÜ).

International application published by the World Intellectual Property Organisation under number:

WO 2011/000405 (art. 158 of the EPC).

Demande internationale publiée par l'Organisation Mondiale de la Propriété sous le numéro:

WO 2011/000405 (art. 158 de la CBE).

Espacenet

Bibliographic data: EP2215755 (A4) — 2012-10-24

IP-BASED CALL CONTENT INTERCEPT USING REPEATERS

Inventor(s): BASTIEN STEPHANE [CA] ± (BASTIEN, STEPHANE)

Applicant(s): BROADSOFT INC [US] ± (BROADSOFT, INC)

Classification: **- international:*H04J3/26***
- cooperative: H04L63/00; H04L63/30; H04L65/1083; H04M3/2281; H04M7/006

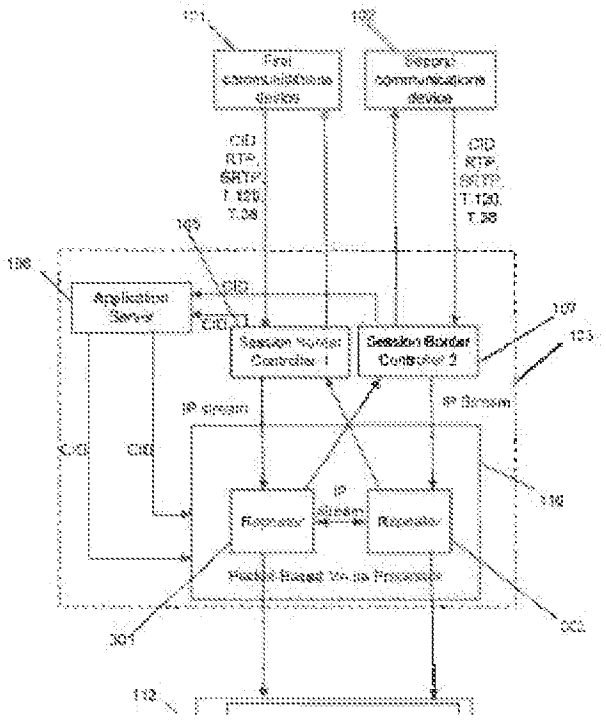
Application number: EP20080854264 20081125

Priority number (s): WO2008US13100 20081125 ; US20070987486 20071130

Also published as: EP2215755 (A1) US2009141883 (A1) US8514841 (B2) WO2009070278 (A1)

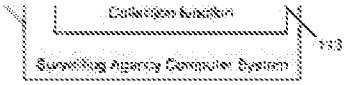
Abstract not available for EP2215755 (A4)
Abstract of corresponding document: US2009141883 (A1)

A computer-readable medium for performing IP-based call intercept includes instructions for receiving call initiation data, a first IP packet from the first communications device, and a second IP packet from a second communications device, generating copies of the first IP packet and the second IP packet, and transmitting one of the first IP packets to the second communications device according to the call initiation data, another of the first IP packets to a surveilling agency computer system without encoding a decoding the IP packet, one of the second IP packets to the first communications device according to the call initiation data, and another of the second IP packets to the surveilling agency computer system



PETITIONER APPLE INC. EX. 1004-832

without encoding or decoding the IP packet.



Europäisches Patentamt
European Patent Office
Office européen des brevets

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 08 85 4264

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2002/009973 A1 (BONDY WILLIAM MICHAEL [US] ET AL) 24 January 2002 (2002-01-24) * paragraph [0019] * * paragraph [0029] - paragraph [0032] * * paragraph [0037] - paragraph [0052] * * paragraph [0072] * -----	1-16	INV. H04M3/22 H04M7/00 H04L29/06 H04L63/30

TECHNICAL FIELDS SEARCHED (IPC)

H04M
H04L

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
Munich	17 September 2012	Agante da Silva, P

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 85 4264

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-09-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002009973 A1	24-01-2002	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

Espacenet

Bibliographic data: EP1829300 (B1) — 2012-11-21

METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM

Inventor(s): KALLIO JUHA [FI] ± (KALLIO, JUHA)

Applicant(s): NOKIA CORP [FI] ± (NOKIA CORPORATION)

Classification: - international: ***H04W76/02; H04W8/10;*** *H04W8/26;* ***H04L***
- cooperative: **H04W76/021**; **H04W8/10**; H04W8/26

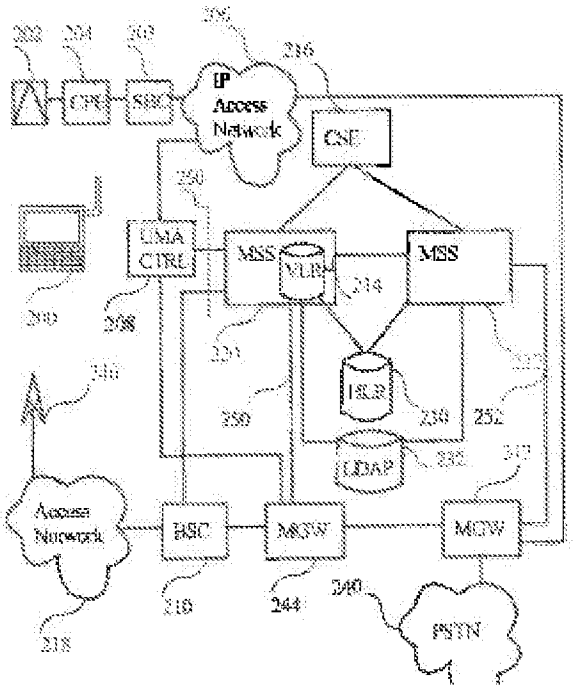
Application number: EP20050821728 20051220

Priority number (s): WO2005FI00540 20051220 ; FI20040001659 20041223

Also published as: EP1829300 (A1) EP1829300 (A4) WO2006067269 (A1) US2006142011 (A1) US7400881 (B2) KR20070097526 (A) KR100886165 (B1) CN101069390 (A) CN101069390 (B) less

Abstract not available for EP1829300 (B1)
Abstract of corresponding document: WO2006067269 (A1)

The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile station. The call control node translates



PETITIONER APPLE INC. EX. 1004-836

the called party number to the logical name using the directory.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 829 300 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
21.11.2012 Bulletin 2012/47

(21) Application number: **05821728.2**

(22) Date of filing: **20.12.2005**

(51) Int Cl.:
H04W 8/10 *(2009.01)* ***H04W 76/02*** *(2009.01)*

(86) International application number:
PCT/FI2005/000540

(87) International publication number:
WO 2006/067269 (29.06.2006 Gazette 2006/26)

(54) **METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM**

VERFAHREN ZUM ROUTING VON KOMMUNIKATIONEN ZU EINEM VOIP-ENDGERÄT IN EINEM MOBILEN KOMMUNIKATIONSSYSTEM

PROCEDE DE ROUTAGE DE COMMUNICATIONS VERS UN TERMINAL DE VOIX SUR IP DANS UN SYSTEME DE COMMUNICATION MOBILE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **23.12.2004 FI 20041659**

(43) Date of publication of application:
05.09.2007 Bulletin 2007/36

(73) Proprietor: **Nokia Corporation**
02150 Espoo (FI)

(72) Inventor: **KALLIO, Juha**
FI-00870 Helsinki (FI)

(74) Representative: **Papula Oy**
P.O. Box 981
00101 Helsinki (FI)

(56) References cited:
WO-A1-00/79814
WO-A1-01/22766
WO-A1-2004/017564
US-A1- 2002 119 775
US-A1- 2004 228 324
US-A1- 2004 229 608

Printed by Jouve, 75001 PARIS (FR)

EP 1 829 300 B1

INFORMATION DISCLOSURE STATEMENT

Inventor	:	Clay Perreault, et al.
App. No.	:	13/966,096
Filed	:	August 13, 2013
For	:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
Examiner	:	Sing, Simon P.
Art Unit	:	2653
Conf. No.	:	8712

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

References and Listing

Pursuant to 37 CFR 1.56, an Information Disclosure Statement listing references is provided herewith. Copies of any listed foreign and non-patent literature references are being submitted.

No Disclaimers

To the extent that anything in the Information Disclosure Statement or the listed references could be construed as a disclaimer of any subject matter supported by the present application, Applicant hereby rescinds and retracts such disclaimer.

Timing of Disclosure

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits, and presumably no fee is required. If a First Office Action on the merits

was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 CFR 1.17(p) to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 11/26/14

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

IDS
19421508
112614

Please Direct All Correspondence to Customer Number 20995

EFS WEB CONTINUING IDS COVER LETTER

Inventor	:	Clay Perreault, et al.
App. No.	:	13/966,096
Filed	:	August 13, 2013
For	:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
Examiner	:	Sing, Simon P.
Art Unit	:	2653
Conf No.	:	8712

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Submitted herewith are references numbered 197 to 238 listed on the PTO/SB/08 or equivalent filed under EFS ID 20803282.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 11/26/14

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20995
(858) 707-4000

IDS-CON

19421570
112614

Electronic Acknowledgement Receipt

EFS ID:	20803634
Application Number:	13966096
International Application Number:	
Confirmation Number:	8712
Title of Invention:	PRODUCING ROUTING MESSAGES FOR VOICE OVER IP COMMUNICATIONS
First Named Inventor/Applicant Name:	CLAY PERREAULT
Customer Number:	20995
Filer:	John M Carson/Norman Green
Filer Authorized By:	John M Carson
Attorney Docket Number:	SMARB19.001C1
Receipt Date:	26-NOV-2014
Filing Date:	13-AUG-2013
Time Stamp:	18:48:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	FRef55_EP2449749B1.pdf	1916042 c7ec55e0d9f344814433055 92ea860b6979bb21d	no	21

Warnings:	
Information:	

2	Foreign Reference	FRef56_EP1266516B1.pdf	1664204 d52be8321c2a689d0166ecd32ebd803ccef7009f	no	18
Warnings:					
Information:					
3	Foreign Reference	FRef57_WO01069899A2.pdf	2259314 94e933342c98664c8d506cceac63b1bc08fbb3fb	no	28
Warnings:					
Information:					
4	Foreign Reference	FRef58_WO01069899A3.pdf	416928 bda88f4ab9a34fa3c2286ac66015aff2a43392a4	no	5
Warnings:					
Information:					
5	Foreign Reference	FRef59_WO0180587A1.pdf	1619706 85242829c5647845bc45ffd8aac6a19d342dfbbd	no	22
Warnings:					
Information:					
6	Foreign Reference	FRef60_WO02082728A1.pdf	2591192 16384beb042c600be3c0e0a879ee9503d244138c	no	34
Warnings:					
Information:					
7	Foreign Reference	FRef61_WO02082782A2.pdf	2914857 f0d50b28dfa8ff26b3fd3d549ccac52021cd732d	no	43
Warnings:					
Information:					
8	Foreign Reference	FRef62_WO02082782A3.pdf	257211 f2a654e281f862589306515292e189bb735b52a5	no	3
Warnings:					
Information:					
9	Foreign Reference	FRef63_WO2005084002A1.pdf	3900912 bf5c5251907802e72fe06271a28ee022af6b3e1b	no	47
Warnings:					
Information:					
10	Foreign Reference	FRef64_WO2006067269A1.pdf	3463501 2d7411d22abd0087e0e6286a27992edb9df69c28	no	42
Warnings:					
Information:					

11	Foreign Reference	FRef65_WO2006072099A1.pdf	2394748 ac5dfcf6234eafca9d46b61e13d08eca85c3aa5a	no	30
Warnings:					
Information:					
12	Foreign Reference	FRef66_WO2006078175A2.pdf	1037300 55a67b931a84a2b31550663a1166ec807d0f377c	no	13
Warnings:					
Information:					
13	Foreign Reference	FRef67_WO2006078175A3.pdf	271651 cb7df71eb16430d59ee154d3d7dc86b94ddfdf26	no	3
Warnings:					
Information:					
14	Foreign Reference	FRef68_WO2007044454A2.pdf	1995500 c9fa9928d60dffdaf6fcdeff504c08952b08345a	no	27
Warnings:					
Information:					
15	Foreign Reference	FRef69_WO2007087077A2.pdf	2004508 7f50929c2a209f3db466f990ac35a95b11071766	no	25
Warnings:					
Information:					
16	Foreign Reference	FRef70_WO2007087077A3.pdf	261160 071fc65c3cd0719ba4b2885bcf92de7e0ed0495d	no	3
Warnings:					
Information:					
17	Foreign Reference	FRef71_WO2008085614A2.pdf	3347354 12b402d41f292c3dd44c36531932dd683fe4b4fb	no	40
Warnings:					
Information:					
18	Foreign Reference	FRef72_WO2008085614A3.pdf	415791 7fea40fec0ec0117d53a4341437056129a65c9b7	no	5
Warnings:					
Information:					
19	Foreign Reference	FRef73_WO2008085614A8.pdf	254937 de8b70f513957e08800b0223b6f3f82bfb5d0ae4	no	4
Warnings:					
Information:					

20	Foreign Reference	FRef74_WO2008086350A2.pdf	2960802 65a44accd0215e7ebf8c8fd92d21781fc62826f5	no	45
Warnings:					
Information:					
21	Foreign Reference	FRef75_WO2008086350A3.pdf	450316 bc738f5e7ed1ff2182902835b4806e906470b4e3	no	6
Warnings:					
Information:					
22	Foreign Reference	FRef76_WO2008103652A1.pdf	2049308 57f7119548f95d8f26aa560cc9a18197c529784d	no	28
Warnings:					
Information:					
23	Foreign Reference	FRef77_WO2008151406A1.pdf	2190191 270b6309c2aac77688db0bc59630f0ba505dba0c	no	27
Warnings:					
Information:					
24	Foreign Reference	FRef78_WO2008151406A8.pdf	101547 58dfd5ffe0133f48384e374a19e46c1afd652a32	no	1
Warnings:					
Information:					
25	Foreign Reference	FRef79_WO2009070202A1.pdf	4494015 b182cddf1e218b2914e6c531e9389f46d3ef89c0	no	60
Warnings:					
Information:					
26	Foreign Reference	FRef80_WO2009070278A1.pdf	3899512 a1c07b2fba7574e3c53857c90de4ff95291c67b3	no	49
Warnings:					
Information:					
27	Foreign Reference	FRef81_WO2011000405A1.pdf	2061771 7a0c468264115ea323bbd3f980ad7c941f44ec2f	no	27
Warnings:					
Information:					
28	Non Patent Literature	NRef1_Baker_Cisco_Support_Apr_2003.pdf	1089613 60278da852d7b93e5b5ab60105289f393cd4fd5a	no	15
Warnings:					
Information:					

29	Non Patent Literature	NRef2_Bhushan_Federated_Accounting_2001.pdf	1342637 2ed16b50935f7a7bcb45d50bf4551263447076c9	no	15
Warnings:					
Information:					
30	Non Patent Literature	NRef3_Jajszczyk_Emergency_Calls_Sept_2007.pdf	435620 54549733f533cde854ba14e0cafc64fb35f67bce	no	3
Warnings:					
Information:					
31	Non Patent Literature	NRef4_Kim_Enhanced_VoIP_May_2006.pdf	904746 25d3bd2fd692570be10dbf833bb335f096515a60	no	8
Warnings:					
Information:					
32	Non Patent Literature	NRef5_Kornfeld_DVB_H_and_IP_Datacast_March_2007.pdf	1363178 24d14dd9f69e8c8c66ae9c1945cb711c88915afa	no	10
Warnings:					
Information:					
33	Non Patent Literature	NRef6_Kortebi_Meddour_SINR_Based_Routing_2007.pdf	841024 9cfabaeac68aaa41468a53a9f379b6b588cff735	no	6
Warnings:					
Information:					
34	Non Patent Literature	NRef7_Lee_VoIP_Interoperation_2004.pdf	644808 59423980e4c93115b22c514e44246eb926b24f29	no	7
Warnings:					
Information:					
35	Non Patent Literature	NRef8_Lin_Effective_VoIP_Call_Routing_2005.pdf	335804 d166b8fc7eea3224222ac929d424a66c4926aec9	no	3
Warnings:					
Information:					
36	Non Patent Literature	NRef9_Ma_Realizing_MPEG4_2005.pdf	514335 065f46bed6d8068577cbad7cb707f6f31f0f3d85	no	4
Warnings:					
Information:					
37	Non Patent Literature	NRef10_Mintz-Habib_A_VoIP_Emergency_2005.pdf	829844 0cde14452c1c8cfb988b4b4f2f5c8c339ac77657	no	6
Warnings:					
Information:					

38	Non Patent Literature	NRef11_Munir_Study_Adaptive_Scheme_2005.pdf	1516334 a6d2fc388fcc9647095760fbbc775ffb70cfabb1	no	17
Warnings:					
Information:					
39	Non Patent Literature	NRef12_Sripanidkulchai_Call_Routing_2007.pdf	784493 59615b3a52b42334065bf89d62a86c2c89a912e4	no	6
Warnings:					
Information:					
40	Non Patent Literature	NRef13_Thernelius_SIP_NAT_May_2000.pdf	5744783 0e8aa8758c56b1027d0655bcab94eeceea0079b2	no	69
Warnings:					
Information:					
41	Non Patent Literature	NRef14_Trad_Adaptive_VoIP_2004.pdf	1055406 b5546a1dd148bf40bc8ec8f7d7aa4613f2301c09	no	12
Warnings:					
Information:					
42	Non Patent Literature	NRef15_Yu_Service-Oriented_Issues_2006.pdf	901174 a1911e8afcc7ef5dfa2fcba549b65d2baca2f77c	no	10
Warnings:					
Information:					
43	Transmittal Letter	IDS_Con_Trans_SMARB19_001C1_11_26_2014.pdf	31131 250f29146fcdbf990e428761d6d0df2e44fd267e	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	69529208	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Espacenet

Bibliographic data: EP2449749 (B1) — 2014-03-12

METHOD AND APPARATUS FOR RELAYING PACKETS

Inventor(s): KERAENEN ARI [FI]; HAUTAKORPI JANI [FI]; MAEENPAEAE JOUNI [FI] + (KERAENEN, ARI, ; HAUTAKORPI, JANI, ; MAEENPAEAE, JOUNI)

Applicant(s): ERICSSON TELEFON AB L M [SE] + (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL))

Classification: - international: ***H04L29/12***
- cooperative: **H04L29/12537**; **H04L61/2578**; **H04L61/2589**

Application number: EP20090780010 20090629

Priority number (s): WO2009EP58129 20090629

Also published as: EP2449749 (A1) WO2011000405 (A1) US2012099599 (A1) US8611354 (B2) RU2012102911 (A) CN102484656 (A) less

Abstract not available for EP2449749 (B1)
Abstract of corresponding document: WO2011000405 (A1)

Apparatus for relaying packets between a first host and a second host. The apparatus comprises a memory for registering for said first host; an address of the first host, a relayed address of the first host, an address of the second host, and an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier. The apparatus further comprises and one or both of : an outbound packet inspector for inspecting packets received from said first host and addressed to an address of the apparatus to determine whether or not they contain a registered outbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the second host; and an inbound packet inspector for inspecting packets received from said second host and addressed to said relayed address to determine whether or not they contain a registered inbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the first host.

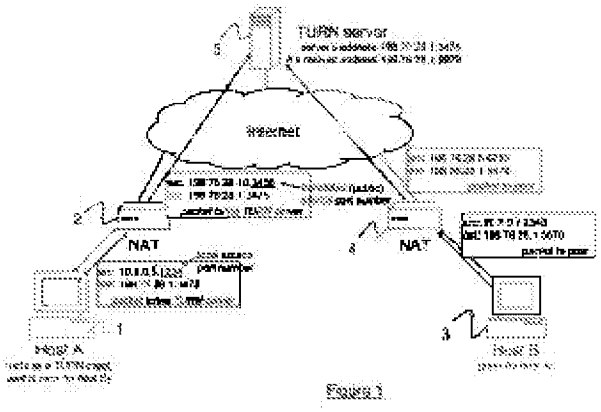


Figure 1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 449 749 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
12.03.2014 Bulletin 2014/11

(21) Application number: **09780010.6**

(22) Date of filing: **29.06.2009**

(51) Int Cl.:
H04L 29/12 *(2006.01)*

(86) International application number:
PCT/EP2009/058129

(87) International publication number:
WO 2011/000405 (06.01.2011 Gazette 2011/01)

(54) **METHOD AND APPARATUS FOR RELAYING PACKETS**

VERFAHREN UND VORRICHTUNG ZUM ROUTING VON PAKETEN

PROCÉDÉ ET APPAREIL DESTINÉS À RELAYER DES PAQUETS

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR

(43) Date of publication of application:
09.05.2012 Bulletin 2012/19

(73) Proprietor: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **KERÄNEN, Ari**
  FIN-02880 Veikkola (FI)
- **HAUTAKORPI, Jani**
  FIN-02430 Masala (FI)
- **MÄENPÄÄ, Jouni**
  FIN-03100 Nummela (FI)

(74) Representative: **Lind, Robert**
Marks & Clerk LLP
Fletcher House
Heatley Road
The Oxford Science Park
Oxford OX4 4GE (GB)

(56) References cited:
- **PERREAULT S ET AL: "Traversal Using Relays around NAT (TURN) Extensions for TCP Allocations; draft-ietf-behave-turn-tcp-03.txt" TRAVERSAL USING RELAYS AROUND NAT (TURN) EXTENSIONS FOR TCP ALLOCATIONS; DRAFT-IETF-BEHAVE-TURN-TCP-03.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, vol. behave, no. 3, 4 May 2009 (2009-05-04), XP015062268 [retrieved on 2009-05-04]**
- **ROSENBERG CISCO R MAHY PLANTRONICS P MATTHEWS AVAYA J: "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN); draft-ietf-behave-turn-07.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. behave, no. 7, 25 February 2008 (2008-02-25), XP015053106 ISSN: 0000-0004**
- **SCHULZRINNE COLUMBIA U R HANCOCK SIEMENS/RMR H: "GIST: General Internet Signaling Transport; draft-ietf-nsis-ntlp-08.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. nsis, no. 8, 27 September 2005 (2005-09-27), XP015040926 ISSN: 0000-0004**
- **KOMU M ET AL: "HIP Extensions for the Traversal of Network Address Translators; draft-ietf-hip-nat-traversal-02.txt", 20070706, vol. hip, no. 2, 6 July 2007 (2007-07-06), XP015051263, ISSN: 0000-0004**

EP 2 449 749 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Technical Field

[0001] The present invention relates to a method and apparatus for relaying packets. It is applicable to achieving traversal of a Network Address Translation (NAT) server and in particular to such a method and apparatus that makes use of the Traversal Using Relays around NAT (TURN) protocol.

Background

[0002] Network Address Translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. NAT is used in conjunction with network masquerading (or IP masquerading) which is a technique that hides an entire address space, usually consisting of private network addresses, behind a single IP address in another, often public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single address and then rewrites the outgoing Internet Protocol (IP) packets on exit so that they appear to originate from the router. In the reverse communications path, responses are mapped back to the originating IP address using the rules ("state") stored in the translation tables. The translation table rules established in this fashion are flushed after a short period without new traffic refreshing their state.

[0003] Of course, the use of Network Address Translation means that many hosts in the Internet cannot be contacted directly by other hosts because they are behind a Network Address Translator (NAT) that prevents inbound connections. Different NAT traversal techniques, e.g., Interactive Connectivity Establishment (ICE) [see J. Rosenberg. Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols. draft-ietf-mmusicice-19 (work in progress). October 2007] have been developed to overcome this problem, but with certain kinds of NATs the only way to create a peer-to-peer connection between two hosts is to relay all the traffic through a node that both of the peers can contact (including the peer or peers behind a NAT).

[0004] Traversal Using Relays around NAT (TURN) [see Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). draft-ietf-behave-turn-15 (work in progress). February, 2009] allows a host (that is a TURN client) to register a "relayed address" (a combination of IP address and port number) at the TURN server such that a session is established "through" the NAT between the TURN server and the TURN client (nb. a connection initiated by the host behind the NAT will generally result in a session being established through the NAT and via which the node to which the connection is initiated can send packets to the host). A connection initiated by a remote peer to the relayed address is relayed by the TURN server to the TURN client, such that it passes through the punched hole in the NAT. The TURN client can send data to the peer via the TURN server such that, from the point of view of the peer, the data appears to originate from the relayed address. Using a TURN server, even with the most restrictive type of NATs, a communication path can be established between two peers.

[0005] After obtaining a relayed address from the TURN server, a TURN client needs to maintain its state in the NAT by sending periodic keep-alive messages to the TURN server via the NAT. To minimize the volume of keep-alive messages, TURN allows multiple connections with different peers to re-use the same relayed address. Thus, regardless of the number of peers, only one set of keep-alive messages is required. In addition to reducing the volume of keep-alive traffic, this method also conserves public ports at the TURN server and at the NAT allowing them to serve a larger number of simultaneous users.

[0006] In the case where multiple peer connections are multiplexed onto one connection between the TURN client and the TURN server, it is necessary to provide a mechanism which allows the TURN server and the TURN client to identify peers within the data packets that they exchange. For this purpose, data sent between the server and client is encapsulated within TURN messages.

[0007] TURN encapsulation increases the per-packet overhead and decreases the Maximum Transmission Unit (MTU) on the link between the TURN server and client. The overhead problem is especially severe in restricted bandwidth environments (e.g., when using a cellular data connection), and for data that is sent in multiple small packets (e.g., real time audio). More significantly perhaps, encapsulation prevents the use of unmodified operating system kernel protocol stacks for receiving and sending the data. This gives rise at least to performance problems, as data needs to be sent back and forth between the kernel and user space process. In the case of restricted operating systems (such as those commonly used in mobile devices) it may of course be impossible to feed the packets back to the kernel protocol stack or capture the packets after the stack processing. TURN encapsulation is not a viable option in such cases.

[0008] The Internet (IETF) draft - "Traversal Using Relays around NAT: Relay Extensions to Session Traversal Utilities for NAT (July 8, 2007)" provides a mechanism for avoiding encapsulation. This mechanism makes use of the "Set Active Destination" request. However, the mechanism does not allow multiple sessions to be multiplexed onto the TURN server to client link. This proposal is further considered in Rosenberg J et al, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN); draft-ietf-behave-turn-07.txt, describes the use of TURN

[0009] Perreault S et al, "Traversal Using Relays

around NAT (TURN) Extensions for TCP Allocations; draft-ietf-behave-turn-tcp-03.txt", describes a procedure for establishing TCP connections via a TURN server. The use of a "connection identifier" allows the TURN server to bind together a first TCP connection between the TURN server and a host and a second TCP connection between the TURN server and a peer.

[0010] The Internet (IETF) draft - "HIP Extensions for the Traversal of Network Address Translators (July 6, 2007)" provides HIP extensions which enable NAT traversal. The method of NAT traversal requires a peer to have registered itself with a HIP relay in order for NAT traversal to be able to occur.

Summary

[0011] It is an object of the present invention to allow packets to be sent between a client and a relay server without using encapsulation, and which mitigates the problems of known solutions. The invention is defined by a method according to claim 17, a relay apparatus according to claim 1, and a client terminal according to claim 10.

[0012] According to a first aspect of the present invention there is provided apparatus for relaying packets between a first host and a second host. The apparatus comprises a memory for registering for said first host; an address of the first host, a relayed address of the first host, an address of the second host, and an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier. The apparatus further comprises and one or both of:

an outbound packet inspector for inspecting packets received from said first host and addressed to an address of the apparatus to determine whether or not they contain a registered outbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the second host; and

an inbound packet inspector for inspecting packets received from said second host and addressed to said relayed address to determine whether or not they contain a registered inbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the first host.

[0013] Embodiments of the invention allow packets to be sent between the first host and the apparatus, acting as relay server, without encapsulation in one or both of the inbound and outbound directions. The bandwidth occupied on the link between the first host and the apparatus can be reduced, whilst at the same time allowing multiple sessions to be multiplexed onto that link.

[0014] The outbound packet inspector, if present, may be configured to replace the address of the first host in a source address field of packets to be forwarded to said second host, with said relayed address.

[0015] The inbound packet inspector, if present, may be configured to replace said relayed address in a destination address field of packets to be forwarded to said first host, with said address of the first host, and to replace said address of the second host in a source address field of those packets with an address of the apparatus. The inbound packet inspector may be configured to deliver packets which contain said inbound Higher Layer Identifier, to said first host, without additional relay encapsulation.

[0016] The memory may be configured to additionally register for said first host an offset position for the or each of said inbound and outbound Higher Layer Identifiers, the offset position identifying a position of the associated Higher Layer Identifier within a packet, and the outbound and inbound packet inspectors being configured to use the respective offset position to determine the presence of a Higher Layer Identifier.

[0017] The memory and the or each of said inbound packet inspector and said outbound packet inspector may be configured to additionally handle the relaying of packets between said first host and one or more further hosts using one or both of the inbound and outbound Higher Layer Identifiers.

[0018] The invention is applicable to the case where said first host is located behind a Network Address Translator, and said address of the first host is a NATed address of the first host. In this case, any additional relay encapsulation is encapsulation according to the Traversal Using Relays around NAT protocol. The apparatus acting as relay server may comprise a client terminal registration unit for registering said first host and any further hosts, the registration unit being configured to use the Traversal

[0019] Using Relays around NAT, TURN, protocol.

[0020] According to a second aspect of the present invention there is provided a client terminal configured to exchange packets with a peer terminal via a relay server. The client terminal comprises a relay unit for registering with the relay server so as to be allocated a relayed address by the relay server, and an identification determining unit for determining an inbound Higher Layer Identifier to be used in packets exchanged with said peer terminal. The terminal further comprises an identifier registration unit for registering the inbound Higher Layer Identifier with said relay server, together with said relayed address, an address of the client terminal, and an address of the peer terminal, and a packet handler for associating packets received from said relay server with said peer terminal using said inbound Higher Layer Identifier.

[0021] The identification determining unit of the terminal may be configured to determine an outbound Higher Layer Identifier to be used in packets exchanged with said peer terminal, with said identifier registration unit being configured to register the outbound Higher Layer Identifier with said relay server together with the inbound Higher Layer Identifier.

[0022] The identification determining unit may be configured to determine inbound and/or outbound Higher

Layer Identifiers by identifying and using one of the following protocol parameters: a Host Identity Tag, HIT; a synchronisation source (SSRC) identifier; a Security Parameter Index (SPI); TCP port numbers.

[0023] The relay unit may be configured to implement NAT traversal and said address of the client terminal being a NATed address. In this case, the relay unit and said identifier registration unit may be configured to use the Traversal Using Relays around NAT, TURN, protocol. A further packet handler may be provided for using Traversal Using Relays around NAT, TURN, encapsulation to send and/or receive packets to a peer terminal in the event that said identification determining unit is unable to determine an inbound and, optionally, an outbound Higher Layer Identifier, or a TURN encapsulated packet is received from said relay server.

[0024] The relay unit may be configured to determine whether or not a relay server supports a Higher Layer Identifier based relaying method and, if not, to initiate packet routing with said peer terminal using relaying encapsulation.

[0025] According to a third aspect of the present invention there is provided a method of sending packets between a first host and a second host. The method comprises registering at a relay server, on behalf of the first host an address of the first host, a relayed address of the first host, an address of the second host, and an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier. The method further comprises one or both of the steps of:

at the relay server, inspecting packets received from said first host and addressed to an address of the relay server to determine whether or not they contain said outbound Higher Layer Identifier and, if so, forwarding the packets to said address of the second host; and

inspecting packets received from said second host and addressed to said relayed address to determine whether or not they contain said inbound Higher Layer Identifier and, if so, forwarding the packets to said address of the first host.

[0026] The first host may be located behind a Network Address Translator., in which case said step of registering may be carried out using the Traversal Using Relays around NAT, TURN, protocol. Packets sent from the relay server to the first host may be forwarded using TURN encapsulation if packets received from the second host do not contain said inbound Higher Layer Identifier.

Brief Description of the Drawings

[0027]

Figure 1 illustrates schematically a network communication scenario involving NAT traversal using TURN;

Figure 2 illustrates registration signalling in the network scenario of Figure 1 and associated with the modified TURN protocol;

Figure 3 illustrates schematically an ESP packet format;

Figure 4 illustrates packet relaying in the network scenario of Figure 1;

Figure 5 illustrates schematically a TURN client and TURN server of the network scenario of Figure 1;

Figure 6 is a flow diagram illustrating TURN server registration and packet relay processes;

Figure 7 illustrates schematically an RTP packet format; and

Figure 8 illustrates schematically a HIP packet format.

Detailed Description

[0028] The problem of NAT traversal has been considered above in the context of TURN encapsulation. An enhancement to TURN and other NAT traversal solutions using data relaying will now be described.

[0029] Data that may otherwise be the subject of TURN encapsulation between the TURN client and the TURN server will often include a persistent Higher Layer Identifier (HLI) at a consistent location within packets. It is proposed here to make use of such a HLI on top of the transport layer protocol, to multiplex/demultiplex packets in place of TURN encapsulation. When a TURN client wants to communicate with a peer without using TURN encapsulation, it first checks with the TURN server to determine whether or not the TURN server supports the HLI mechanism described here. If so, then the TURN client registers a pair of HLIs (one inbound and one outbound) at the TURN server. A TURN server HLI registration contains two byte arrays (one for each HLI), as well as an array length, offset and peer address. For inbound traffic, when the TURN server receives a packet directed to the relayed address, it checks to see if the packet data matches a registered inbound HLI and, if it does, it sends the packet without any encapsulation to the TURN client as the inbound HLI will uniquely identify the peer address to the TURN client. When the TURN server receives a packet from the TURN client, it checks to see if the packet data matches a registered outbound HLI and, if it does, the packet is sent to the peer address that was registered for that outbound HLI (the public address allocated to the TURN client by the NAT, i.e. the "NATed" address of the client, which is included as the source address of the packet received at the TURN server, is switched for the relayed address according to normal TURN behaviour).

[0030] The HLI can be any byte array whose value and location is known before data is sent or received. The length of the arrays and their offsets (i.e. how many bytes after the transport layer header the HLI starts) can be defined at registration of the HLIs (by TURN client) with the TURN server. For example, in the case of UDP en-

capsulated ESP [RFC3948], the SPI value could be used as the HLI. Another example of a potential HLI would be a TCP port number if TCP is tunneled over UDP and relayed through a TURN server. A Real-time Transport Protocol's (RTP) synchronization source identifier is another example of an HLI.

[0031] Packets sent to the relayed address (from a peer) that do not match to a registered HLI are forwarded by the TURN server to the TURN client with TURN encapsulation. Any packets arriving at the TURN server from the TURN client that do not contain a match to any registered HLI are assumed to be TURN encapsulated. This behaviour allows a TURN server including the new functionality to be compatible with legacy TURN clients, and to be useable with traffic which does not include useable HLIs.

[0032] If data associated with a certain protocol needs to be exchanged between the TURN client and a single peer only, any constant field in the protocol header that is different from other concurrently relayed protocols is sufficient. For example, a protocol version number or a magic cookie value could be sufficient for this purpose. A "magic cookie" value (in this context) is a constant value in a protocol header that is used for differentiating certain protocol messages from messages associated with other protocols in the same stream. For example, STUN [RFC5389], the protocol used by TURN and ICE, carries this kind of identifier in all messages.

[0033] If, on the other hand, messages using the same protocol are exchanged by the TURN client with multiple peers, an identifier that is different for each peer is needed. Many protocols have some identifier in each packet for the source and/or destination of the data (e.g., HIP sender and receiver HITs or RTP synchronization source). For other protocols, it may be necessary to generate a HLI by combining information in multiple protocol fields.

[0034] Usually the TURN client knows implicitly the value for the outbound HLI since it is the entity originating the packets and generating the higher layer messages. If an external protocol stack (such as IPsec provided by the operating system) is used and the stack generates the value used as the HLI, the client may need to query the value from the stack or look it up from sent packets.

[0035] If the TURN client knows *a priori* the HLI value for the peer (e.g., it is a constant protocol field or certain peers always use the same value), no additional signaling is needed before registering HLIs at the TURN server. For example, in the case of HIP signaling traffic, hosts know the Host Identity Tags (HITs) that will be used in the HIP header even prior to contacting each other since a HIT is calculated from a host identity. Hence, HITs can be used as HLIs without any extra signaling. If however the HLI is not known *a priori* by the TURN client, the TURN client needs to learn the HLI value either from protocol signaling or automatically from the first received packet. Of course, that signalling (assuming that it goes through the TURN server and not via some other relay, e.g. a SIP server or HIP relay server) or first data packet must be TURN encapsulated. By way of example, consider an IPsec security association set up using IKE [RFC4306] or HIP. The hosts negotiate the SPI value that will be inserted into the beginning of every encrypted ESP packet. Thus, before any data is sent, the TURN client learns the peer's SPI value that it can utilize as HLI. The methods described do not require any support for HLI, or even for regular TURN, in the peer. An alternative approach that does require HLI support in the peer involves the TURN client explicitly asking the peer (using e.g., new STUN/TURN messages) for an HLI value.

[0036] To illustrate the proposed approach to implementing TURN without necessarily requiring TURN encapsulation, consider the case of UDP encapsulated ESP. Figure 1 illustrates schematically a TURN client (Host A) 1 that is behind a NAT 2. A peer, Host B, 3 is also behind a NAT 4, and wishes to communicate with Host A using UDP encapsulated ESP. This is achieved using a TURN server (or relay) 5. Figure 1 shows exemplary source (src) and destination (dst) IP addresses and port numbers included in packets at various points in the network. Figure 2 illustrates signalling associated with this scenario. A TURN client that supports the HLI extension first registers at the TURN server using a standard TURN allocation request (step 1). The client includes HLI-SUPPORTED parameter in the request to test whether the TURN server supports this extension. If the server supports HLI relaying, it responds with an Allocation OK message (step 2). If however the TURN server does not support HLI relaying, it rejects the request and the client can either register to the server without the extension or try some other TURN server. The HLI-SUPPORTED parameter has "comprehension-required" [RFC5389] type so that if a (legacy) TURN server does not recognize it, it rejects the request. One or both of the hosts in Figure 1 may be located behind multiple NATs. This does not change the principle of the relaying process.

[0037] Next, the hosts negotiate IPsec Security Associations. They can use for example HIP or IKE for this purpose. The negotiation can be done either through the TURN server or using some other relaying service such as HIP relay server [id-hip-nat-traversal: see Basic HIP Extensions for Traversal of Network Address Translators. draft-ietf-hip-nat-traversal-06 (work in progress). March 2009] or a peer-to-peer overlay network. If a TURN server is involved in the IPsec signalling, the signaling messages are TURN encapsulated between the TURN server and client unless HLIs have been set for the signaling protocol.

[0038] The TURN client then requests "permissions" for the peer and includes the inbound and outbound HLIs that should be checked against all relayed data (step 3). The TURN server responds with a Permission OK (step 4). Permissions are part of the normal TURN behavior and increase security by allowing only peers with registered permission to use the relayed address. The HLI

registration is piggybacked on the standard permission registration procedure. As the client will use UDP encapsulated ESP, it registers the SPI values for the peer (at address 198.76.28.5:6789) as the HLIs. In the example of Figure 1, the inbound SPI is "0xA1B2C3D4" and the outbound SPI is "0xB2C3D4E5". Both parameters are four bytes long and start immediately after the UDP header (HLI offset is zero) since the SPI is always in the first four bytes of the ESP packet. At the TURN client, the peer's address in the IPsec SAs is set to the TURN server's address so that the IPsec stack sends ESP packets, destined for the peer, to the TURN server. Figure 3 illustrates the packet format of ESP.

[0039] Figure 4 illustrates an exchange of ESP packets between the TURN client and the peer (the lower message sequence in the Figure) and which does not require TURN encapsulation. When the peer sends a packet that does not match to the registered HLI (in this example, something other than ESP, e.g., a NAT traversal connectivity check message or a signaling protocol message), the data is forwarded to the client with TURN encapsulation (the upper sequence in Figure 4). The client can reply to the message by encapsulating the response and signaling the peer's address in the encapsulation meta data. When the TURN server relays the response, it removes the TURN encapsulation. After receiving the response, the peer sends UDP encapsulated ESP packets with an SPI that matches the registered HLI. The TURN server detects the match and forwards the packets without any encapsulation. The TURN client's IPsec stack receives the data and processes it accordingly. When the program using IPsec sends data back to the peer, the IPsec stack automatically sends the data (with only UDP encapsulation) to the TURN server. The TURN server detects that the data matches to a registered HLI and forwards the data to the peer whose address was registered for the HLI. It will be readily apparent that the great majority of the packets exchanged do not require TURN encapsulation when utilising the approach described here.

[0040] While the method above uses simple byte arrays for matching data to permissions, more complicated forwarding rules could be implemented. For example, one could augment the byte arrays with bit-masks and allow bit-level checks for multiplexing the connections. Also, instead of just a single forwarding rule, a TURN client could add multiple rules that all match to a certain peer address. Even logical operations taking into account multiple byte/bit positions in the data could be used for selecting a rule. This would make it possible, for example, to forward all packets to the TURN client without encapsulation, except for packets relating to NAT traversal connectivity checks (and for which the real sender address information is necessary).

[0041] Figure 5 illustrates schematically a client terminal 1 (or UE) and a TURN server 5 configured to implement the approach described above (with a NAT interposed between these two entities). Within the UE 1, a NAT traversal unit 6 is provided, the role of which is to register the UE with TURN server in order to allocate to the UE a relayed address. An HLI determining unit 7 is provided to determine appropriate HLIs for both inbound and outbound flows towards a given peer. Once determined, these HLIs are passed to an HLI registration unit 8 which registers the HLIs with the TURN server, in association with the address of the peer. The registration details are also passed to a packet handler 9 which uses the HLIs and the peer's address to determine whether or not TURN encapsulation is required for outgoing packets, and to correctly route incoming packets to higher layers.

[0042] Figure 5 further illustrates the TURN server 5. This comprises a client terminal registration unit 10 and associated memory 11 for registering HLI associations for the UE 1. An inbound packet inspector 12 is configured to examine packets addressed to the relayed address to identify the registered inbound HLI, and to forward such packets to the UE without TURN encapsulation. An outbound packet inspector 13 is configured to identify the registered outbound HLI in packets received from the UE, and to route packets to the destination address of the peer accordingly. It will be appreciated of course that the TURN server will handle multiple HLI registrations in parallel for different UEs (and also, potentially, for the same UE).

[0043] Figure 6 is a flow diagram illustrating the main steps in the HLI based packet handling process. The process begins at step 100, and at step 200 the UE registers itself with the TURN server to obtain a relayed address. This registration may occur before the user decides to initiate a session. Assuming that this is the case, at step 300 the user initiates a session with a peer, via the UE. This step may be in response to receipt of a session initiation message from the peer (e.g. received via the TURN server using TURN encapsulation or via some other relay server). At step 400 the UE then determines inbound and outbound HLIs for the session, and registers these with the TURN server, in association with an address of the peer, at step 500. Following completion of this registration step, at steps 600 and 700, the UE and TURN server handle packets as described, to avoid TURN encapsulation between the UE and the TURN server. Steps 600 and 700 are performed in parallel.

[0044] The following subsections illustrate how HLI relaying can be used with some example protocols, other than ESP. The list is not exhaustive however, and the skilled person will appreciate that the approach described is applicable to a large number of different protocols.

Real-time Transport Protocol (RTP)

[0045] RTP [RFC3550: RTP: A Transport Protocol for Real-Time Applications. RFC 3550. July 2003] packets start with a fixed header, as illustrated in Figure 7. The SSRC field, used to label streams from different sources, contains a random number that is required to be globally unique within an RTP session. When using RTP with HLI

relaying, the TURN client sets its outbound HLI to match to its own SSRC used with a certain peer, and its inbound HLI to match the SSRC of the peer.

Host Identity Protocol (HIP)

[0046] A HIP [RFC5201: Host Identity Protocol. RFC 5201. April 2008] packet header is logically an IPv6 extension header and its format is shown in Figure 8. The sender and receiver Host Identity Tags (HITs) identify the communicating endpoints and are therefore suitable for HLIs. The TURN client using HLI relaying sets the outbound HLI to match the "receiver's HIT" with the peer's HIT and the inbound HLI to match the "sender's HIT" with the peer's HIT.

[0047] TCP port numbers may also be used as HLIs in the case where TCP packets are encapsulated in UDP.

[0048] It will be apparent from the above discussion that HLI-based relaying removes or reduces the bandwidth overhead created by TURN encapsulation between the TURN client and server. Also, the processing overhead is reduced since there is no need to add and remove the encapsulation headers at TURN client and server. Furthermore, native operating system stacks can be used for handling the relayed data due to the absence of a requirement for encapsulation. The solution is backward compatible with existing TURN clients and does not require HLI support from peers.

[0049] The extended TURN server described here is not protocol dependent and the HLI-based relaying can be achieved for any protocol that is carried over UDP and contains sufficient markers that can be used for multiplexing connections. Even where a protocol does not provide for such markers, if there is no requirement for multiplexing multiple connections (e.g., only a single connection through the TURN server is used), HLIs with zero length can be used to make TURN encapsulation unnecessary.

[0050] HLIs registered with the TURN server may be considered more generally as a rule set. For example, where no single, unique, identifier is present in packets a rule set such as, "If HLI_1 is at position 1 and HLI_2 in position 2 but there is no HLI_3 in position 3, a packet matches to a relaying rule/permission" may be specified and registered with the TURN server.

[0051] It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, the approach may be applied to relaying protocols other than TURN (and which use encapsulation of the relayed packets), e.g. SOCKS 5 (IETF RFC 1928), and indeed to further enhancements of the currently specified TURN protocol, for example. Certain embodiments may allow the TURN server, or some other network based node, to determine the HLIs to be used for a session. In this case, that determining node may signal the HLI(s) to the TURN client, and also to the TURN server if the node is not itself the TURN server. The skilled person will also appreciate that the relaying mechanism described here is not only applicable to NAT traversal. It could for example be applied to a scenario where a client makes use of a relay server in order to maintain anonymity. The skilled person will also appreciate that a benefit may be achieved by applying this HLI-based approach in only one of the inbound and outbound directions, and not both.

Claims

1. Apparatus (5) for relaying packets between a first host (1) and a second host (3), the apparatus comprising:

   a memory (11) for registering for said first host (1)

   an address of the first host (1),
   a relayed address of the first host (1),

   the apparatus **characterized by**:

   the memory including, for said first host (1),

   an address of the second host (3), and
   an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier;

   and one or both of

   an outbound packet inspector (13) for inspecting packets received from said first host (1) and addressed to an address of the apparatus to determine whether or not they contain a registered outbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the second host (3);
   an inbound packet inspector (12) for inspecting packets received from said second host (3) and addressed to said relayed address to determine whether or not they contain a registered inbound Higher Layer Identifier and, if so, for forwarding the packets to said address of the first host (1).

2. Apparatus (5) according to claim 1, said outbound packet inspector (13) being configured to replace the address of the first host in a source address field of packets to be forwarded to said second host (3), with said relayed address.

3. Apparatus (5) according to claim 1 or 2, said inbound packet inspector (12) being configured to replace said relayed address in a destination address field of packets to be forwarded to said first host (1), with said address of the first host (1), and to replace said

address of the second host (3) in a source address field of those packets with an address of the apparatus.

4. Apparatus (5) according to any one of the preceding claims, said inbound packet inspector (12) being configured to deliver packets which contain said inbound Higher Layer Identifier, to said first host (1), without additional relay encapsulation.

5. Apparatus (5) according to any one of the preceding claims, wherein said memory is configured to additionally register for said first host (1) an offset position for the or each of said inbound and outbound Higher Layer Identifiers, the offset position identifying a position of the associated Higher Layer Identifier within a packet, and the outbound and inbound packet inspectors (12) being configured to use the respective offset position to determine the presence of a Higher Layer Identifier.

6. Apparatus (5) according to any one of the preceding claims, wherein said memory and the or each of said inbound packet inspector (12) and said outbound packet inspector (13) being configured to additionally handle the relaying of packets between said first host (1) and one or more further hosts using one or both of the inbound and outbound Higher Layer Identifiers.

7. Apparatus (5) according to any one of the preceding claims, wherein said first host (1) is located behind a Network Address Translator (2), and said address of the first host (1) is a NATed address of the first host (1).

8. Apparatus (5) according to claim 7 when appended to claim 4, wherein said additional relay encapsulation is encapsulation according to the Traversal Using Relays around NAT protocol.

9. Apparatus (5) according to claim 7 or 8 and comprising a client terminal registration unit for registering said first host (1) and any further hosts, the registration unit being configured to use the Traversal Using Relays around NAT, TURN, protocol.

10. A client terminal (1) configured to exchange packets with a peer terminal (3) via a relay server (5), the client terminal (1) comprising:

a relay unit for registering with the relay server (5) so as to be allocated a relayed address by the relay server (5); and being **characterised by**:

an identification determining unit (7) for determining an inbound Higher Layer Identifier to be used in packets exchanged with said peer terminal (3);
an identifier registration unit (8) for registering the inbound Higher Layer Identifier with said relay server (5), together with said relayed address, an address of the client terminal, and an address of the peer terminal;
a packet handler (9) for associating packets received from said relay server (5) with said peer terminal (3) using said inbound Higher Layer Identifier.

11. A client terminal (1) according to claim 10, said identification determining unit (7) being configured to determine an outbound Higher Layer Identifier to be used in packets exchanged with said peer terminal (3), and said identifier registration unit (8) being configured to register the outbound Higher Layer Identifier with said relay server (5) together with the inbound Higher Layer Identifier.

12. A client terminal (1) according to claim 9 or 10, said identification determining unit (7) being configured to determine inbound and/or outbound Higher Layer Identifiers by identifying and using one of the following protocol parameters:

a Host Identity Tag, HIT;
a synchronisation source (SSRC) identifier;
a Security Parameter Index (SPI);
TCP port numbers.

13. A client terminal (1) according to any one of claims 10 to 12, said relay unit being configured to implement NAT traversal and said address of the client terminal being a NATed address.

14. A client terminal (1) according to claim 13, said relay unit and said identifier registration unit (8) being configured to use the Traversal Using Relays around NAT, TURN, protocol.

15. A client terminal (1) according to claim 13 or 14 and comprising a further packet handler (9) for using Traversal Using Relays around NAT, TURN, encapsulation to send and/or receive packets to a peer terminal (3) in the event that said identification determining unit (7) is unable to determine an inbound and, optionally, an outbound Higher Layer Identifier, or a TURN encapsulated packet is received from said relay server (5).

16. A client terminal (1) according to any one of claims 13 to 15, said relay unitbeing configured to determine whether or not a relay server (5) supports a Higher Layer Identifier based relaying method and, if not, to initiate packet routing with said peer terminal (3) using relaying encapsulation.

17. A method of sending packets between a first host (1) and a second host (3), the method comprising:

registering at a relay server (5), on behalf of the first host (1)

an address of the first host (1),
a relayed address of the first host (1),

the method **characterised by**:

registering at a relay server (5), on behalf of the first host (1)

an address of the second host (3), and
an outbound Higher Layer Identifier and/or an inbound Higher Layer Identifier;

and one or both of the steps of
at the relay server (5), inspecting packets received from said first host (1) and addressed to an address of the relay server (5) to determine whether or not they contain said outbound Higher Layer Identifier and, if so, forwarding the packets to said address of the second host (3);
inspecting packets received from said second host (3) and addressed to said relayed address to determine whether or not they contain said inbound Higher Layer Identifier and, if so, forwarding the packets to said address of the first host (1).

18. A method according to claim 17, wherein said first host (1) is located behind a Network Address Translator.

19. A method according to claim 18, said step of registering being carried out using the Traversal Using Relays around NAT, TURN, protocol.

20. A method according to claim 19 and comprising forwarding the packets from the relay server to the first host (1) using TURN encapsulation if packets received from the second host (3) do not contain said inbound Higher Layer Identifier.

Patentansprüche

1. Vorrichtung (5) zur Vermittlung von Paketen zwischen einem ersten Host (1) und einem zweiten Host (3), wobei die Vorrichtung umfasst:

einen Speicher (11) zur Registrierung von Folgendem für den ersten Host (1):

einer Adresse des ersten Hosts (1),
einer vermittelten Adresse des ersten Hosts (1),
wobei die Vorrichtung **gekennzeichnet ist**

dadurch, dass der Speicher Folgendes für den ersten Host (1) aufweist:

eine Adresse des zweiten Hosts (3) und
eine abgehende höherschichtige Kennung und/oder eine eingehende höherschichtige Kennung;
und **durch** eines oder beides von Folgendem:

einen Abgangspaketinspektor (13) zum Inspizieren von Paketen, die von dem ersten Host (1) kommend empfangen werden und an eine Adresse der Vorrichtung adressiert sind, um zu bestimmen, ob sie eine registrierte abgehende höherschichtige Kennung enthalten ist oder nicht, und wenn ja, zum Vermitteln der Pakete an die Adresse des zweiten Hosts (3),
einen Eingangspaketinspektor (12) zum Inspizieren von Paketen, die von dem zweiten Host (3) kommend empfangen werden und an die vermittelte Adresse adressiert sind, um zu bestimmen, ob sie eine registrierte eingehende höherschichtige Kennung enthalten oder nicht, und wenn ja, zum Vermitteln der Pakete an die Adresse des ersten Hosts (1).

2. Vorrichtung (5) nach Anspruch 1, wobei der Abgangspaketinspektor (13) dafür konfiguriert ist, die Adresse des ersten Hosts in einem Quelladressfeld von Paketen, die an den zweiten Host (3) weiterzuleiten sind, durch die vermittelte Adresse zu ersetzen.

3. Vorrichtung (5) nach Anspruch 1 oder 2, wobei der Eingangspaketinspektor (12) dafür konfiguriert ist, die vermittelte Adresse in einem Zieladressfeld von Paketen, die an den ersten Host (1) weiterzuleiten sind, durch die Adresse des ersten Hosts (1) zu ersetzen und die Adresse des zweiten Hosts (3) in einem Quelladressfeld dieser Pakete durch eine Adresse der Vorrichtung zu ersetzen.

4. Vorrichtung (5) nach einem der vorhergehenden Ansprüche, wobei der Eingangspaketinspektor (12) dafür konfiguriert ist, Pakete, die die eingehende höherschichtige Kennung enthalten, ohne zusätzliche Vermittlungseinkapselung an den ersten Host (1) zu liefern.

5. Vorrichtung (5) nach einem der vorhergehenden Ansprüche, wobei der Speicher dafür konfiguriert ist, für den ersten Host (1) eine Verschiebungsposition

für die oder jede der eingehenden und abgehenden höherschichtigen Kennungen zusätzlich zu registrieren, wobei die Verschiebungsposition eine Position der zugeordneten höherschichtigen Kennung in einem Paket identifiziert und die Abgangs- und Eingangspaketinspektoren (12) dafür konfiguriert sind, die jeweilige Verschiebungsposition zu verwenden, um das Vorhandensein einer höherschichtigen Kennung zu bestimmen.

6. Vorrichtung (5) nach einem der vorhergehenden Ansprüche, wobei der Speicher und der oder jeder, nämlich der Eingangspaketinspektor (12) und der Abgangspaketinspektor (13) dafür konfiguriert sind, die Vermittlung von Paketen zwischen dem ersten Host (1) und einem oder mehreren weiteren Hosts unter Verwendung von einer oder beiden der eingehenden und ausgehenden höherschichtigen Kennungen zusätzlich abzuwickeln.

7. Vorrichtung (5) nach einem der vorhergehenden Ansprüche, wobei der erste Host (1) sich hinter einem NAT bzw. Netzadressübersetzer (2) befindet und die Adresse des ersten Hosts (1) eine NAT-verarbeitete Adresse des ersten Hosts (1) ist.

8. Vorrichtung (5) nach Anspruch 7, sofern abhängig von Anspruch 4, wobei die zusätzliche Vermittlungseinkapselung eine Einkapselung gemäß dem Traversal Using Relays around NAT-Protokoll ist.

9. Vorrichtung (5) nach Anspruch 7 oder 8 und umfassend eine Client-Endgerät-Registrierungseinheit für die Registrierung der ersten Hosts (1) und jeglicher weiterer Hosts, wobei die Registrierungseinheit dafür konfiguriert ist, das Traversal Using Relays around NAT- bzw. TURN-Protokoll zu verwenden.

10. Client-Endgerät (1), das dafür konfiguriert ist, Pakete über einen Vermittlungsserver (5) mit einem gleichrangigen Endgerät (3) auszutauschen, wobei das Client-Endgerät (1) umfasst:

eine Vermittlungseinheit zur Registrierung beim Vermittlungsserver (5), um durch den Vermittlungsserver (5) eine vermittelte Adresse zugewiesen zu bekommen; und **gekennzeichnet durch**:

eine Identifikationsbestimmungseinheit (7) zum Bestimmen einer eingehenden höherschichtigen Kennung, die in Paketen zu verwenden ist, die mit dem gleichrangigen Endgerät (3) ausgetauscht werden;
eine Kennungsregistrierungsseinheit (8) zur Registrierung der eingehenden höherschichtigen Kennung bei dem Vermittlungsserver (5) zusammen mit der vermittelten Adresse, einer Adresse des Client-Endgerätes und einer Adresse des gleichrangigen Endgerätes;
einen Paket-Handler (9) zum Zuordnen von Paketen, die von dem Vermittlungsserver (5) empfangen werden, zu dem gleichrangigen Endgerät (3) unter Verwendung der eingehenden höherschichtigen Kennung.

11. Client-Endgerät (1) nach Anspruch 10, wobei die Identifikationsbestimmungseinheit (7) dafür konfiguriert ist, eine abgehende höherschichtige Kennung zu bestimmen, die in Paketen zu verwenden ist, die mit dem gleichrangigen Endgerät (3) ausgetauscht werden, und die Kennungsregistrierungseinheit (8) dafür konfiguriert ist, die abgehende höherschichtige Kennung zusammen mit der eingehenden höherschichtigen Kennung bei dem Vermittlungsserver (5) zu registrieren.

12. Client-Endgerät (1) nach Anspruch 9 oder 10, wobei die Identifikationsbestimmungseinheit (7) dafür konfiguriert ist, eingehende und/oder abgehende höherschichtige Kennungen zu bestimmen, indem einer der folgenden Protokoll-Parameter identifiziert und verwendet wird:

ein Host-Identitäts-Tag, HIT;
eine Synchronisationsquellen-(SSRC-)Kennung;
einen Sicherheitsparameterindex (SPI);
TCP-Portnummern.

13. Client-Endgerät (1) nach einem der Ansprüche 10 bis 12, wobei die Vermittlungseinheit dafür konfiguriert ist, einen NAT-Durchlauf zu implementieren, und die Adresse des Client-Endgerätes eine NAT-verarbeitete Adresse ist.

14. Client-Endgerät (1) nach Anspruch 13, wobei die Vermittlungseinheit und die Kennungsregistrierungseinheit (8) dafür konfiguriert sind, das Traversal Using Relays around NAT- bzw. TURN-Protokoll zu verwenden.

15. Client-Endgerät (1) nach Anspruch 13 oder 14 und umfassend einen weiteren Paket-Handler (9) zur Verwendung der Traversal Using Relays around NAT- bzw. TURN-Einkapselung, um Pakete an ein gleichrangiges Endgerät (3) für den Fall zu senden und/oder zu empfangen, dass die Identifikationsbestimmungseinheit (7) nicht in der Lage ist, eine eingehende und gegebenenfalls eine abgehende höherschichtige Kennung zu bestimmen, oder ein TURN-gekapseltes Paket von dem Vermittlungsserver (5) empfangen wird.

16. Client-Endgerät (1) nach einem der Ansprüche 13

bis 15, wobei die Vermittlungseinheit dafür konfiguriert ist, zu bestimmen, ob ein Vermittlungsserver (5) ein auf einer höherschichtigen Kennung beruhendes Vermittlungsverfahren unterstützt oder nicht, und wenn nicht, Paketweiterleitung mit dem gleichrangigen Endgerät (3) unter Verwendung einer Vermittlungseinkapselung zu initiieren.

17. Verfahren zum Senden von Paketen zwischen einem ersten Host (1) und einem zweiten Host (3), wobei das Verfahren umfasst:

Registrieren von Folgendem in einem Vermittlungsserver (5) im Auftrag des ersten Hosts (1):

eine Adresse des ersten Hosts (1),
eine vermittelte Adresse des ersten Hosts (1),
wobei das Verfahren **gekennzeichnet ist durch**:

Registrieren von Folgendem in einem Vermittlungsserver (5) im Auftrag des ersten Hosts (1):

eine Adresse des zweiten Hosts (3) und
eine abgehende höherschichtige Kennung und/oder eine eingehende höherschichtige Kennung,

und **durch** einen oder beide der folgenden Schritte:

im Vermittlungsserver (5) erfolgendes Inspizieren von Paketen, die von dem ersten Host (1) kommend empfangen werden und an eine Adresse des Vermittlungsservers (5) adressiert sind, um zu bestimmen, ob sie die abgehende höherschichtige Kennung enthalten oder nicht, und wenn ja, Vermitteln der Pakete an die Adresse des zweiten Hosts (3);
Inspizieren von Paketen, die von dem zweiten Host (3) kommend empfangen werden und an die vermittelte Adresse adressiert sind, um zu bestimmen, ob sie die eingehende höherschichtige Kennung enthalten oder nicht, und wenn ja, Vermitteln der Pakete an die Adresse des ersten Hosts (1).

18. Verfahren nach Anspruch 17, wobei der erste Host (1) sich hinter einem Netzadressübersetzer befindet.

19. Verfahren nach Anspruch 18, wobei der Schritt der Registrierung unter Verwendung des Traversal Using Relays around NAT- bzw. TURN-Protokolls durchgeführt wird.

20. Verfahren nach Anspruch 19 und umfassend: Vermitteln der Pakete vom Vermittlungsserver an den ersten Host (1) unter Verwendung einer TURN-Einkapselung, wenn von dem zweiten Host (3) empfangene Pakete die eingehende höherschichtige Kennung nicht enthalten.

Revendications

1. Appareil (5) destiné à relayer des paquets entre un premier hôte (1) et un second hôte (3), l'appareil comprenant :

une mémoire (11) destinée à enregistrer, pour ledit premier hôte (1) :

une adresse du premier hôte (1) ;
une adresse relayée du premier hôte (1) ;

l'appareil étant **caractérisé en ce que** :

la mémoire comporte, pour ledit premier hôte (1) :
une adresse du second hôte (3) ; et
un identifiant de couche supérieure sortant et/ou un identifiant de couche supérieure entrant ;

et un ou les deux modules parmi :

un module d'inspection de paquets sortants (13) destiné à inspecter des paquets reçus à partir dudit premier hôte (1) et adressés à une adresse de l'appareil, en vue de déterminer s'ils contiennent ou non un identifiant de couche supérieure sortant enregistré et, le cas échéant, d'acheminer les paquets vers ladite adresse du second hôte (3) ;
un module d'inspection de paquets entrants (12) destiné à inspecter des paquets reçus à partir dudit second hôte (3) et adressés à ladite adresse relayée, en vue de déterminer s'ils contiennent ou non un identifiant de couche supérieure entrant enregistré et, le cas échéant, d'acheminer les paquets vers ladite adresse du premier hôte (1).

2. Appareil (5) selon la revendication 1, dans lequel ledit module d'inspection de paquets sortants (13) est configuré de manière à remplacer l'adresse du premier hôte dans un champ d'adresse source de paquets à acheminer audit second hôte (3), par ladite adresse relayée.

3. Appareil (5) selon la revendication 1 ou 2, dans lequel ledit module d'inspection de paquets entrants (12) est configuré de manière à remplacer ladite adresse relayée, dans un champ d'adresse de destination de paquets à acheminer audit premier hôte (1), par ladite adresse du premier hôte (1), et à remplacer ladite adresse du second hôte (3), dans un

champ d'adresse source de ces paquets, par une adresse de l'appareil.

4. Appareil (5) selon l'une quelconque des revendications précédentes, dans lequel ledit module d'inspection de paquets entrants (12) est configuré de manière à délivrer des paquets qui contiennent ledit identifiant de couche supérieure entrant, audit premier hôte (1), sans encapsulation de relais supplémentaire.

5. Appareil (5) selon l'une quelconque des revendications précédentes, dans lequel ladite mémoire est configurée de manière à enregistrer en outre, pour ledit premier hôte (1), une position de décalage pour lesdits ou chacun desdits identifiants de couches supérieures sortants et entrants, la position de décalage identifiant une position de l'identifiant de couche supérieure associé au sein d'un paquet, et les modules d'inspection de paquets entrants et sortants (12) étant configurés de manière à utiliser la position de décalage respective en vue de déterminer la présence d'un identifiant de couche supérieure.

6. Appareil (5) selon l'une quelconque des revendications précédentes, dans lequel ladite mémoire et le ou chaque module parmi ledit module d'inspection de paquets entrants (12) et ledit module d'inspection de paquets sortants (13) sont configurés de manière à traiter en outre la transmission par relais de paquets entre ledit premier hôte (1) et un ou plusieurs hôtes supplémentaires en utilisant l'un et/ou l'autre des identifiants de couches supérieures sortants et entrants.

7. Appareil (5) selon l'une quelconque des revendications précédentes, dans lequel ledit premier hôte (1) est situé derrière un traducteur d'adresses réseau (2), et ladite adresse du premier hôte (1) est une adresse NAT traduite du premier hôte (1).

8. Appareil (5) selon la revendication 7, lorsqu'elle dépend de la revendication 4, dans lequel ladite encapsulation de relais supplémentaire est une encapsulation selon le protocole TURN de traversée des obstacles (Traversal Using Relays around NAT, TURN).

9. Appareil (5) selon la revendication 7 ou 8, comprenant une unité d'enregistrement de terminaux clients destinée à enregistrer ledit premier hôte (1) et d'autres hôtes quelconques, l'unité d'enregistrement étant configurée de manière à utiliser le protocole Traversal Using Relays around NAT, TURN.

10. Terminal client (1) configuré de manière à échanger des paquets avec un terminal homologue (3) par l'intermédiaire d'un serveur relais (5), le terminal client (1) comprenant :

une unité relais destinée à l'enregistrement auprès du serveur relais (5) de manière à se voir affecter une adresse relayée par le serveur relais (5) ; et étant **caractérisé par** :

une unité de détermination d'identification (7) destinée à déterminer un identifiant de couche supérieure entrant à utiliser dans des paquets échangés avec ledit terminal homologue (3) ;
une unité d'enregistrement d'identifiant (8) destinée à enregistrer l'identifiant de couche supérieure entrant auprès dudit serveur relais (5), conjointement avec ladite adresse relayée, une adresse du terminal client, et une adresse du terminal homologue ;
un module de traitement de paquets (9) destiné à associer des paquets, reçus à partir dudit serveur relais (5), audit terminal homologue (3), en utilisant ledit identifiant de couche supérieure entrant.

11. Terminal client (1) selon la revendication 10, dans lequel ladite unité de détermination d'identification (7) est configurée de manière à déterminer un identifiant de couche supérieure sortant à utiliser dans des paquets échangés avec ledit terminal homologue (3), et ladite unité d'enregistrement d'identifiant (8) est configurée de manière à enregistrer l'identifiant de couche supérieure sortant auprès dudit serveur relais (5) conjointement avec l'identifiant de couche supérieure entrant.

12. Terminal client (1) selon la revendication 9 ou 10, dans lequel ladite unité de détermination d'identification (7) est configurée de manière à déterminer des identifiants de couches supérieures sortants et/ou entrants en identifiant et en utilisant l'un des paramètres de protocole ci-dessous :

une balise d'identité d'hôte, HIT ;
un identifiant de source de synchronisation (SSRC) ;
un index de paramètres de sécurité (SPI) ; et
des numéros de port TCP.

13. Terminal client (1) selon l'une quelconque des revendications 10 à 12, dans lequel ladite unité relais est configurée de manière à mettre en oeuvre une traversée de NAT et ladite adresse du terminal client est une adresse NAT traduite.

14. Terminal client (1) selon la revendication 13, dans lequel ladite unité relais et ladite unité d'enregistrement d'identifiant (8) sont configurées de manière à utiliser le protocole Traversal Using Relays around

NAT, TURN.

15. Terminal client (1) selon la revendication 13 ou 14 et comprenant un module de traitement de paquets (9) supplémentaire destiné à utiliser une encapsulation Traversal Using Relays around NAT, TURN, en vue d'envoyer et/ou de recevoir des paquets vers ou à partir d'un terminal homologue (3) dans le cas où ladite unité de détermination d'identification (7) n'est pas en mesure de déterminer un identifiant de couche supérieure entrant et, éventuellement, un identifiant de couche supérieure sortant, ou un paquet encapsulé par encapsulation TURN est reçu à partir dudit serveur relais (5).

16. Terminal client (1) selon l'une quelconque des revendications 13 à 15, dans lequel ladite unité relais est configurée de manière à déterminer si un serveur relais (5) prend ou non en charge un procédé de relais à base d'identifiant de couche supérieure et, dans la négative, à initier un routage de paquets avec ledit terminal homologue (3), en utilisant une encapsulation de relais.

17. Procédé d'envoi de paquets entre un premier hôte (1) et un second hôte (3), le procédé consistant à :

enregistrer au niveau d'un serveur relais (5), au nom du premier hôte (1) :

une adresse du premier hôte (1) ;
une adresse relayée du premier hôte (1) ;

le procédé étant **caractérisé en ce qu'**il consiste à :

enregistrer au niveau d'un serveur relais (5), au nom du premier hôte (1) :

une adresse du second hôte (3) ; et
un identifiant de couche supérieure sortant et/ou un identifiant de couche supérieure entrant ;

et une ou les deux étapes ci-dessous consistant à :

au niveau du serveur relais (5), inspecter des paquets reçus à partir dudit premier hôte (1) et adressés à une adresse du serveur relais (5), en vue de déterminer s'ils contiennent ou non ledit identifiant de couche supérieure sortant et, le cas échéant, d'acheminer les paquets vers ladite adresse du second hôte (3) ;
inspecter des paquets reçus à partir dudit second hôte (3) et adressés à ladite adresse relayée, en vue de déterminer s'ils contiennent ou non ledit identifiant de couche supérieure entrant et, le cas échéant, d'acheminer les paquets vers ladite adresse du premier hôte (1).

18. Procédé selon la revendication 17, dans lequel ledit premier hôte (1) est situé derrière un traducteur d'adresses réseau.

19. Procédé selon la revendication 18, dans lequel ladite étape d'enregistrement est mise en oeuvre en utilisant le protocole Traversal Using Relays around NAT, TURN.

20. Procédé selon la revendication 19 et consistant à acheminer les paquets, du serveur relais au premier hôte (1), en utilisant une encapsulation TURN si les paquets reçus à partir du second hôte (3) ne contiennent pas ledit identifiant de couche supérieure entrant.

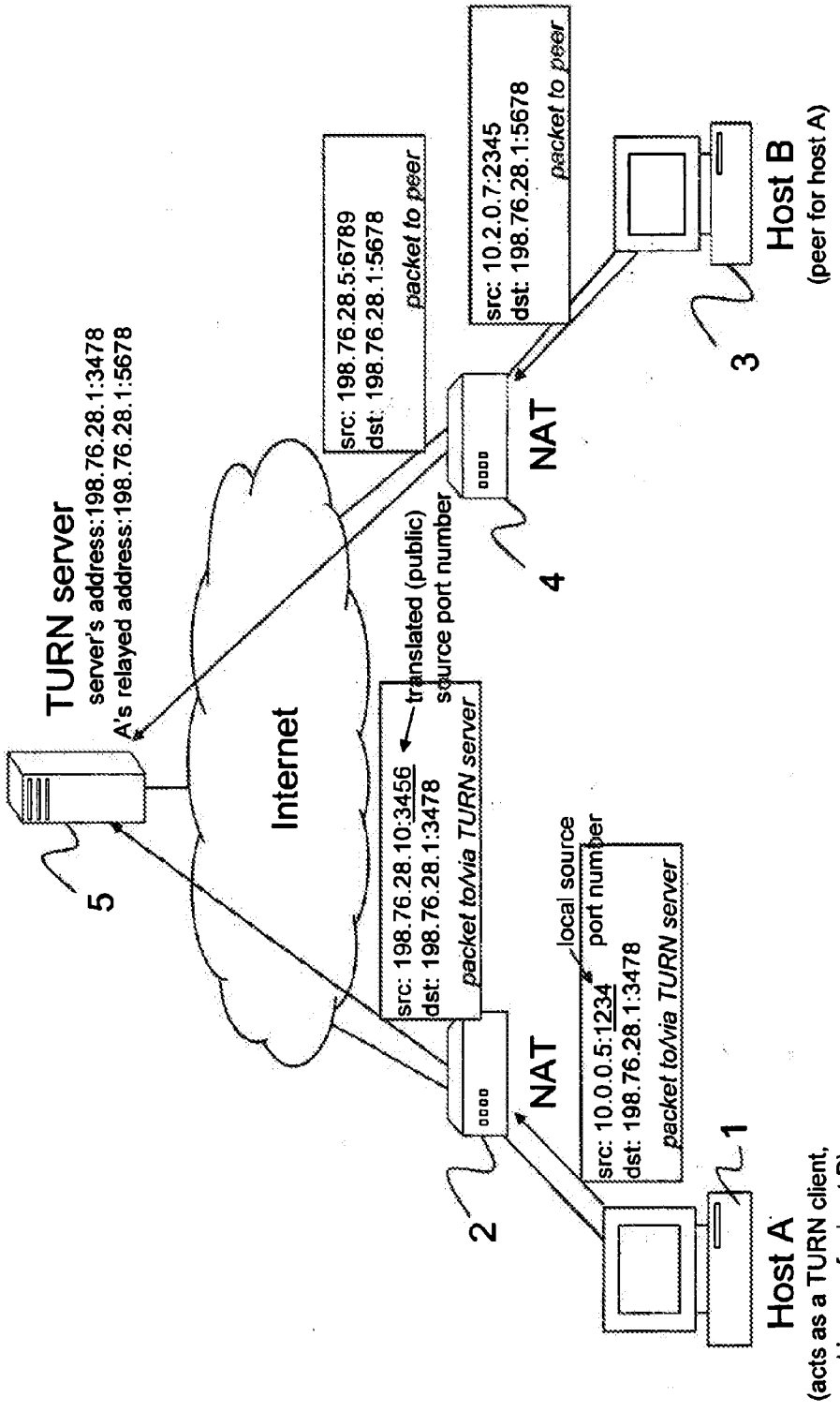


Figure 1

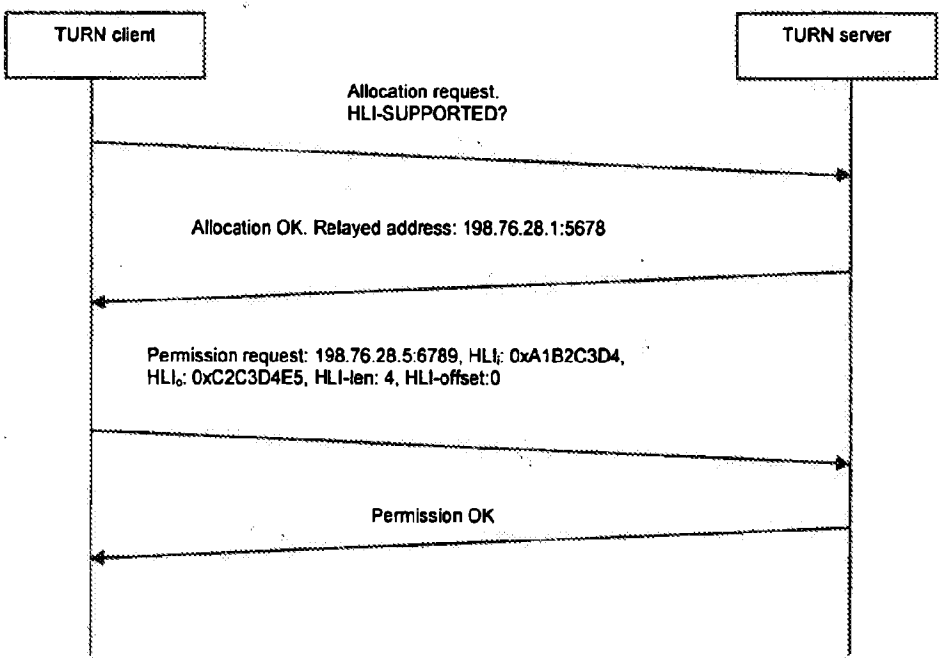


Figure 2

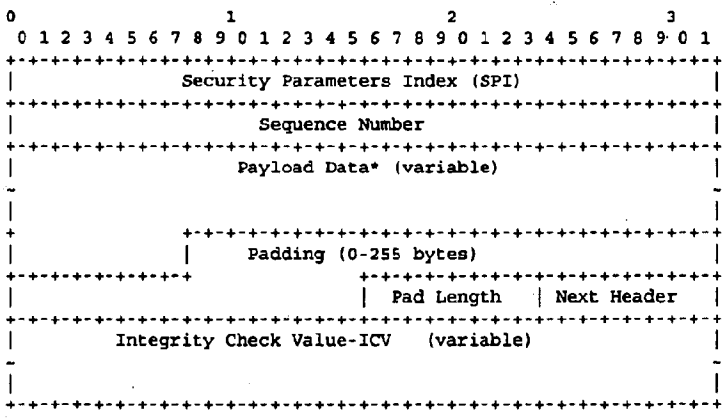


Figure 3

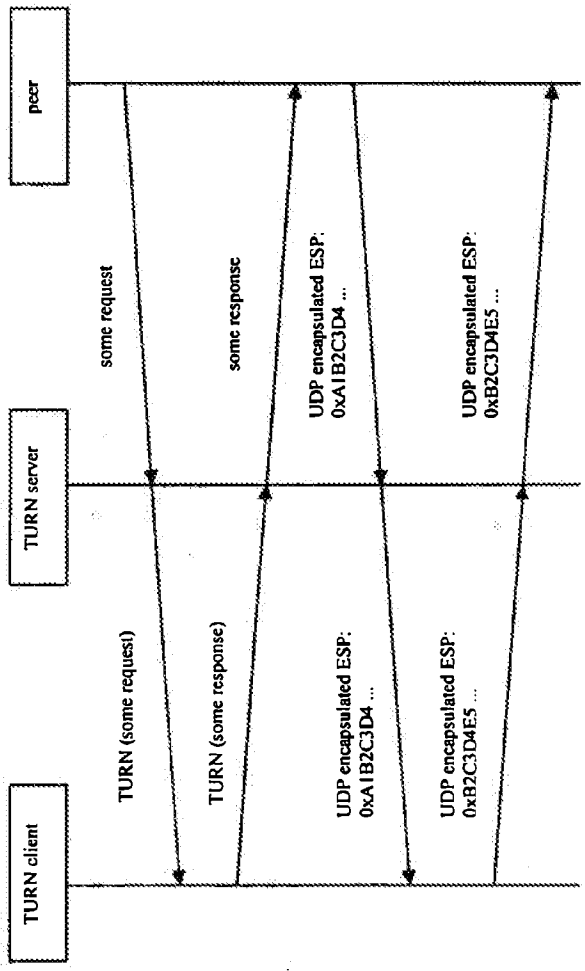


Figure 4

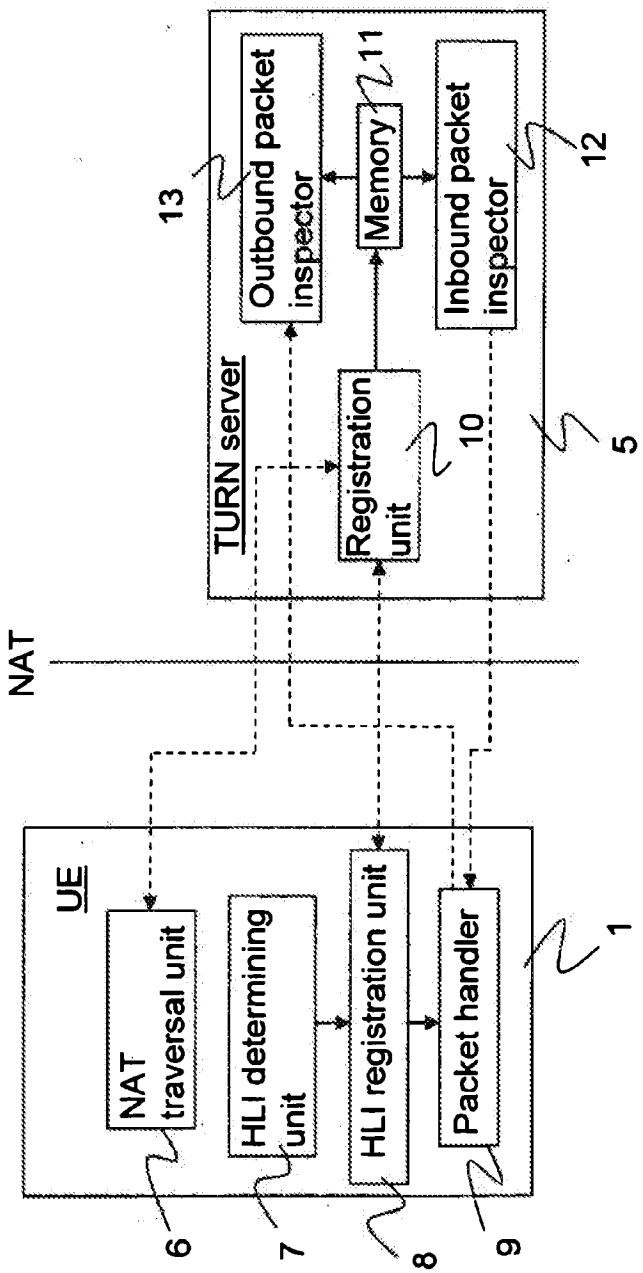


Figure 5

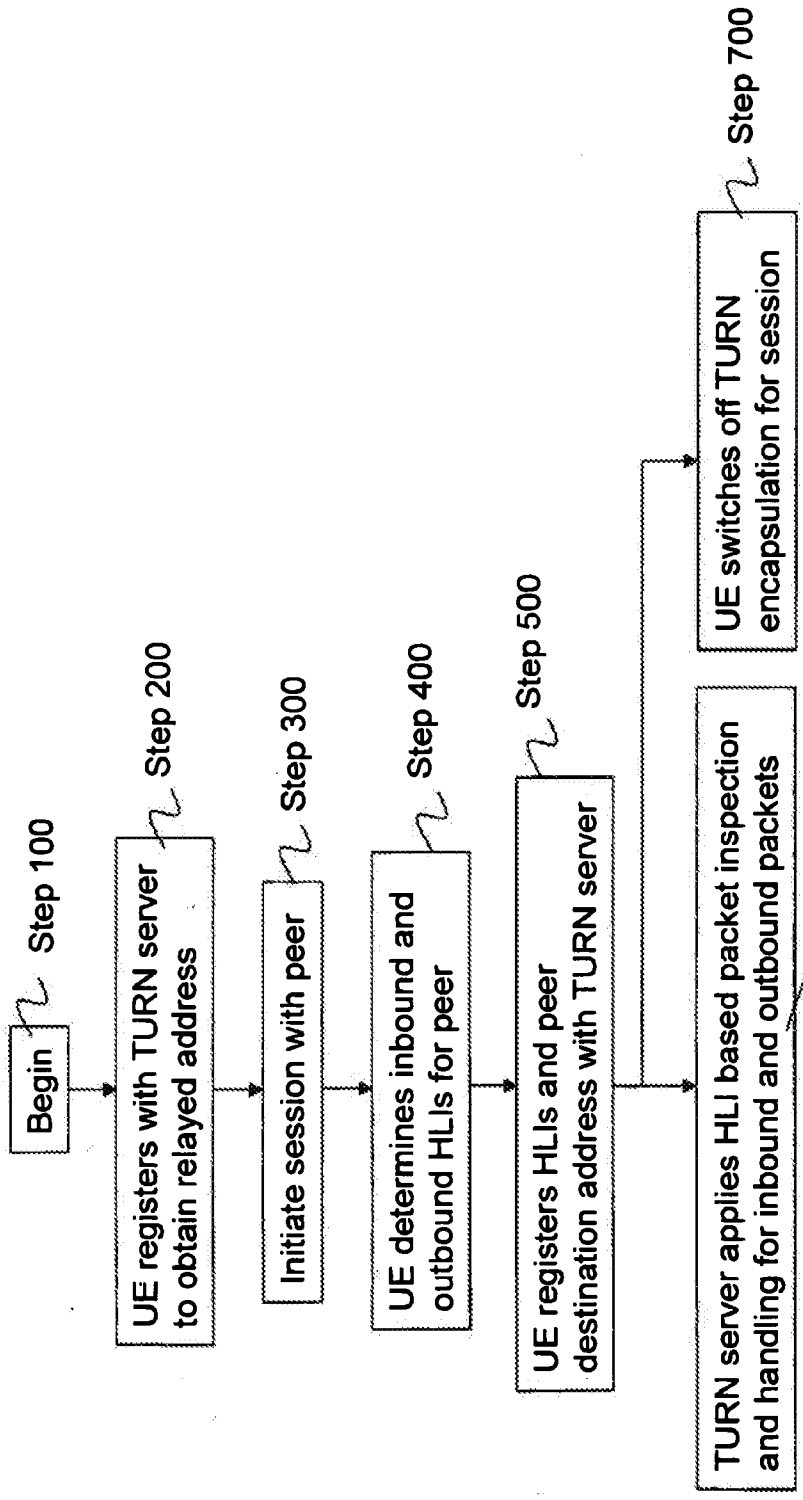


Figure 6

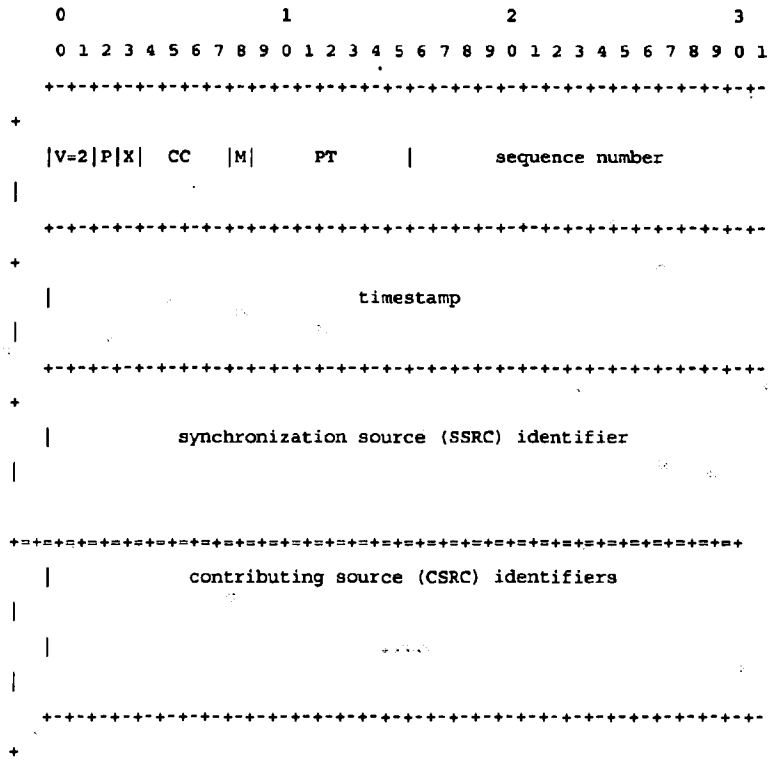


Figure 7

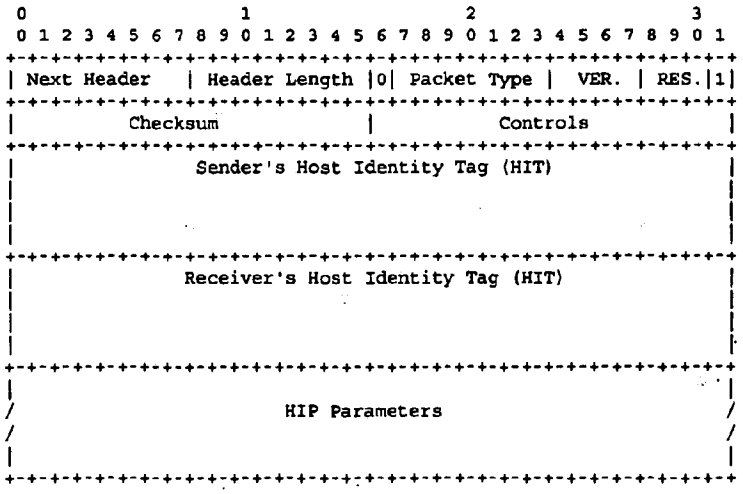


Figure 8

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **J. ROSENBERG.** *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols,* October 2007 **[0003]**
- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN,* February 2009 **[0004]**
- *Traversal Using Relays around NAT: Relay Extensions to Session Traversal Utilities for NAT,* 08 July 2007 **[0008]**
- **ROSENBERG J et al.** *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN, draft-ietf-behave-turn-07.txt* **[0008]**
- *HIP Extensions for the Traversal of Network Address Translators,* 06 July 2007 **[0010]**
- RFC3550: RTP: A Transport Protocol for Real-Time Applications. *RFC 3550,* July 2003 **[0045]**
- RFC5201: Host Identity Protocol. *RFC 5201,* April 2008 **[0046]**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 266 516 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
07.05.2014 Bulletin 2014/19

(21) Application number: **01918523.0**

(22) Date of filing: **12.03.2001**

(51) Int Cl.:
H04M 7/00 *(2006.01)* ***H04M 1/253*** *(2006.01)*
H04M 3/42 *(2006.01)*

(86) International application number:
PCT/US2001/007686

(87) International publication number:
WO 2001/069899 (20.09.2001 Gazette 2001/38)

(54) **Establishing real-time interactive audio calls by a computer on behalf of a packet-switched data network telephone**

Herstellung von echtzeitbasierten interaktiven Audio-Anrufen von einem Computer im Auftrag eines paketvermittelten Datennetzwerk-Telefons

Établissement d'appels audio interactifs en temps réel par un ordinateur pour le compte d'un téléphone d'un réseau de données à commutation de paquets

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.03.2000 US 524342**

(43) Date of publication of application:
18.12.2002 Bulletin 2002/51

(73) Proprietor: **Genband US LLC**
Frisco, TX 75034 (US)

(72) Inventors:
- **SOLLEE, Patrick, N.**
  Richardson, TX 75082 (US)
- **CREECH, David, R.**
  Carrollton, TX 75007 (US)
- **OSTERHOUT, Gregory, T.**
  Coppell, TX 75019 (US)
- **JESSEN, Christopher, L.**
  McKinney, TX 75070 (US)

(74) Representative: **Brophy, David Timothy et al**
FRKelly
27 Clyde Road
Ballsbridge
Dublin 4 (IE)

(56) References cited:
EP-A- 0 721 266 **EP-A- 0 829 995**
EP-A- 0 836 295 **WO-A-99/05590**

- **THOM G A: "H. 323: THE MULTIMEDIA COMMUNICATIONS STANDARD FOR LOCAL AREA NETWORKS" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER. PISCATAWAY, N.J, US, vol. 34, no. 12, 1 December 1996 (1996-12-01), pages 52-56, XP000636454 ISSN: 0163-6804**
- **FOO S; YEO C K; HUI S C: "A telephone adapter for Internet telephony systems", MICROPROCESSORS AND MICROSYSTEMS, IPC BUSINESS PRESS LTD., vol. 21, no. 4, 30 December 1997 (1997-12-30), pages 213-221, XP004107416, LONDON, GB**
- **CATCHPOLE A; CROOK G; CHESTERMAN D: "INTRODUCTION TO COMPUTER TELEPHONY INTEGRATION", BRITISH TELECOMMUNICATIONS ENGINEERING, vol. 14, no. 2, 1 July 1995 (1995-07-01), pages 98-105, XP000520841, LONDON, GB**
- **BOULLET M: "Voice over IP in Alcatel OmniPCX 4400 and OmniOffice", ALCATEL TELECOMMUNICATIONS REVIEW, 1 January 2000 (2000-01-01), pages 7-11, XP007005352, ALCATEL, PARIS CEDEX, FR**

EP 1 266 516 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Background

[0001] The invention relates to controlling voice communications over a data network.

[0002] Data networks are widely used to link various types of network elements, such as personal computers, servers, gateways, network telephones, and so forth. Data networks may include private networks (such a local area networks or wide area networks) and public networks (such as the Internet). Popular forms of communications between network elements across such data networks include electronic mail, file transfer, web browsing, and other exchanges of digital data.

[0003] With the increased capacity and reliability of data networks, voice communications (including telephone calls, video conferencing, and so forth) over data networks have become possible. Voice communications over data networks are unlike voice communications in a conventional public switched telephone network (PSTN), which provides users with dedicated, end-to-end circuit connections for the duration of each call. Communications over data networks, such as IP (Internet Protocol) networks, are performed using packets or datagrams that are sent in bursts from a source to one or more destination nodes. Voice data sent over a data network typically shares network bandwidth with conventional non-voice data (e.g., data associated with electronic mail, file transfer, web access, and other traffic).

[0004] Various standards have been proposed for voice and multimedia communications over data networks. One such standard is the H.323 Recommendation from the International Telecommunications Union (ITU), which describes terminals, equipment, and services for multimedia communications over data networks.

[0005] Another standard for voice and multimedia communications is the Session Initiation Protocol (SIP), which establishes, maintains, and terminates multimedia sessions over a data network. SIP is part of a multimedia data and control architecture developed by the Internet Engineering Task Force (IETF). The IETF multimedia data and control architecture also includes the Resource Reservation Protocol (RSVP) for reserving network resources; the Real-Time Transport Protocol (RTP) for transporting real-time data and providing quality of service (QoS) feedback; the Real-Time Streaming Protocol (RTSP) for controlling delivery of streaming media; the Session Announcement Protocol (SAP) for advertising multimedia sessions by multicast; and the Session Description Protocol (SDP) for describing multimedia sessions.

[0006] To perform voice communications over a data network, a typical computer system (such as a desktop computer system or a portable computer system) may be equipped with voice processing capabilities. Such capabilities include a microphone, ear phones or speakers, and speech processing software. Typically, the speech processing software includes coder/decoders (CODECs) to encode and decode voice data. The voice processing software, including the CODECs, may be run on a microprocessor of a typical computer system. However, due to the intensive data processing typically required to process voice data, speech performance may not be optimum. For example, there may be delays associated with the transfer of such voice data due to the amount of time needed to process the voice data. Also, if certain types of CODECs that have less resource requirements are selected, voice quality may suffer.

[0007] Also, the computer system needs to be fitted with speakers, microphones, and sound cards to enable speech processing. Further, such speakers, microphones, and sound cards may not provide the desired level of quality, or if they do, may be relatively expensive. Additionally, to add such speech processing components to a computer system may require some configuration to be performed by a user, a process that an unsophisticated user may have difficulty with.

[0008] Unless a computer system with powerful processing capabilities are provided, the voice quality provided by such computer systems are not at the level typically experienced (and expected) by users of standard telephones. Such "standard" telephones may include analog telephones coupled to a local or central switching office or digital telephones coupled to a private branch exchange (PBX) system. More recently, network telephones have been developed, for example, as disclosed in Boullet M "Voice over IP in Alcatel Omni PCX 4400 and OmniOffice", Alcatel Telecommunications Review, 1 January 2000, pages 7-11, that are capable of being connected directly to a data network, such as an IP network. These network telephones are capable of placing telephony calls over a data network. The voice quality offered by such telephones are typically superior to those that can be offered by computer systems, since such network telephones typically include dedicated digital signal processors (DSPs) that perform the data intensive calculations involved in speech processing. However, the existing network telephones do not provide desired multimedia presentation capabilities such as those offered by displays of computer systems. Thus, while network telephones offer superior speech capabilities, it does have the desired multimedia capabilities. On the other hand, computer systems have superior multimedia capabilities, but they suffer from relatively poor speech processing performance.

[0009] Catchpole A el at "Introduction to computer telephony integration", British Telecommunications Engineering, Vol. 14, No. 2, 1 July 1995, pages 98-105, discloses a method of communicating over a packet-switched data network according to the pre-characterizing portion of claim 1.

[0010] A need remains for an improved method and apparatus for controlling voice communications over data networks.

Summary

[0011] The present invention provides a method of communicating over a packet-switched data network characterized according to claim 1.

[0012] In general, according to one embodiment, a method of communicating over a data network includes communicating, in a control system, one or more control messages over the data network to establish a call session with a remote device coupled to the data network. One or more commands are transmitted to a voice device coupled to the data network. The call session between the voice device and the remote device is established over the data network. Information associated with the call session is displayed on the control system

[0013] In general, according to another embodiment, a method of communicating over a data network includes providing a user interface in a control system for establishing call sessions. One or more control messages are communicated by the control system over the data network to establish a call session with a remote device in response to receipt of a request through the user interface. One or more commands are transmitted to a voice device associated with a control system to establish the call session between the voice device and the remote device over the data network.

[0014] Some embodiments of the invention may include one or more of the following advantages. The voice processing capabilities of a voice device, such as a network telephone, may be advantageously used to provide superior voice quality, while at the same time, a control system such as a computer may be used to provide a convenient user interface for the user to perform call control and to view status and other information relating to the call session. Thus, voice quality associated with call sessions over data networks such as packet-switched data networks is enhanced using embodiments of the invention.

[0015] Other features and advantages will become apparent from the following description, from the drawings, and from the claims.

Brief Description Of The Drawings

[0016]

Fig. 1 is block diagram of an embodiment of a communications system.

Fig. 2 illustrates components in a network telephone and a call control system in accordance with an embodiment.

Fig. 3 illustrates control and data paths between network elements used during a call session in accordance with one embodiment.

Figs. 4 and 5 illustrate example screens displayed by the call control system of Fig. 2 in accordance with an embodiment.

Fig. 6 is a message flow diagram of messages exchanged between network elements in the communications system of Fig. 1 for placing an outgoing call.

Detailed Description

[0017] In the following description, numerous details are set forth to provide an understanding of the present invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these details and that numerous variations or modifications from the described embodiments may be possible. For example, although reference is made to Session Initiation Protocol (SIP) communications sessions in accordance with some embodiments, other protocols may be performed in further embodiments.

[0018] Referring to Fig. 1, a communications system 10 includes a first data network 12 and a second data network 14 that are coupled through a data network cloud 16. The data network cloud 16 may include various links, communications paths, and routers for routing messages between data networks 12 and 14. The data network cloud 16 may include a public network such as the Internet. The data networks 12 and 14 may be private networks such as local area networks (LANs) or wide area networks (WANs). In the ensuing discussion, one or some combination of the data networks 12 and 14 and data network cloud 16 may be referred to collectively as the data network 11. As used here, a "data network" or "network" may refer to one or more communications networks, channels, links, or paths and systems (such as routers) used to route data over such networks, channels, links, or paths.

[0019] The data network 11 may include an Internet Protocol (IP) network, which is a packet-switched network. One version of IP is described in Request for Comments (RFC) 791, entitled "Internet Protocol," dated September 1981. Other versions of IP, such as IPv6, or other connectionless, packet-switched standards may also be utilized in further embodiments. A version of IPv6 is described in RFC 2460, entitled "Internet Protocol, Version 6 (IPv6) Specification," dated December 1998. Packet-switched data networks such as IP networks communicate with packets, datagrams or other units of data over the data networks. Unlike circuit-switched networks, which provide a dedicated end-to-end connection or physical path for the duration of a call session, a packet-switched network is one in which the same path may be shared by several network elements. Packet-switched networks such as IP networks are based on a connectionless internetwork layer. Packets or other units of data injected into a packet-switched data network may travel independently over any path (and possibly over different paths) to a destination point. The packets may even arrive out of order. Routing of the packets is based on one or more addresses carried in each packet.

[0020] The packet-based network 12 may also be connection-oriented, such as an ATM (Asynchronous Transfer Mode) network or a Frame Relay network. In a con-

nection-oriented, packet-based network, a virtual circuit or connection is established between two end points. In such connection-oriented networks, packets are received in the same order in which they were transmitted.

[0021] Network elements connected to the data network 11 may also be coupled through a data network-PSTN gateway 20 to a public-switched telephone network (PSTN) 22. The link between the gateway 20 and the PSTN 22 may be a primary rate interface (PRI) link according to ISDN (Integrated Services Digital Network). Standard non-data network telephones 24 may be coupled to the PSTN 22. Call sessions can thus be established between a data network element and one of telephones 84.

[0022] In the example embodiment as illustrated in Fig. 1, audio (e.g., voice) and multimedia (e.g., audio and video) communications may occur over the data network 11 between or among various network elements, including network telephones 30 and 34 and call control systems 32 and 36. Other devices capable of voice or multimedia sessions include SIP (Session Initiation Protocol) client systems 38 and 40. The SIP client systems 38 and 40 are capable of communicating using SIP messaging to establish call sessions. As used here, a "call session" refers generally to either a voice or a multimedia session established between two or more elements coupled to the data network 11 (or any other packet-switched data network). SIP is part of the multimedia data and control architecture from the Internet Engineering Task Force (IETF). A version of SIP is described in RFC 2543, entitled "SIP: Session Initiation Protocol," dated August 1999. SIP may be used to initiate call sessions as well as to invite members to a session that may have been advertised by some other mechanism, such as electronic mail, news groups, web pages, and other mechanisms. The other protocols in the IETF multimedia and control architecture include the Resource Reservation Protocol (RSVP), as described in RFC 2205; the Real-Time Transport Protocol (RTP), as described in RFC 1889; the Real-Time Streaming Protocol (RTSP), as described in RFC 2326; the Session Description Protocol (SDP), as described in RFC 2327; and the Session Announcement Protocol (SAP).

[0023] Other standards may be employed in further embodiments for controlling call sessions over the data network 11. Such other standards may be any other standard that provides for interactive, real-time voice communications over the data network.

[0024] The SIP client systems 38 and 40 as shown in Fig. 1 include client application programs that are capable of sending SIP requests to perform call requests. The systems 38 and 40 may also be SIP servers. A server according to SIP may be an application program that accepts SIP requests to service calls and to send back responses to SIP requests. Thus, a system can be either a SIP client or a SIP server. A SIP proxy system, such as system 42, may include an intermediary program that acts as both a server and a client for making requests on behalf of other clients.

[0025] In the system 10 as shown in Fig. 1, the call control systems 32 and 36 are SIP-enabled; that is, the call control systems 32 and 36 are capable of sending and accepting SIP requests to establish call sessions. The call control systems 32 and 36 may be implemented on a standard computer system platform. Unlike the call control systems 32 and 36, however, the network telephones 30 and 34 are not SIP-enabled in one embodiment. Although they are capable of communicating audio data over the data network 11, the network telephones 30 and 34 are not enabled to send or accept SIP messages (or other types of messages for establishing interactive, real-time voice communications) to establish call sessions. In accordance with some embodiments, the establishment, management, and termination of call sessions are controlled by the call control systems 32 and 36. Thus, the call control system 32 makes SIP requests on behalf of the network telephone 30, while the call control system 36 makes SIP requests on behalf of the network telephone 34. Once a call session is established, the network telephone 30 or 34 participates in the communication of voice data over the network 11.

[0026] By employing the arrangement as shown in Fig. 1, the superior voice capabilities of network telephones 30 and 34 may be utilized to provide enhanced voice quality for users making telephony calls over the data network 11. At the same time, associated call control systems 32 and 36 are used to provide call signaling communications and to provide the user with a convenient user interface to perform call control as well as display information associated with the call session.

[0027] The call control system 32 and the network telephone 30 may be collectively referred to as a telephony system 31. Similarly, the call control system 36 and network telephone 34 may be collectively referred to as a telephony system 33. To establish a call session between the telephony system 31 or 33 and another SIP-enabled remote system 100, as shown in Fig. 3, the call control system 32 or 36 sends SIP messages to the remote system 100 to establish a call session. The remote system 100 may be any system or device on the data network 11 that is capable of participating in a SIP-established call session. The call control system 32 or 36 also exchanges commands according to a predetermined format with the network telephone 30 or 34 to let the network telephone 30 or 34 know of the current status of the call setup. Once a call is established, a link may be established between the network telephone 30 or 34 and the remote system 100 over the data network 11. The link may be a Real-Time Protocol (RTP) link to communicate with voice data. Thus, in the telephony system 31 or 33, the call control system 32 or 36 communicates the control signaling to establish a call session, while a real-time link is established directly between the network telephone 30 or 34 and the remote system 100 for communicating voice or other types of audio data. In one embodiment, the call control messaging between the call control sys-

tem and remote system, the control messaging between the call control system and the network telephone, and the call session between the network telephone and the remote system all occur over the data network 11.

[0028] The call control system 32 or 36 is also equipped with speech processing elements to allow it to communicate voice data with other devices on the data network 11. Thus, a user at the call control system 32 or 36 may select whether to use the call control system or the network telephone as the terminal device in the established call session. In addition, if the call control system 32 or 36 is powered off, the network telephone 30 or 34 may be used as a stand-alone device to communicate voice in call sessions over the data network 11.

[0029] Referring to Fig. 2, the components in the network telephone 30 or 34 and in the call control system 32 or 36 are illustrated in greater detail. The network telephone 30 or 34 includes a network interface 102 that is coupled to the data network 11. Above the network interface 102 are several software layers, including a device driver layer 104, a TCP/IP or UDP/IP stack 106, and an RTP layer 108. TCP is described in RFC 793, entitled "Transmission Control Protocol," dated September 1981; and UDP is described in RFC 768, entitled "User Datagram Protocol," dated August 1980. TCP and UDP are transport layers for managing connections between network elements over an IP network. Packets received by the network interface 102 are passed up through the several layers 104, 106 and 108. Control packets are transmitted by the TCP/IP or UDP/IP stack 106 to one or more control tasks 110 in the network telephone 30 or 34. The one or more control tasks 110 may be implemented as software routines executable on a control unit 112. Instructions and data associated with the control tasks 110 may be stored in a storage device 114. The control tasks 110 are responsible for generation of control signaling as well as exchanging commands and responses with its associated call control system 32 or 36 over the data network 11.

[0030] Voice data may be passed through the RTP layer 108 to a speech processing application 116, which may also be executable on the control unit 112. For faster processing of voice data, a digital signal processor (DSP) 118 is included in the network telephone 30 or 34 to provide data intensive signal processing tasks. For example, the coder/encoder (CODEC) may be implemented in the DSP 118. The network telephone may also include a display screen to display text data associated with a call session. The size of the display screen 120 may be limited so that only limited amounts of text data may be displayed in the display screen 120. The network telephone also includes numerals buttons that may be controlled by button control circuitry 122. The buttons may include numeric buttons, speed dial buttons, a transfer button, a hold button, a redial button, and other telephony buttons. Activation of any one of the buttons may cause generation of some type of an indication (such as an interrupt) that is forwarded to the control tasks 110.

[0031] The call control system 32 or 36 also includes a network interface 150. Above the network interface 150 are several layers, including a device driver layer 152, a TCP/IP or UDP/IP stack 154, a SIP stack 156, and an RTP layer 158. The SIP stack 156 is responsible for processing or generating SIP requests and responses communicated over the data network 11. The SIP stack 156 is in communication with one or more control tasks 160 in the call control system 32 or 36. The SIP stack 156 is generally a state machine that provides parsing, processing, and generation of SIP requests and responses.

[0032] The call control tasks 160 are responsible for generating control signaling to establish call sessions over the data network 11 as well as to respond to received control signaling. In addition, the control tasks 160 are responsible for exchanging commands and responses with the network telephone 30 or 34 to establish such call sessions. The call control system 32 or 36 may also include one or more graphical user interface (GUI) routines 162 that control the presentation of information (text or graphical) on a display 164 of the call control system. Further, the user interface provided by the GUI routines 162 may include selectors for call control and indicators of the status of a call session.

[0033] In the illustrated arrangement, the RTP layer 158 sends audio data to, or receives audio data from, a CODEC 166. The CODEC 166 encodes or decodes voice data. A speech processing routine 168 may perform further processing of voice data. In further embodiments, the audio CODEC 166 and the speech processing routine 118 may be omitted. The various software routines in the call control system 32 or 36, including the various layers 152, 154, 156, and 158 as well as the control tasks 160, CODECs 166, speech processing routine 168, and GUI routine 162, are executable on a control unit 170. The control unit 170 is coupled to a storage device 172 in which instructions and data associated with the various software routines may be stored.

[0034] In the illustrated example arrangement, to provide a voice or audio user interface to a user sitting at the call control system 32 or 36, a peripheral controller 174 is coupled to a microphone 176 and a speaker or head phone 178 through which a user can talk or listen during a call session. If the call control system 32 or 36 is not speech-enabled, the microphone 176 and speaker or head phone 178 may be omitted.

[0035] One call control system 32 or 36 may be associated with a corresponding network telephone 30 or 34. Thus, the network telephone 30 or 34 can identify which device is its controller. Similarly, a call control system 32 or 36 can identify the network telephone it is controlling. The network telephone 30 or 34 includes one or more fields 120 in the storage device 114 to store an identifier of its call controller, in this case the call control system 32 or 36. The identifier may be in the form of a network address and port number. For example, an IP address and a TCP or UDP port may form part of the identifier of

the call controller 120. Similarly, the call control system 32 or 36 stores one or more fields 180 in the storage device 172 that stores the identifier of the network telephone it is controlling. Again, the identifier 180 may be in the form of a network address and port number, such as an IP address and a TCP or UDP port number. The identifier stored in the field 120 of the network telephone may be changed by a user to change the associated call control system. Similarly, the identifier stored in the field 180 of the call control system may be modified to change the controlled network telephone.

[0036] In further embodiments, one call control system may be associated with plural network telephones. Also, a single network telephone may be associated with plural call control systems.

[0037] The various control units in the network telephone 30 or 34, the call control 32 or 36, and any other system or device on the data network 11 may each include a microprocessor, a microcontroller, a processor card (including one or more microprocessors or controllers), or other control or computing devices. The storage devices referred to in this discussion may include one or more machine-readable storage media for storing data and instructions. The storage media may include different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; and optical media such as compact disks (CDs) or digital video disks (DVDs). Instructions that make up the various software routines, modules, or layers in the various network elements may be stored in respective storage devices. The instructions when executed by a respective control unit cause the corresponding network element to perform programmed acts.

[0038] The instructions of the software routines, modules or layers may be loaded or transported to the network element in one of many different ways. For example, code segments including instructions stored on floppy disks, CD or DVD media, a hard disk, or transported through a network interface card, modem, or other interface device may be loaded into the system and executed as corresponding software routines, modules, or layers. In the loading or transport process, data signals that are embodied in carrier waves (transmitted over telephone lines, network lines, wireless links, cables, and the like) may communicate the code segments, including instructions, to the network element. Such carrier waves may be in the form of electrical, optical, acoustical, electromagnetic, or other types of signals.

[0039] Referring to Fig. 4, in accordance with one embodiment, a screen 200 that may be provided by the control tasks 160 and graphical user interface routines 162 in the call control system 32 or 36 is illustrated. The screen 200 as shown in Fig. 4 includes various icons and items (generally referred to as indicators) to allow a user sitting at the call control system to initiate, terminate, and screen calls over the data network 11. In the example shown in Fig. 4, the screen 200 includes a menu 202, a series of control buttons 204, and a list 206 of potential callees. The list 206 provides the first and last names of potential callees as well associated electronic mail addresses (or other information such as telephone numbers and so forth). As illustrated in Fig. 4, the name R. Smith may be highlighted in the list 206. The address of R. Smith is displayed in an address field 208. The address field 208 may include various formats, such as a PSTN number (e.g., 972-555-1234); a PSTN number and a proxy address (e.g., 972-555-1234 @ CTEXI300); an IP address (e.g., 47.161.18.72); a SIP address (e.g., rsmith@nortelnetworks.com); or a SIP address at a specific IP address (e.g., rsmith@47.161.18.72). Identifiers according to other formats may be illustrated in the address field 208 in further embodiments.

[0040] A status field 212 may also be included in the screen 200, which may show the status as "not in call," "outgoing call to R. Smith," "incoming call from R. Smith," and so forth. A plurality of indicators 214 may also be provided in the screen 200. A C indicator flashes when an incoming call has been missed. An S indicator gives an indication that call screening is active. A P indicator gives an indication that a SIP proxy is in use or not in use. An E indicator gives an indication of the state of the associated network telephone. Thus, the E indicator is at a first state if the network telephone is not active and at a second state if the network telephone is active and available. The E indicator may also be at a third state to indicate that a call is currently in progress.

[0041] The screen 200 is also capable of providing a pop-up menu 210 to allow a user to select one or several methods of contacting the desired callee. For example, a first option in the pop-up menu 210 is to call R. Smith. Another option is to send an electronic mail to R. Smith. A third option is to go to R. Smith's web site.

[0042] Other call control operations that may be performed by a user through the screen 200 includes volume control, screening of incoming calls, termination of a call session, and other operations.

[0043] Referring to Fig. 5, once a call is established with either a caller or a callee, another screen 300 may be shown. A picture of the caller or callee may be displayed in the screen 300. An icon 304 may be provided to allow the user to hang-up the call, and another icon 306 may be provided to allow the call to be placed on hold. A status field 308 indicates the current status of the call.

[0044] Referring to Fig. 6, an outgoing call message flow is illustrated. In the illustrated example, the user can initiate the call from the call control system. However, the user can also make the external call from the network telephone by entering the desired number in appropriate buttons of the network telephone. In that case, messages are exchanged between the network telephone and the

call control system initially to indicate to the call control system that the user has started a phone call from the network telephone.

[0045] To start the call session, the call control system sends (at 502) an Invite request to the remote system. The remote system then sends back (at 504) a Ringing response. In response, the call control system sends (at 506) a Remote_Alerting message to the network telephone indicating that the call has been placed. The network telephone then returns (at 508) an Ack_Alerting message. At some point, the remote system, once it has answered the call, issues (at 510) a 200 OK message to the call control system. In response, the call control system then sends (at 512) an Ack request back to the remote system. The call control system also sends (at 514) a Remote_Answer message to the network telephone, which returns (at 516) an Ack_Answer message to the call control system. At that point, a voice path (e.g., an RTP path) is established (at 518) between the network telephone and the remote system over the data network 11.

[0046] To terminate the call, the remote system may issue (at 520) a Bye request. In response, the call control system may terminate the call by sending (at 522) a 200 OK message. The call control system then sends (at 524) a Disconnect_Req message to the network telephone, which returns (at 526) an Ack_Disconnect message to the call control system. At this point, the RTP voice path is terminated.

Claims

1. A method of communicating over a packet-switched data network (11), comprising:

   providing a user interface (162,164) in a computer system (32,36), which is adapted to establish call sessions on behalf of a packet-switched data network telephone (30,34); and

   communicating (502,504), between the computer system and a remote device, one or more request and response control messages according to a protocol defining real-time interactive call sessions over the data network to establish a call session for communicating audio data between the network telephone and the remote device in response to receipt of a request through the user interface; **characterised in that** this call session is established by

   transmitting (506) one or more commands comprising at least a ring command to activate a ringer of the network telephone and a command to open or connect an audio stream to the network telephone directly connected to the data network and associated, by storing in the computer system an identifier of the network telephone, with the computer system;

   establishing (518) a voice path between the network telephone and the remote device over the data network.

2. The method of claim 1, wherein the communicated one or more control messages and the transmitted one or more commands are according to different formats.

3. The method of claim 1, wherein communicating the one or more control messages includes communicating one or more Session Initiation Protocol messages.

4. The method of claim 3, wherein storing the identifier includes storing an Internet Protocol address and a port of the network telephone.

5. The method of claim 1, further comprising receiving an indication from the network telephone to establish another call session with the remote device.

6. The method of claim 1, further comprising displaying graphical user interface information (300) of the call session on the computer system.

7. The method of claim 1, further comprising terminating the call session using either the user interface or the network telephone.

8. A computer system (32,36) for controlling a packet-switched data network telephone (30,34) connected to a packet-switched data network (11), comprising:

   a user interface (162,164) including one or more selectors for call control relating to call sessions to be established on behalf of the network telephone;

   a controller (170) adapted to receive a request from the user interface in response to which a call session for communicating audio data between the network telephone and a remote device over the data network is established, whereby one or more request and response control messages according to a protocol defining real-time interactive call sessions for communication over the data network are communicated between the computer system and the remote device; and

   an interface (150) adapted to transmit one or more commands to the network telephone comprising at least a ring command to activate a ringer of the network telephone and a command to open or connect an audio stream to the network telephone, and to establish a voice path between the network telephone and the remote device;

   whereby the network telephone is directly con-

nected to the data network; and associated with the computer system by an identifier (180) of the network telephone which is stored in the controller.

9. The system of claim 8, wherein the one or more messages include Session Initiation Protocol messages.

10. The system of claim 9, further comprising a module (156) to process the one or more Session Initiation Protocol messages.

11. The system of claim 8, wherein the interface includes a network interface (150) for coupling to the data network.

12. The system of claim 8, further comprising a storage element (172) including an identifier of the network telephone.

13. The system of claim 8, wherein the user interface includes one or more elements (300) to display information relating to the call session.

14. The system of claim 13, wherein the information includes graphical information.

15. A computer program product comprising
at least one storage medium having thereon computer program code means to make a computer system (32, 36) execute a method for controlling a call session over a packet-switched data network (11), the method comprising:

providing a user interface (162, 164) in the computer system, which is adapted to establish the call session on behalf of a packet-switched data network telephone (30, 34); and
communicating (502, 504), between the computer system and a remote device, one or more request and response control messages according to a protocol defining real-time interactive call sessions over the data network to establish the call session for communicating audio data between the network telephone and the remote device in response to a request received through the user interface; **characterised in that** this call session is established by
transmitting (506) one or more commands comprising at least a ring command to activate a ringer of the network telephone and a command to open or connect an audio stream to the network telephone, directly connected to the data network and associated, by storing in the computer system an identifier of the network telephone, with the computer system;
establishing (518) a voice path between the network telephone and the remote device over the data network.

Patentansprüche

1. Verfahren zur Übermittlung über ein paketvermitteltes Datennetz (11), das Folgendes umfasst:

Bereitstellen einer Benutzerschnittstelle (162, 164) in einem Computersystem (32, 36), die dafür ausgelegt ist, Anrufsitzungen im Namen eines paketvermittelten Datennetzwerktelefons (30, 34) herzustellen und
Übermitteln (502, 504) zwischen dem Computersystem und einem entfernten Gerät einer oder mehrerer Anfrage- und Antwortsteuernachrichten gemäß einem Protokoll, das interaktive Echtzeit-Anrufsitzungen über das Datennetzwerk definiert, um eine Anrufsitzung für die Übermittlung von Audiodaten zwischen dem Netzwerktelefon und der entfernten Vorrichtung als Reaktion auf den Empfang einer Anforderung durch die Benutzerschnittstelle herzustellen; **dadurch gekennzeichnet, dass** diese Anrufsitzung durch Folgendes hergestellt wird:

Übertragen (506) eines oder mehrerer Befehle, die mindestens einen Ruftonbefehl umfassen, um einen Ruftonerzeuger des Netzwerktelefons und einen Befehl zum Öffnen oder Verbinden eines Audiostroms mit dem Netzwerktelefon zu aktivieren, das direkt mit dem Datennetzwerk verbunden ist und dem Computersystem zugeordnet ist, indem in dem Computersystem eine Kennung des Netzwerktelefons gespeichert wird;
Herstellen (518) eines Sprachpfads zwischen dem Netzwerktelefon und dem entfernten Gerät über das Datennetzwerk.

2. Verfahren nach Anspruch 1, wobei die eine oder die mehreren übermittelten Steuernachrichten und der eine oder die mehreren übermittelten Befehle verschiedenen Formaten entsprechen.

3. Verfahren nach Anspruch 1, wobei die Übermittlung der einen oder der mehreren Steuernachrichten die Übermittlung einer oder mehrerer Sitzungsinitiierungsprotokollnachrichten umfasst.

4. Verfahren nach Anspruch 3, wobei das Speichern der Kennung das Speichern einer Internetprotokoll-Adresse und eines Ports des Netzwerktelefons umfasst.

5. Verfahren nach Anspruch 1, das ferner den Empfang eines Hinweises von dem Netzwerktelefon umfasst,

eine weitere Anrufsitzung mit dem entfernten Gerät herzustellen.

6. Verfahren nach Anspruch 1, das ferner das Anzeigen von Informationen der graphischen Benutzerschnittstelle (300) der Anrufsitzung auf dem Computersystem umfasst.

7. Verfahren nach Anspruch 1, das ferner die Beendigung der Anrufsitzung entweder über die Benutzerschnittstelle oder das Netzwerktelefon umfasst.

8. Computersystem (32, 36) zur Steuerung eines paketvermittelten Datennetzwerktelefons (30, 34), das mit einem paketvermittelten Datennetzwerk (11) verbunden ist, wobei das Computersystem Folgendes umfasst:

eine Benutzerschnittstelle (162, 164), die einen oder mehrere Selektoren für die Anrufsteuerung im Zusammenhang mit Anrufsitzungen umfasst, die im Auftrag des Netzwerktelefons herzustellen sind;
eine Steuerung (170), die dafür ausgelegt ist, eine Anforderung von der Benutzerschnittstelle zu empfangen, wobei als Reaktion darauf eine Anrufsitzung für die Übermittlung von Audiodaten zwischen dem Netzwerktelefon und einer entfernten Vorrichtung über das Datennetzwerk hergestellt wird, wodurch eine oder mehrere Anfrage- und Antwortsteuernachrichten gemäß einem Protokoll, das interaktive Echtzeit-Anrufsitzungen für die Übermittlung über das Datennetzwerk definiert, zwischen dem Computersystem und der entfernten Vorrichtung übermittelt werden, und
eine Schnittstelle (150), die dafür ausgelegt ist, einen oder mehrere Befehle zu dem Netzwerktelefon zu übertragen, das mindestens einen Ruftonbefehl umfasst, um einen Ruftonerzeuger des Netzwerktelefons und einen Befehl zum Öffnen oder Verbinden eines Audiostroms mit dem Netzwerktelefon zu aktivieren und einen Sprachpfad zwischen dem Netzwerktlefon und der entfernten Vorrichtung herzustellen;
wodurch das Netzwerktelefon direkt mit dem Datennetzwerk verbunden ist und dem Computersystem durch eine Kennung (180) des Netzwerktelefons, die in der Steuerung gespeichert ist, zugeordnet ist.

9. System nach Anspruch 8, wobei die eine oder die mehreren Nachrichten Sitzungsinitiierungsprotokollnachrichten umfassen.

10. System nach Anspruch 9, das ferner ein Modul (156) zur Verarbeitung der einen oder der mehreren Sitzungsinitiierungsprotokollnachrichten umfasst.

11. System nach Anspruch 8, wobei die Schnittstelle eine Netzwerkschnittstelle (150) zum Verbinden mit dem Datennetzwerk umfasst.

12. System nach Anspruch 8, das ferner ein Speicherelement (172) umfasst, das eine Kennung des Netzwerktelefons aufweist.

13. System nach Anspruch 8, wobei die Benutzerschnittstelle ein oder mehrere Elemente (300) umfasst, um Informationen über die Anrufsitzung anzuzeigen.

14. System nach Anspruch 13, wobei die Informationen grafische Informationen umfassen.

15. Computerprogrammprodukt, das mindestens ein Speichermedium umfasst, auf dem sich Computerprogrammcodemittel befinden, um ein Computersystem (32, 36) zu veranlassen, ein Verfahren zum Steuern einer Anrufsitzung über ein paketvermitteltes Datennetzwerk (11) auszuführen, wobei das Verfahren Folgendes umfasst:

Bereitstellen einer Benutzerschnittstelle (162, 164) in dem Computersystem, die dafür ausgelegt ist, die Anrufsitzung im Namen eines paketvermittelten Datennetzwerktelefons (30, 34) herzustellen und
Übermitteln (502, 504) zwischen dem Computersystem und einem entfernten Gerät einer oder mehrerer Anfrage- und Antwortsteuernachrichten gemäß einem Protokoll, das interaktive Echtzeit-Anrufsitzungen über das Datennetzwerk definiert. um die Anrufsitzung für die Übertragung von Audiodaten zwischen dem Netzwerktelefon und der entfernten Vorrichtung als Reaktion auf den Empfang einer Anforderung durch die Benutzerschnittstelle herzustellen; **dadurch gekennzeichnet, dass** dieser Anrufsitzung durch Folgendes hergestellt wird
Übertragen (506) eines oder mehrerer Befehle, die mindestens einen Ruftonbefehl umfassen, um einen Ruftonerzeuger des Netzwerktelefons und einen Befehl zum Öffnen oder Verbinden eines Audiostroms mit dem Netzwerktelefon zu aktivieren, das direkt mit dem Datennetzwerk verbunden ist und dem Computersystem zugeordnet ist, indem in dem Computersystem eine Kennung des Netzwerktelefons gespeichert wird;
Herstellen (518) eines Sprachpfads zwischen dem Netzwerktelefon und dem entfernten Gerät über das Datennetzwerk.

Revendications

1. Un procédé de communication par l'intermédiaire d'un réseau de données à commutation de paquets (11), comprenant :

   la fourniture d'une interface utilisateur (162, 164) dans un système informatique (32, 36) qui est adaptée de façon à établir des sessions d'appel pour le compte d'un téléphone de réseau de données à commutation de paquets (30, 34), et la communication (502, 504), entre le système informatique et un dispositif distant, d'un ou de plusieurs messages de commande de demande et de réponse selon un protocole définissant des sessions d'appel interactives en temps réel par l'intermédiaire du réseau de données de façon à établir une session d'appel pour la communication de données audio entre le téléphone de réseau et le dispositif distant en réponse à la réception d'une demande par l'intermédiaire de l'interface utilisateur, **caractérisé en ce que** cette session d'appel est établie par
   la transmission (506) d'une ou de plusieurs commandes comprenant au moins une commande de sonnerie destinée à activer un dispositif de sonnerie du téléphone de réseau et une commande destinée à ouvrir ou connecter un flux audio au téléphone de réseau directement raccordé au réseau de données et associé, par la conservation en mémoire dans le système informatique d'un identifiant du téléphone de réseau, au système informatique,
   l'établissement (518) d'un trajet vocal entre le téléphone de réseau et le dispositif distant par l'intermédiaire du réseau de données.

2. Le procédé selon la Revendication 1, où les un ou plusieurs messages de commande communiqués et les une ou plusieurs commandes transmises sont conformes à différents formats.

3. Le procédé selon la Revendication 1, où la communication des un ou plusieurs messages de commande comprend la communication d'un ou de plusieurs messages de protocole d'ouverture de session.

4. Le procédé selon la Revendication 3, où la conservation en mémoire de l'identifiant comprend la conservation en mémoire d'une adresse de protocole Internet et d'un port du téléphone de réseau.

5. Le procédé selon la Revendication 1, comprenant en outre la réception d'une indication provenant du téléphone de réseau de façon à établir une autre session d'appel avec le dispositif distant.

6. Le procédé selon la Revendication 1, comprenant en outre l'affichage d'informations d'interface utilisateur graphique (300) de la session d'appel sur le système informatique.

7. Le procédé selon la Revendication 1, comprenant en outre la terminaison de la session d'appel au moyen de soit l'interface utilisateur ou du téléphone de réseau.

8. Un système informatique (32, 36) destiné à commander un téléphone de réseau de données à commutation de paquets (30, 34) raccordé à un réseau de données à commutation de paquets (11), comprenant :

   une interface utilisateur (162, 164) comprenant un ou plusieurs sélecteurs pour une commande d'appel relative à des sessions d'appel à établir pour le compte du téléphone de réseau,
   un dispositif de commande (170) adapté de façon à recevoir une demande provenant de l'interface utilisateur en réponse à laquelle une session d'appel pour la communication de données audio entre le téléphone de réseau et un dispositif distant par l'intermédiaire du réseau de données est établie, grâce à quoi un ou plusieurs messages de commande de demande et de réponse selon un protocole définissant des sessions d'appel interactives en temps réel pour une communication par l'intermédiaire du réseau de données sont communiqués entre le système informatique et le dispositif distant, et une interface (150) adaptée de façon à transmettre une ou plusieurs commandes au téléphone de réseau comprenant au moins une commande de sonnerie destinée à activer un dispositif de sonnerie du téléphone de réseau et une commande destinée à ouvrir ou connecter un flux audio au téléphone de réseau et de façon à établir un trajet vocal entre le téléphone de réseau et le dispositif distant,
   grâce à quoi le téléphone de réseau est directement raccordé au réseau de données et associé au système informatique par un identifiant (180) du téléphone de réseau qui est conservé en mémoire dans le dispositif de commande.

9. Le système selon la Revendication 8, où les un ou plusieurs messages comprennent des messages de protocole d'ouverture de session.

10. Le système selon la Revendication 9, comprenant en outre un module (156) destiné à traiter les un ou plusieurs messages de protocole d'ouverture de session.

11. Le système selon la Revendication 8, où l'interface comprend une interface de réseau (150) pour un

couplage au réseau de données.

12. Le système selon la Revendication 8, comprenant en outre un élément à mémoire (172) contenant un identifiant du téléphone de réseau.

13. Le système selon la Revendication 8, où l'interface utilisateur comprend un ou plusieurs éléments (300) destinés à afficher des informations relatives à la session d'appel.

14. Le système selon la Revendication 13, où les informations comprennent des informations graphiques.

15. Un produit de programme informatique comprenant au moins un support à mémoire possédant sur celui-ci un moyen de code de programme informatique destiné à amener un système informatique (32, 36) à exécuter un procédé destiné à commander une session d'appel par l'intermédiaire d'un réseau de données à commutation de paquets (11), le procédé comprenant :

la fourniture d'une interface utilisateur (162, 164) dans le système informatique qui est adaptée de façon à établir la session d'appel pour le compte d'un téléphone de réseau de données à commutation de paquets (30, 34), et
la communication (502, 504), entre le système informatique et un dispositif distant, d'un ou de plusieurs messages de commande de demande et de réponse selon un protocole définissant des sessions d'appel interactives en temps réel par l'intermédiaire du réseau de données de façon à établir la session d'appel pour la communication de données audio entre le téléphone de réseau et le dispositif distant en réponse à une demande reçue par l'intermédiaire de l'interface utilisateur, **caractérisé en ce que** cette session d'appel est établie par
la transmission (506) d'une ou de plusieurs commandes comprenant au moins une commande de sonnerie destinée à activer un dispositif de sonnerie du téléphone de réseau et une commande destinée à ouvrir ou connecter un flux audio au téléphone de réseau, directement raccordé au réseau de données et associé, par la conservation en mémoire dans le système informatique d'un identifiant du téléphone de réseau, au système informatique,
l'établissement (518) d'un trajet vocal entre le téléphone de réseau et le dispositif distant par l'intermédiaire du réseau de données.

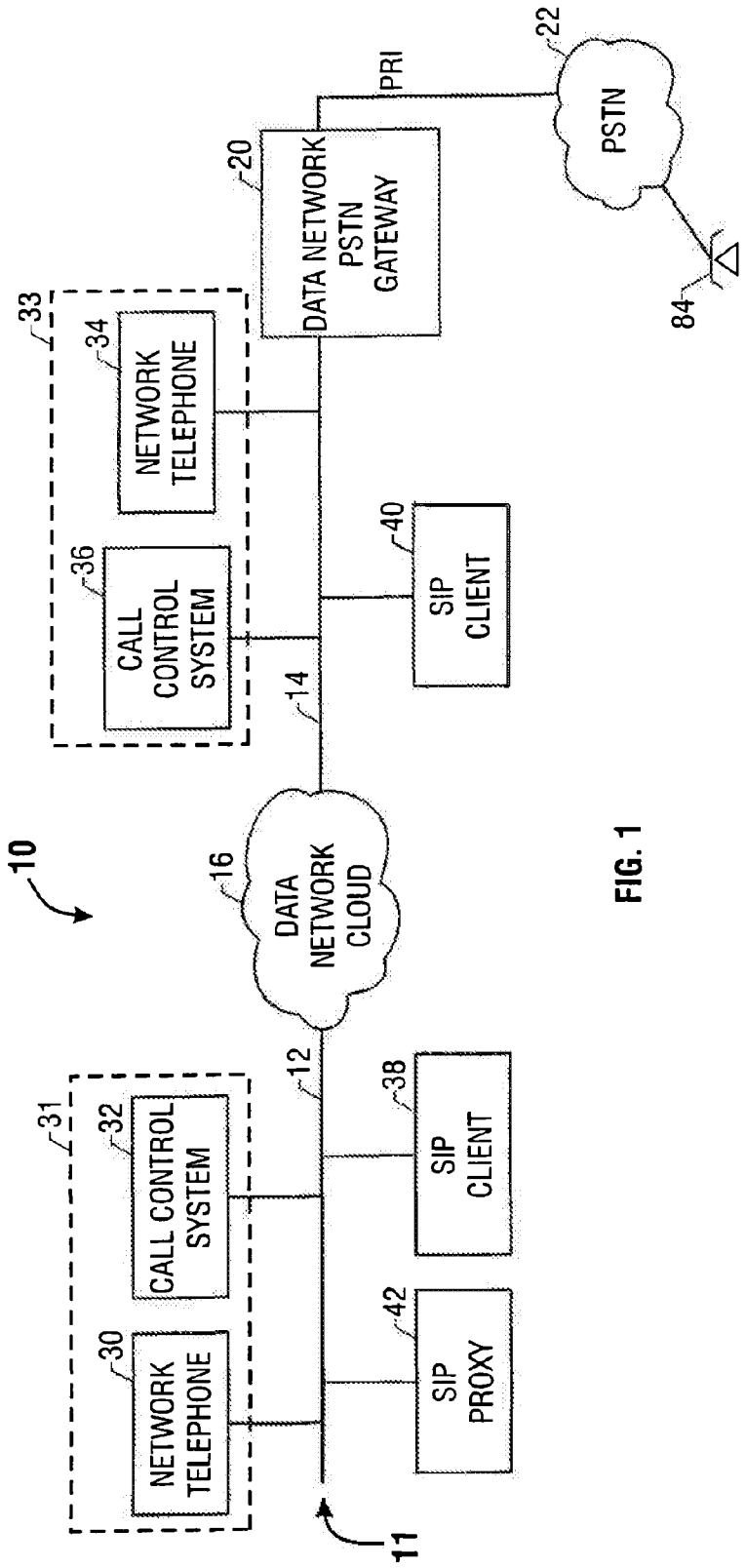


FIG. 1

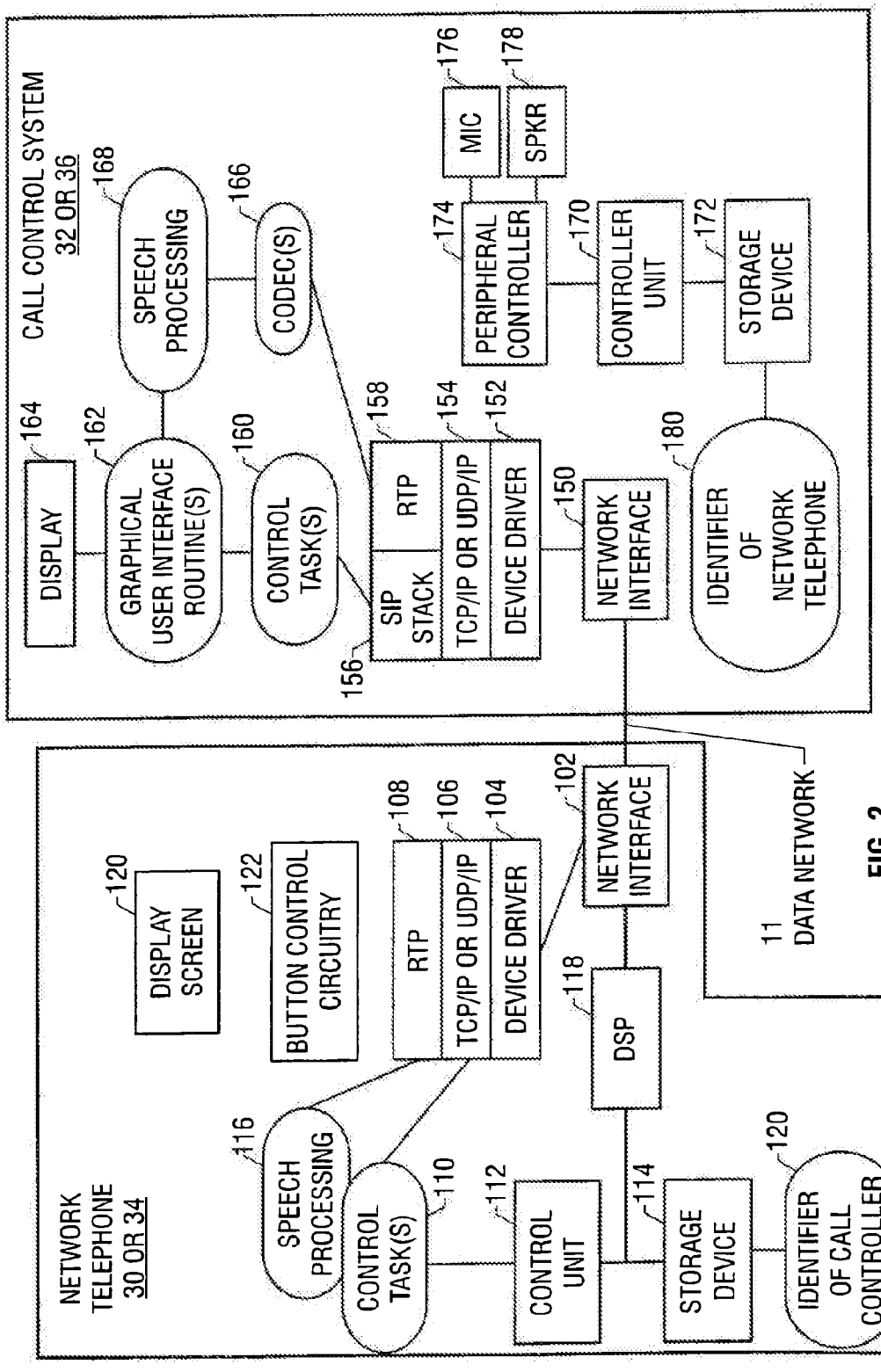


FIG. 2

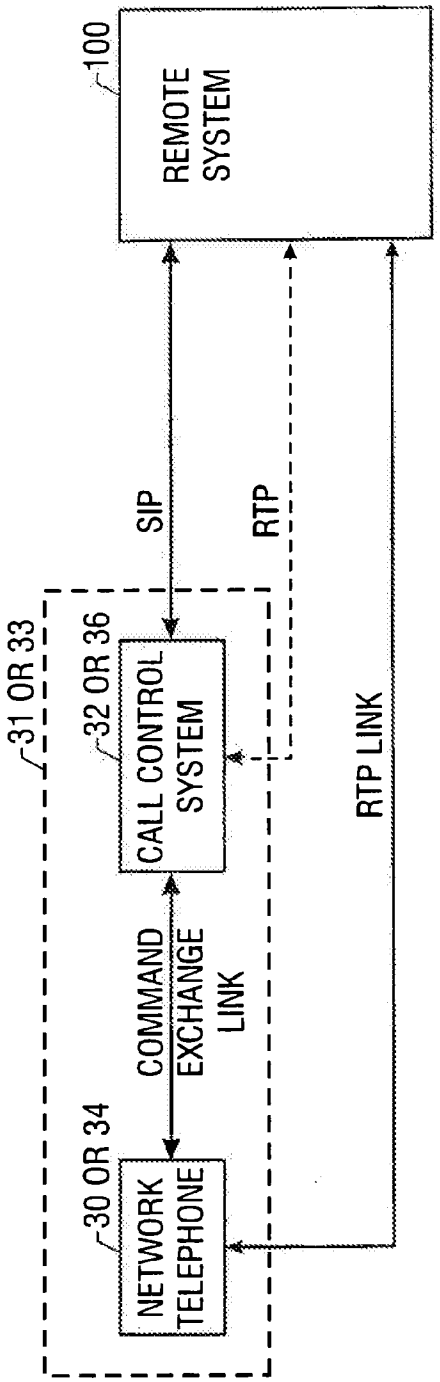


FIG. 3

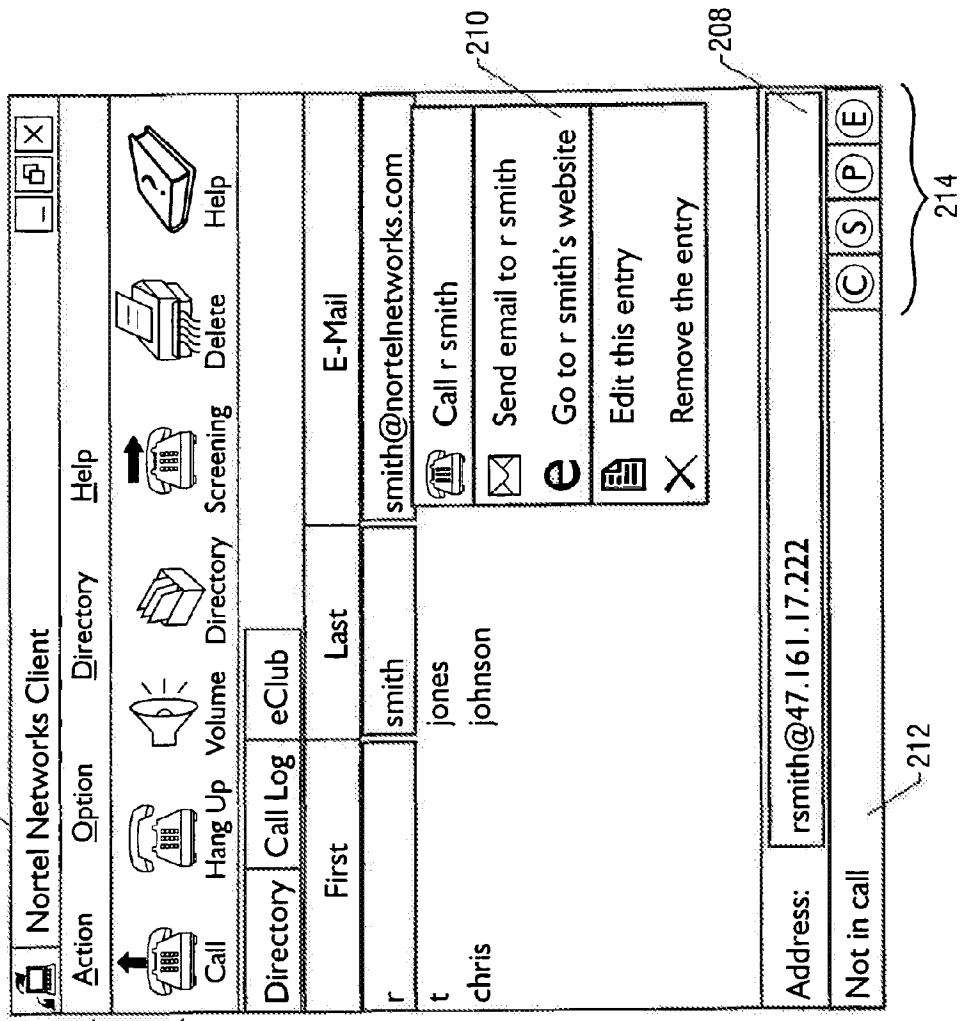


FIG. 4

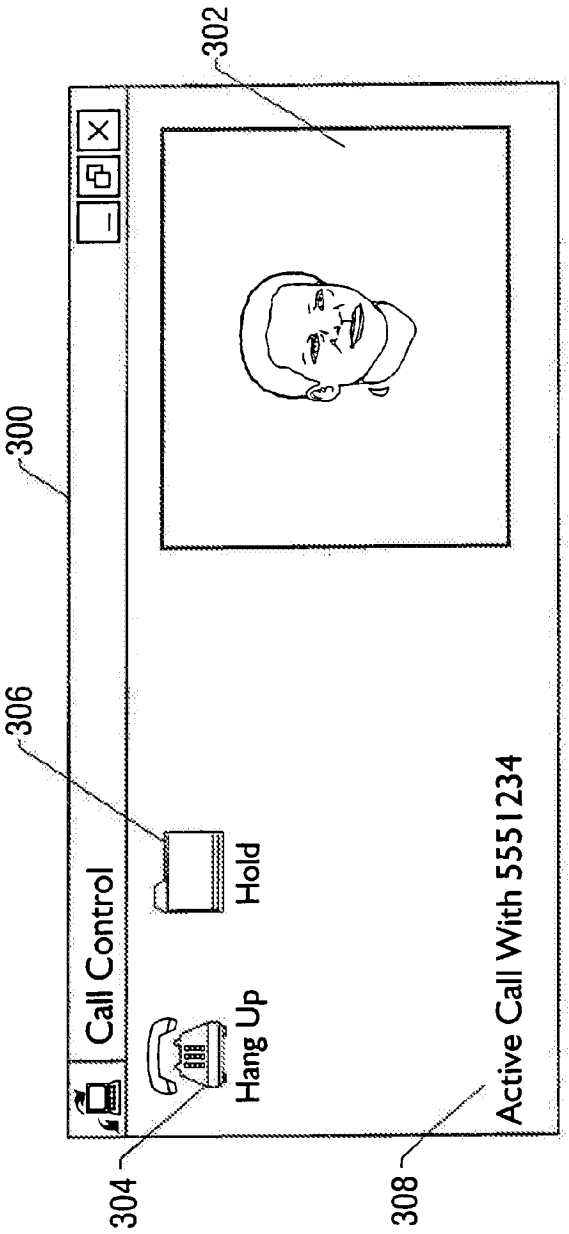


FIG. 5

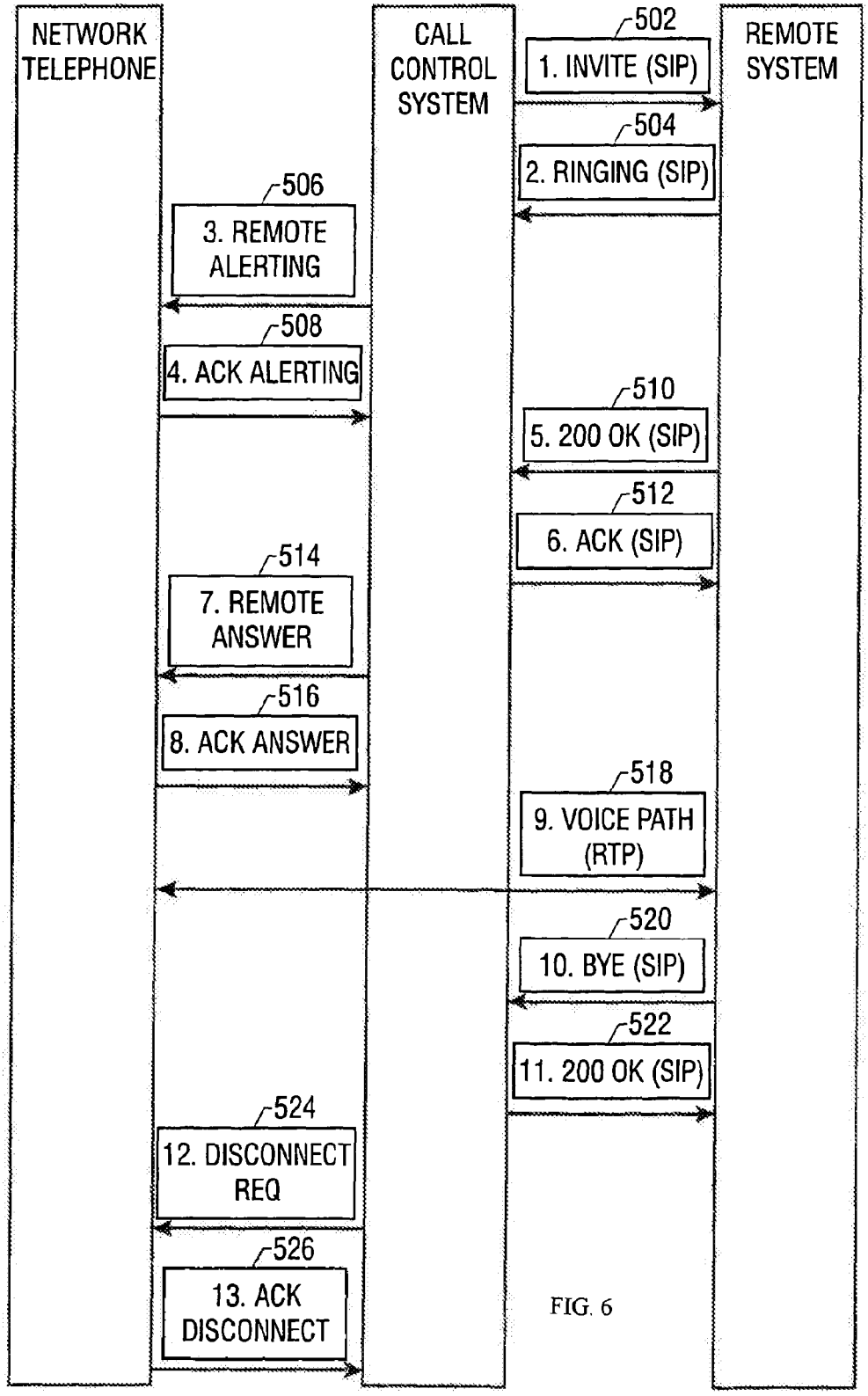


FIG. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **BOULLET.** Voice over IP in Alcatel Omni PCX 4400 and OmniOffice. *Alcatel Telecommunications Review,* 01 January 2000, 7-11 **[0008]**
- **CATCHPOLE A.** Introduction to computer telephony integration. *British Telecommunications Engineering,* 01 July 1995, vol. 14 (2), 98-105 **[0009]**

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69899 A2

(51) International Patent Classification[7]: H04M 3/00

(21) International Application Number: PCT/US01/07686

(22) International Filing Date: 12 March 2001 (12.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/524,342 13 March 2000 (13.03.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/524,342 (CON)
Filed on 13 March 2000 (13.03.2000)

(71) Applicant *(for all designated States except US)*: **NORTEL NETWORKS LTD.** [CA/CA]; World Trade Center of Montreal, 380 St. Antoine Street West, 8th Floor, Montreal, Queéec H2Y 3Y4 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SOLLEE, Patrick, N.** [US/US]; 2708 Garden Springs, Richardson, TX 75082 (US). **CREECH, David, R.** [US/US]; 2526 Fallview Lane, Carrollton, TX 75007 (US). **OSTERHOUT, Gregory, T.** [US/US]; 313 Falcon Court, Coppell, TX 75019 (US). **JESSEN, Christopher, L.** [US/US]; 107 Ledgenest, McKinney, TX 75070 (US).

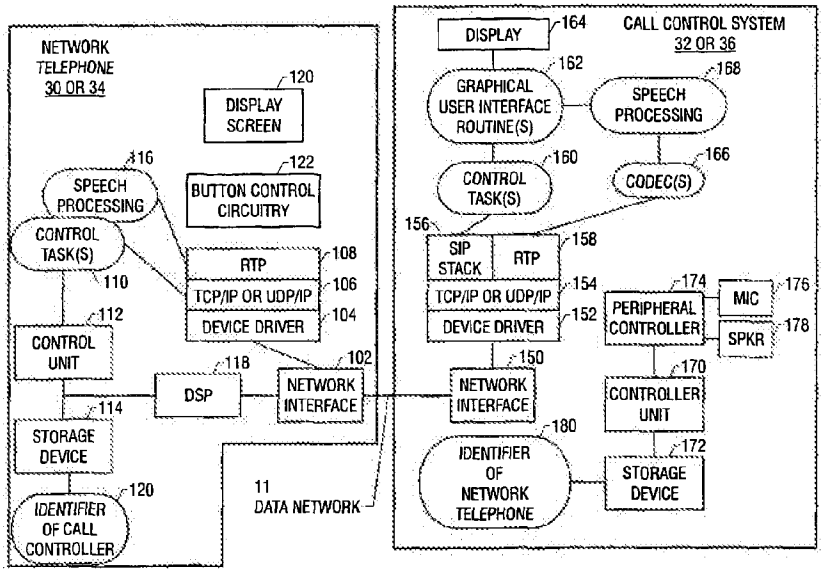
(74) Agent: **HU, Dan, C.**; Trop, Pruner & Hu, P.C., 8554 Katy Freeway, Suite 100, Houston, TX 77024 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, 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, US, 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

[Continued on next page]

(54) Title: CONTROLLING VOICE COMMUNICATIONS OVER A DATA NETWORK



(57) Abstract: A method and apparatus of communicating over a data network (11) includes providing a user interface (200) in a control system (32, 36) for call control and to display information relating to a call session. The control system (32, 36) communicates one or more control messages (e.g., Session Initiation Protocol or SIP messages) over the data network (11) to establish a call session with a remote device in response to receipt of a request through the user interface. One or more commands are transmitted to a voice device (30, 34) associated with the control system (32, 36) to establish the call session between the voice device (30, 34) and the remote device over the data network (11). A Real-Time Protocol (RTP) link may be established between the voice device (30, 34) and the remote device.

WO 01/69899 A2

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).

Declaration under Rule 4.17:

of inventorship (Rule 4.17(iv)) for US only

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.

Controlling Voice Communications Over A Data Network

Background

The invention relates to controlling voice communications over a data network.

Data networks are widely used to link various types of network elements, such as personal computers, servers, gateways, network telephones, and so forth. Data networks may include private networks (such a local area networks or wide area networks) and public networks (such as the Internet). Popular forms of communications between network elements across such data networks include electronic mail, file transfer, web browsing, and other exchanges of digital data.

With the increased capacity and reliability of data networks, voice communications (including telephone calls, video conferencing, and so forth) over data networks have become possible. Voice communications over data networks are unlike voice communications in a conventional public switched telephone network (PSTN), which provides users with dedicated, end-to-end circuit connections for the duration of each call. Communications over data networks, such as IP (Internet Protocol) networks, are performed using packets or datagrams that are sent in bursts from a source to one or more destination nodes. Voice data sent over a data network typically shares network bandwidth with conventional non-voice data (e.g., data associated with electronic mail, file transfer, web access, and other traffic).

Various standards have been proposed for voice and multimedia communications over data networks. One such standard is the H.323 Recommendation from the International Telecommunications Union (ITU), which describes terminals, equipment, and services for multimedia communications over data networks.

Another standard for voice and multimedia communications is the Session Initiation Protocol (SIP), which establishes, maintains, and terminates multimedia sessions over a data network. SIP is part of a multimedia data and control architecture developed by the Internet Engineering Task Force (IETF). The IETF multimedia data and control architecture also includes the Resource Reservation Protocol (RSVP) for reserving network resources; the Real-Time Transport Protocol (RTP) for transporting real-time data and providing quality of service (QoS) feedback; the Real-Time Streaming Protocol (RTSP) for controlling delivery of streaming media; the Session Announcement Protocol (SAP) for advertising multimedia sessions by multicast; and the Session Description Protocol (SDP) for describing multimedia sessions.

To perform voice communications over a data network, a typical computer system (such as a desktop computer system or a portable computer system) may be equipped with voice processing capabilities. Such capabilities include a microphone, ear phones or speakers, and speech processing software. Typically, the speech processing software includes coder/decoders (CODECs) to encode and decode voice data. The voice processing software, including the CODECs, may be run on a microprocessor of a typical computer system. However, due to the intensive data processing typically required to process voice data, speech performance may not be optimum. For example, there may be delays associated with the transfer of such voice data due to the amount of time needed to process the voice data. Also, if certain types of CODECs that have less resource requirements are selected, voice quality may suffer.

Also, the computer system needs to be fitted with speakers, microphones, and sound cards to enable speech processing. Further, such speakers, microphones, and sound cards may not provide the desired level of quality, or if they do, may be relatively expensive. Additionally, to add such speech processing components to a computer system may require some configuration to be performed by a user, a process that an unsophisticated user may have difficulty with.

Unless a computer system with powerful processing capabilities are provided, the voice quality provided by such computer systems are not at the level typically experienced (and expected) by users of standard telephones. Such "standard" telephones may include analog telephones coupled to a local or central switching office or digital telephones coupled to a private branch exchange (PBX) system. More recently, network telephones have been developed that are capable of being connected directly to a data network, such as an IP network. These network telephones are capable of placing telephony calls over a data network. The voice quality offered by such telephones are typically superior to those that can be offered by computer systems, since such network telephones typically include dedicated digital signal processors (DSPs) that perform the data intensive calculations involved in speech processing. However, the existing network telephones do not provide desired multimedia presentation capabilities such as those offered by displays of computer systems. Thus, while network telephones offer superior speech capabilities, it does have the desired multimedia capabilities. On the other hand, computer systems have superior multimedia capabilities, but they suffer from relatively poor speech processing performance.

A need thus exists for an improved method and apparatus for controlling voice communications over data networks.

Summary

In general, according to one embodiment, a method of communicating over a data network includes communicating, in a control system, one or more control messages over the data network to establish a call session with a remote device coupled to the data network. One or more commands are transmitted to a voice device coupled to the data network. The call session between the voice device and the remote device is established over the data network. Information associated with the call session is displayed on the control system.

In general, according to another embodiment, a method of communicating over a data network includes providing a user interface in a control system for establishing call sessions. One or more control messages are communicated by the control system over the data network to establish a call session with a remote device in response to receipt of a request through the user interface. One or more commands are transmitted to a voice device associated with a control system to establish the call session between the voice device and the remote device over the data network.

Some embodiments of the invention may include one or more of the following advantages. The voice processing capabilities of a voice device, such as a network telephone, may be advantageously used to provide superior voice quality, while at the same time, a control system such as a computer may be used to provide a convenient user interface for the user to perform call control and to view status and other information relating to the call session. Thus, voice quality associated with call sessions over data networks such as packet-switched data networks is enhanced using embodiments of the invention.

Other features and advantages will become apparent from the following description, from the drawings, and from the claims.

Brief Description Of The Drawings

Fig. 1 is block diagram of an embodiment of a communications system.

Fig. 2 illustrates components in a network telephone and a call control system in accordance with an embodiment.

Fig. 3 illustrates control and data paths between network elements used during a call session in accordance with one embodiment.

Figs. 4 and 5 illustrate example screens displayed by the call control system of Fig. 2 in accordance with an embodiment.

Fig. 6 is a message flow diagram of messages exchanged between network elements in the communications system of Fig. 1 for processing an incoming call.

Fig. 7 is a message flow diagram of messages exchanged between network elements in the communications system of Fig. 1 for placing an outgoing call.

Detailed Description

In the following description, numerous details are set forth to provide an understanding of the present invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these details and that numerous variations or modifications from the described embodiments may be possible. For example, although reference is made to Session Initiation Protocol (SIP) communications sessions in accordance with some embodiments, other protocols may be performed in further embodiments.

Referring to Fig. 1, a communications system 10 includes a first data network 12 and a second data network 14 that are coupled through a data network cloud 16. The data network cloud 16 may include various links, communications paths, and routers for routing messages between data networks 12 and 14. The data network cloud 16 may include a public network such as the Internet. The data networks 12 and 14 may be private networks such as local area networks (LANs) or wide area networks (WANs). In the ensuing discussion, one or some combination of the data networks 12 and 14 and data network cloud 16 may be referred to collectively as the data network 11. As used here, a "data network" or "network" may refer to one or more communications networks, channels, links, or paths and systems (such as routers) used to route data over such networks, channels, links, or paths.

The data network 11 may include an Internet Protocol (IP) network, which is a packet-switched network. One version of IP is described in Request for Comments (RFC) 791, entitled "Internet Protocol," dated September 1981. Other versions of IP, such as IPv6, or other connectionless, packet-switched standards may also be utilized in further embodiments. A version of IPv6 is described in RFC 2460, entitled "Internet Protocol,

Version 6 (IPv6) Specification," dated December 1998. Packet-switched data networks such as IP networks communicate with packets, datagrams or other units of data over the data networks. Unlike circuit-switched networks, which provide a dedicated end-to-end connection or physical path for the duration of a call session, a packet-switched network is one in which the same path may be shared by several network elements. Packet-switched networks such as IP networks are based on a connectionless internetwork layer. Packets or other units of data injected into a packet-switched data network may travel independently over any path (and possibly over different paths) to a destination point. The packets may even arrive out of order. Routing of the packets is based on one or more addresses carried in each packet.

The packet-based network 12 may also be connection-oriented, such as an ATM (Asynchronous Transfer Mode) network or a Frame Relay network. In a connection-oriented, packet-based network, a virtual circuit or connection is established between two end points. In such connection-oriented networks, packets are received in the same order in which they were transmitted.

Network elements connected to the data network 11 may also be coupled through a data network-PSTN gateway 20 to a public-switched telephone network (PSTN) 22. The link between the gateway 20 and the PSTN 22 may be a primary rate interface (PRI) link according to ISDN (Integrated Services Digital Network). Standard non-data network telephones 24 may be coupled to the PSTN 22. Call sessions can thus be established between a data network element and one of telephones 84.

In the example embodiment as illustrated in Fig. 1, audio (e.g., voice) and multimedia (e.g., audio and video) communications may occur over the data network 11 between or among various network elements, including network telephones 30 and 34 and call control systems 32 and 36. Other devices capable of voice or multimedia sessions include SIP (Session Initiation Protocol) client systems 38 and 40. The SIP client systems 38 and 40 are capable of communicating using SIP messaging to establish call sessions. As used here, a "call session" refers generally to either a voice or a multimedia session established between two or more elements coupled to the data network 11 (or any other packet-switched data network). SIP is part of the multimedia data and control architecture from the Internet Engineering Task Force (IETF). A version of SIP is described in RFC 2543, entitled "SIP: Session Initiation Protocol," dated August 1999. SIP may be used to initiate call sessions as

well as to invite members to a session that may have been advertised by some other mechanism, such as electronic mail, news groups, web pages, and other mechanisms. The other protocols in the IETF multimedia and control architecture include the Resource Reservation Protocol (RSVP), as described in RFC 2205; the Real-Time Transport Protocol (RTP), as described in RFC 1889; the Real-Time Streaming Protocol (RTSP), as described in RFC 2326; the Session Description Protocol (SDP), as described in RFC 2327; and the Session Announcement Protocol (SAP).

Other standards may be employed in further embodiments for controlling call sessions over the data network 11. Such other standards may be any other standard that provides for interactive, real-time voice communications over the data network.

The SIP client systems 38 and 40 as shown in Fig. 1 include client application programs that are capable of sending SIP requests to perform call requests. The systems 38 and 40 may also be SIP servers. A server according to SIP may be an application program that accepts SIP requests to service calls and to send back responses to SIP requests. Thus, a system can be either a SIP client or a SIP server. A SIP proxy system, such as system 42, may include an intermediary program that acts as both a server and a client for making requests on behalf of other clients.

In the system 10 as shown in Fig. 1, the call control systems 32 and 36 are SIP-enabled; that is, the call control systems 32 and 36 are capable of sending and accepting SIP requests to establish call sessions. The call control systems 32 and 36 may be implemented on a standard computer system platform. Unlike the call control systems 32 and 36, however, the network telephones 30 and 34 are not SIP-enabled in one embodiment. Although they are capable of communicating audio data over the data network 11, the network telephones 30 and 34 are not enabled to send or accept SIP messages (or other types of messages for establishing interactive, real-time voice communications) to establish call sessions. In accordance with some embodiments, the establishment, management, and termination of call sessions are controlled by the call control systems 32 and 36. Thus, the call control system 32 makes SIP requests on behalf of the network telephone 30, while the call control system 36 makes SIP requests on behalf of the network telephone 34. Once a call session is established, the network telephone 30 or 34 participates in the communication of voice data over the network 11.

By employing the arrangement as shown in Fig. 1, the superior voice capabilities of network telephones 30 and 34 may be utilized to provide enhanced voice quality for users making telephony calls over the data network 11. At the same time, associated call control systems 32 and 36 are used to provide call signaling communications and to provide the user with a convenient user interface to perform call control as well as display information associated with the call session.

The call control system 32 and the network telephone 30 may be collectively referred to as a telephony system 31. Similarly, the call control system 36 and network telephone 34 may be collectively referred to as a telephony system 33. To establish a call session between the telephony system 31 or 33 and another SIP-enabled remote system 100, as shown in Fig. 3, the call control system 32 or 36 sends SIP messages to the remote system 100 to establish a call session. The remote system 100 may be any system or device on the data network 11 that is capable of participating in a SIP-established call session. The call control system 32 or 36 also exchanges commands according to a predetermined format with the network telephone 30 or 34 to let the network telephone 30 or 34 know of the current status of the call setup. Once a call is established, a link may be established between the network telephone 30 or 34 and the remote system 100 over the data network 11. The link may be a Real-Time Protocol (RTP) link to communicate with voice data. Thus, in the telephony system 31 or 33, the call control system 32 or 36 communicates the control signaling to establish a call session, while a real-time link is established directly between the network telephone 30 or 34 and the remote system 100 for communicating voice or other types of audio data. In one embodiment, the call control messaging between the call control system and remote system, the control messaging between the call control system and the network telephone, and the call session between the network telephone and the remote system all occur over the data network 11.

The call control system 32 or 36 is also equipped with speech processing elements to allow it to communicate voice data with other devices on the data network 11. Thus, a user at the call control system 32 or 36 may select whether to use the call control system or the network telephone as the terminal device in the established call session. In addition, if the call control system 32 or 36 is powered off, the network telephone 30 or 34 may be used as a stand-alone device to communicate voice in call sessions over the data network 11.

Referring to Fig. 2, the components in the network telephone 30 or 34 and in the call control system 32 or 36 are illustrated in greater detail. The network telephone 30 or 34 includes a network interface 102 that is coupled to the data network 11. Above the network interface 102 are several software layers, including a device driver layer 104, a TCP/IP or UDP/IP stack 106, and an RTP layer 108. TCP is described in RFC 793, entitled "Transmission Control Protocol," dated September 1981; and UDP is described in RFC 768, entitled "User Datagram Protocol," dated August 1980. TCP and UDP are transport layers for managing connections between network elements over an IP network. Packets received by the network interface 102 are passed up through the several layers 104, 106 and 108. Control packets are transmitted by the TCP/IP or UDP/IP stack 106 to one or more control tasks 110 in the network telephone 30 or 34. The one or more control tasks 110 may be implemented as software routines executable on a control unit 112. Instructions and data associated with the control tasks 110 may be stored in a storage device 114. The control tasks 110 are responsible for generation of control signaling as well as exchanging commands and responses with its associated call control system 32 or 36 over the data network 11.

Voice data may be passed through the RTP layer 108 to a speech processing application 116, which may also be executable on the control unit 112. For faster processing of voice data, a digital signal processor (DSP) 118 is included in the network telephone 30 or 34 to provide data intensive signal processing tasks. For example, the coder/encoder (CODEC) may be implemented in the DSP 118. The network telephone may also include a display screen to display text data associated with a call session. The size of the display screen 120 may be limited so that only limited amounts of text data may be displayed in the display screen 120. The network telephone also includes numerals buttons that may be controlled by button control circuitry 122. The buttons may include numeric buttons, speed dial buttons, a transfer button, a hold button, a redial button, and other telephony buttons. Activation of any one of the buttons may cause generation of some type of an indication (such as an interrupt) that is forwarded to the control tasks 110.

The call control system 32 or 36 also includes a network interface 150. Above the network interface 150 are several layers, including a device driver layer 152, a TCP/IP or UDP/IP stack 154, a SIP stack 156, and an RTP layer 158. The SIP stack 156 is responsible for processing or generating SIP requests and responses communicated over the data network 11. The SIP stack 156 is in communication with one or more control tasks 160 in the call

control system 32 or 36. The SIP stack 156 is generally a state machine that provides parsing, processing, and generation of SIP requests and responses.

The call control tasks 160 are responsible for generating control signaling to establish call sessions over the data network 11 as well as to respond to received control signaling. In addition, the control tasks 160 are responsible for exchanging commands and responses with the network telephone 30 or 34 to establish such call sessions. The call control system 32 or 36 may also include one or more graphical user interface (GUI) routines 162 that control the presentation of information (text or graphical) on a display 164 of the call control system. Further, the user interface provided by the GUI routines 162 may include selectors for call control and indicators of the status of a call session.

In the illustrated arrangement, the RTP layer 158 sends audio data to, or receives audio data from, a CODEC 166. The CODEC 166 encodes or decodes voice data. A speech processing routine 168 may perform further processing of voice data. In further embodiments, the audio CODEC 166 and the speech processing routine 118 may be omitted. The various software routines in the call control system 32 or 36, including the various layers 152, 154, 156, and 158 as well as the control tasks 160, CODECs 166, speech processing routine 168, and GUI routine 162, are executable on a control unit 170. The control unit 170 is coupled to a storage device 172 in which instructions and data associated with the various software routines may be stored.

In the illustrated example arrangement, to provide a voice or audio user interface to a user sitting at the call control system 32 or 36, a peripheral controller 174 is coupled to a microphone 176 and a speaker or head phone 178 through which a user can talk or listen during a call session. If the call control system 32 or 36 is not speech-enabled, the microphone 176 and speaker or head phone 178 may be omitted.

One call control system 32 or 36 may be associated with a corresponding network telephone 30 or 34. Thus, the network telephone 30 or 34 can identify which device is its controller. Similarly, a call control system 32 or 36 can identify the network telephone it is controlling. The network telephone 30 or 34 includes one or more fields 120 in the storage device 114 to store an identifier of its call controller, in this case the call control system 32 or 36. The identifier may be in the form of a network address and port number. For example, an IP address and a TCP or UDP port may form part of the identifier of the call controller 120. Similarly, the call control system 32 or 36 stores one or more fields 180 in the storage

device 172 that stores the identifier of the network telephone it is controlling. Again, the identifier 180 may be in the form of a network address and port number, such as an IP address and a TCP or UDP port number. The identifier stored in the field 120 of the network telephone may be changed by a user to change the associated call control system. Similarly, the identifier stored in the field 180 of the call control system may be modified to change the controlled network telephone.

In further embodiments, one call control system may be associated with plural network telephones. Also, a single network telephone may be associated with plural call control systems.

The various control units in the network telephone 30 or 34, the call control 32 or 36, and any other system or device on the data network 11 may each include a microprocessor, a microcontroller, a processor card (including one or more microprocessors or controllers), or other control or computing devices. The storage devices referred to in this discussion may include one or more machine-readable storage media for storing data and instructions. The storage media may include different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; and optical media such as compact disks (CDs) or digital video disks (DVDs). Instructions that make up the various software routines, modules, or layers in the various network elements may be stored in respective storage devices. The instructions when executed by a respective control unit cause the corresponding network element to perform programmed acts.

The instructions of the software routines, modules or layers may be loaded or transported to the network element in one of many different ways. For example, code segments including instructions stored on floppy disks, CD or DVD media, a hard disk, or transported through a network interface card, modem, or other interface device may be loaded into the system and executed as corresponding software routines, modules, or layers. In the loading or transport process, data signals that are embodied in carrier waves (transmitted over telephone lines, network lines, wireless links, cables, and the like) may communicate the code segments, including instructions, to the network element. Such carrier

waves may be in the form of electrical, optical, acoustical, electromagnetic, or other types of signals.

Referring to Fig. 4, in accordance with one embodiment, a screen 200 that may be provided by the control tasks 160 and graphical user interface routines 162 in the call control system 32 or 36 is illustrated. The screen 200 as shown in Fig. 4 includes various icons and items (generally referred to as indicators) to allow a user sitting at the call control system to initiate, terminate, and screen calls over the data network 11. In the example shown in Fig. 4, the screen 200 includes a menu 202, a series of control buttons 204, and a list 206 of potential callees. The list 206 provides the first and last names of potential callees as well associated electronic mail addresses (or other information such as telephone numbers and so forth). As illustrated in Fig. 4, the name R. Smith may be highlighted in the list 206. The address of R. Smith is displayed in an address field 208. The address field 208 may include various formats, such as a PSTN number (e.g., 972-555-1234); a PSTN number and a proxy address (e.g., 972-555-1234 @ CTEXI300); an IP address (e.g., 47.161.18.72); a SIP address (e.g., rsmith@nortelnetworks.com); or a SIP address at a specific IP address (e.g., rsmith@47.161.18.72). Identifiers according to other formats may be illustrated in the address field 208 in further embodiments.

A status field 212 may also be included in the screen 200, which may show the status as "not in call," "outgoing call to R. Smith," "incoming call from R. Smith," and so forth. A plurality of indicators 214 may also be provided in the screen 200. A C indicator flashes when an incoming call has been missed. An S indicator gives an indication that call screening is active. A P indicator gives an indication that a SIP proxy is in use or not in use. An E indicator gives an indication of the state of the associated network telephone. Thus, the E indicator is at a first state if the network telephone is not active and at a second state if the network telephone is active and available. The E indicator may also be at a third state to indicate that a call is currently in progress.

The screen 200 is also capable of providing a pop-up menu 210 to allow a user to select one or several methods of contacting the desired callee. For example, a first option in the pop-up menu 210 is to call R. Smith. Another option is to send an electronic mail to R. Smith. A third option is to go to R. Smith's web site.

Other call control operations that may be performed by a user through the screen 200 includes volume control, screening of incoming calls, termination of a call session, and other operations.

Referring to Fig. 5, once a call is established with either a caller or a callee, another screen 300 may be shown. A picture of the caller or callee may be displayed in the screen 300. An icon 304 may be provided to allow the user to hang-up the call, and another icon 306 may be provided to allow the call to be placed on hold. A status field 308 indicates the current status of the call.

Referring to Fig. 6, a message flow between a network telephone, a call control system, and a remote system is illustrated. According to SIP, messages that may be exchanged between network elements include requests and responses. The remote system may be another call control system, one of the SIP client systems 38 and 40, the data network-PSTN gateway 20, or any other system capable of establishing a call session on the data network 11. The remote system first sends (at 402) an Invite request (according to SIP) to the call control system. The Invite request indicates that the receiving node is being invited to participate in a session. The message body of the Invite request contains a description (e.g., in SDP format) of the session to which the receiving node is being invited.

The call control system may then send (at 404) a Ringing (SIP) response back to the remote system. The Ringing response indicates that the called user agent has located a possible location where the user has registered recently and is trying to alert the user. The call control system may then send (at 406) a Connection_Req message to the network telephone to initiate a connection between the call control system and the network telephone. The messaging format between the network telephone and the call control system may be any predetermined format that allows call establishment and control to be performed by the call control system with the network telephone. One such format is the Unified Networks IP Stimulus Protocol, Draft Version 2.1, dated December 7, 1999. In further embodiments, other interface protocols may be employed. A description of one embodiment of a protocol for message exchange between the network telephone and the call control system is provided in U.S. Patent Application Serial No. 09/307,356, entitled "Telephony and Data Network Services at a Telephone," filed on May 7, 1999, which is hereby incorporated by reference.

The Connection_Req message is a generic message which includes one or more commands that indicates a request to establish a connection. The Connection_Req message

may actually include a ring command to activate the ringer of the network telephone and other commands to activate the network telephone, such as activation of the handset, headset, microphone, speaker, and so forth. The network telephone may then send back (at 408) an Ack_Req message to the call control system to acknowledge that the network telephone is available and ready. The Ack_Req message may also be a generic message to acknowledge receipt of the Connection_Req message. Upon receipt of Ack_Req message from the network telephone, the call control system sends (at 410) a 200 OK SIP response to the remote system to indicate that the request has succeeded. The remote system then sends (at 412) an Ack request (according to SIP) to the call control system. The Ack request confirms that the client has received a final response to an Invite request.

Upon receipt of Ack request, the call control system sends (at 414) a Remote_Answer message to the network telephone to indicate a request to establish a path for a call session. If accepted, the network telephone then sends (at 416) an Ack_Answer message back to the call control system. The Remote_Answer message may be a generic message that includes one or more commands to activate the network telephone for call session. One such command is a command to open or connect the audio stream to the handset, headset, microphone and speaker of the network telephone. At that point, a voice path is established (at 418) directly between the network telephone and the remote system. The voice path may be an RTP link over the data network 11.

To terminate the call, the remote system may issue (at 420) a Bye request to the call control system. The call control system then responds (at 422) with a 200 OK, indicating that the call has been terminated. Then, the call control system sends (at 424) a Disconnect_Req message to the network telephone to disconnect the network telephone from the data network. The Disconnect_Req message be a generic message including one or more commands to deactivate various components of the network telephone. For example, the audio stream may be closed or disconnected, and the handset, headset, microphone, and speaker may be deactivated. The network telephone then returns (at 426) an Ack_Disconnect message back to the call control system to indicate that the call has been disconnected.

Referring to Fig. 7, an outgoing call message flow is illustrated. In the illustrated example, the user can initiate the call from the call control system. However, the user can also make the external call from the network telephone by entering the desired number in appropriate buttons of the network telephone. In that case, messages are exchanged between

the network telephone and the call control system initially to indicate to the call control system that the user has started a phone call from the network telephone.

To start the call session, the call control system sends (at 502) an Invite request to the remote system. The remote system then sends back (at 504) a Ringing response. In response, the call control system sends (at 506) a Remote_Alerting message to the network telephone indicating that the call has been placed. The network telephone then returns (at 508) an Ack_Alerting message. At some point, the remote system, once it has answered the call, issues (at 510) a 200 OK message to the call control system. In response, the call control system then sends (at 512) an Ack request back to the remote system. The call control system also sends (at 514) a Remote_Answer message to the network telephone, which returns (at 516) an Ack_Answer message to the call control system. At that point, a voice path (e.g., an RTP path) is established (at 518) between the network telephone and the remote system over the data network 11.

To terminate the call, the remote system may issue (at 520) a Bye request. In response, the call control system may terminate the call by sending (at 522) a 200 OK message. The call control system then sends (at 524) a Disconnect_Req message to the network telephone, which returns (at 526) an Ack_Disconnect message to the call control system. At this point, the RTP voice path is terminated.

While the invention has been disclosed with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of the invention.

What is claimed is:

1. A method of communicating over a data network, comprising:

providing a user interface in a control system for establishing call sessions;

communicating, by the control system, one or more control messages over the data network to establish a call session with a remote device in response to receipt of a request through the user interface; and

transmitting one or more commands to a voice device connected to the data network and associated with the control system to establish the call session between the voice device and the remote device over the data network.

2. The method of claim 1, wherein the communicated one or more control messages and the transmitted one or more commands are according to different formats.

3. The method of claim 1, wherein transmitting the one or more commands to the voice device includes transmitting one or more commands to a network telephone including a network interface to the data network.

4. The method of claim 1, wherein establishing the call session includes establishing a Real-Time Protocol session over the data network.

5. The method of claim 1, wherein communicating the one or more control messages includes communicating messages according to a protocol defining real-time, interactive call sessions over a packet-switched data network.

6. The method of claim 1, wherein communicating the one or more control messages includes communicating one or more Session Initiation Protocol messages.

7. The method of claim 1, further comprising storing, in the control system, an identifier of the voice device.

8. The method of claim 7, wherein storing the identifier includes storing an Internet Protocol address and a port of the voice device.

9. The method of claim 1, further comprising receiving an indication from the voice device to establish another call session with the remote device.

10. The method of claim 1, further comprising displaying graphical user interface information of the call session on the control system.

11. The method of claim 1, further comprising terminating the call session using either the user interface or the voice device.

12. A method of communicating over a data network, comprising:

in a control system, communicating one or more control messages over the data network to establish a call session with a remote device coupled to the data network;

transmitting one or more commands to a voice device coupled to the data network

establishing the call session between the voice device and the remote device over the data network; and

displaying information associated with the call session on the control system.

13. The method of claim 12, wherein displaying the information includes displaying graphical user interface information.

14. The method of claim 12, wherein communicating the one or more control messages includes communicating Session Initiation Protocol messages.

15. The method of claim 12, further comprising providing one or more indicators for call control in the control system.

16. The method of claim 12, further comprising communicating Real-Time Protocol messages between the voice device and the remote device over the data network.

17. The method of claim 12, further comprising identifying, in the control system, an address of the voice device to be controlled by the control system.

18. The method of claim 12, further comprising providing a user interface on a display of the control system, the user interface enabling selection of one or more criteria associated with the voice device.

19. The method of claim 18, wherein the one or more criteria includes selection of the voice device for use in a voice session established by the control system.

20. The method of claim 19, wherein the one or more criteria includes an identifier of the voice device.

21. The method of claim 12, further comprising providing voice processing components in the control system and selecting one of the voice processing components and the voice device to communicate in the established call session.

22. The method of claim 21, further comprising receiving user selections entered in a user interface of the control system to select one of the voice processing components and the voice device.

23. The method of claim 21, further comprising redirecting selection to the other one of the voice processing components and voice device.

24. The method of claim 12, wherein the data network includes a packet-switched data network.

25. A system for controlling a voice device connected to a data network, comprising:

a user interface including one or more selectors for call control relating to call sessions;

a controller adapted to receive a request from the user interface and to generate one or more messages for communication over the data network to establish a call session with a remote device; and

an interface to transmit one or more commands relating to the call session to the voice device to establish a link between the voice device and the remote device over the data network.

26. The system of claim 25, wherein the one or more messages include Session Initiation Protocol messages.

27. The system of claim 26, further comprising a module to process the one or more Session Initiation Protocol messages.

28. The system of claim 25, wherein the interface includes a network interface for coupling to the data network.

29. The system of claim 25, further comprising a storage element including an identifier of the voice device.

30. The system of claim 25, wherein the user interface includes one or more elements to display information relating to the call session.

31. The system of claim 30, wherein the information includes graphical information.

32. A computer program capable of running in a system so that the system so programmed carries out a method for controlling voice communications over a data network, the method comprising:

providing a user interface in the system to display information associated with a call session;

communicating one or more control messages over the data network with a remote device to establish the call session between a voice device and the remote device; and

controlling the voice device during the call session.

33. The computer program of claim 32, wherein communicating comprises communicating Session Initiation Protocol messages.

34. The computer program of claim 32, wherein the method further comprises displaying a picture of a callee.

35. The computer program of claim 32, wherein the method further comprises displaying icons selectable by a user for call control.

36. A computer program product comprising at least one storage medium having thereon computer program code means to make a system execute a method for controlling a call session over a data network, the method comprising:

providing a user interface in the system for establishing the call session;

communicating one or more control messages over the data network to establish the call session with a remote device in response to a request received through the user interface; and

transmitting one or more commands to a voice device connected to the data network and associated with the control system to establish the call session between the voice device and the remote device over the data network.

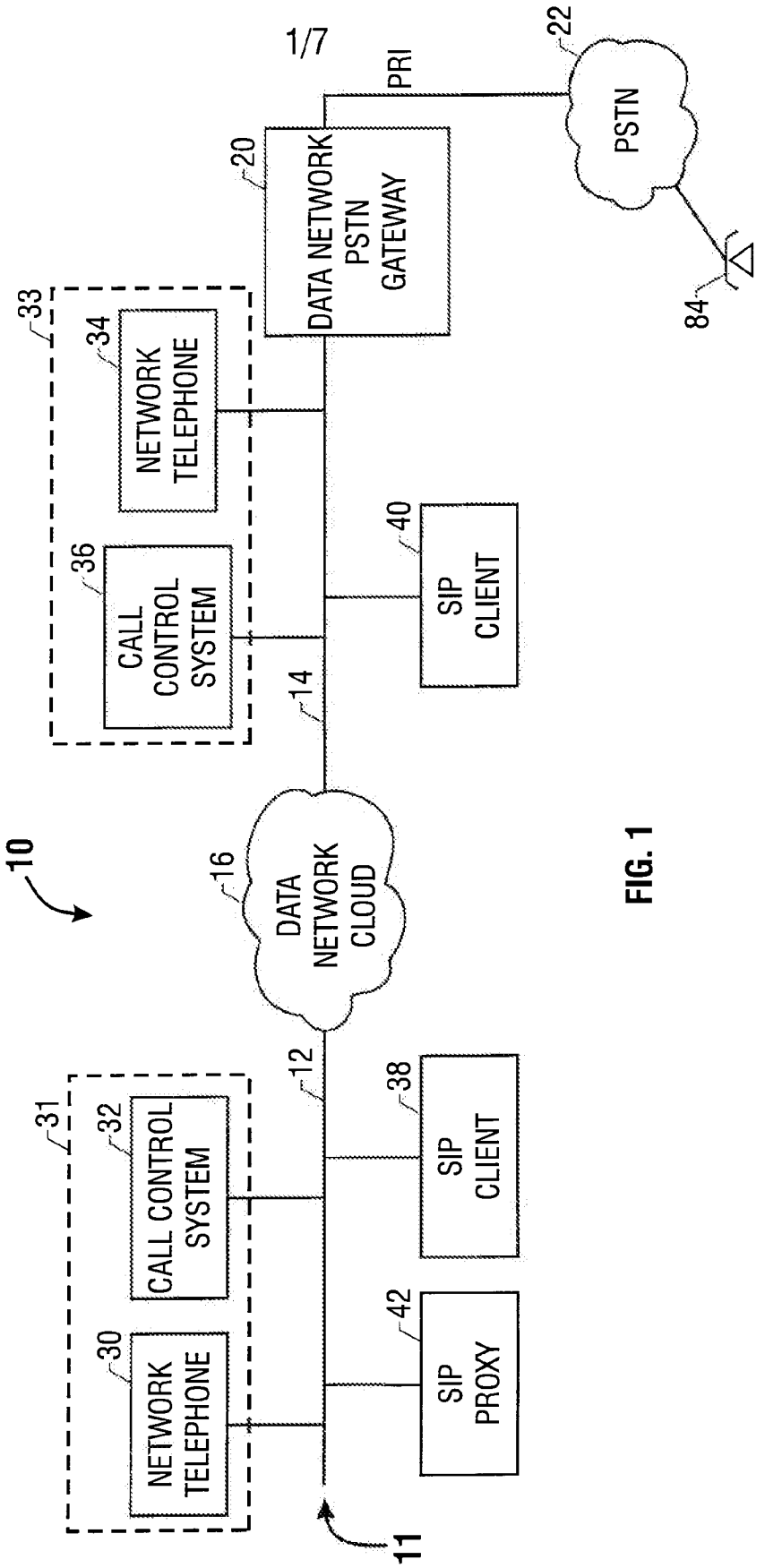

10
11
12
14
16
20
22
30
31
32
33
34
36
38
40
42
84
PRI
PSTN
DATA NETWORK PSTN GATEWAY
DATA NETWORK CLOUD
NETWORK TELEPHONE
CALL CONTROL SYSTEM
SIP CLIENT
SIP PROXY

FIG. 1

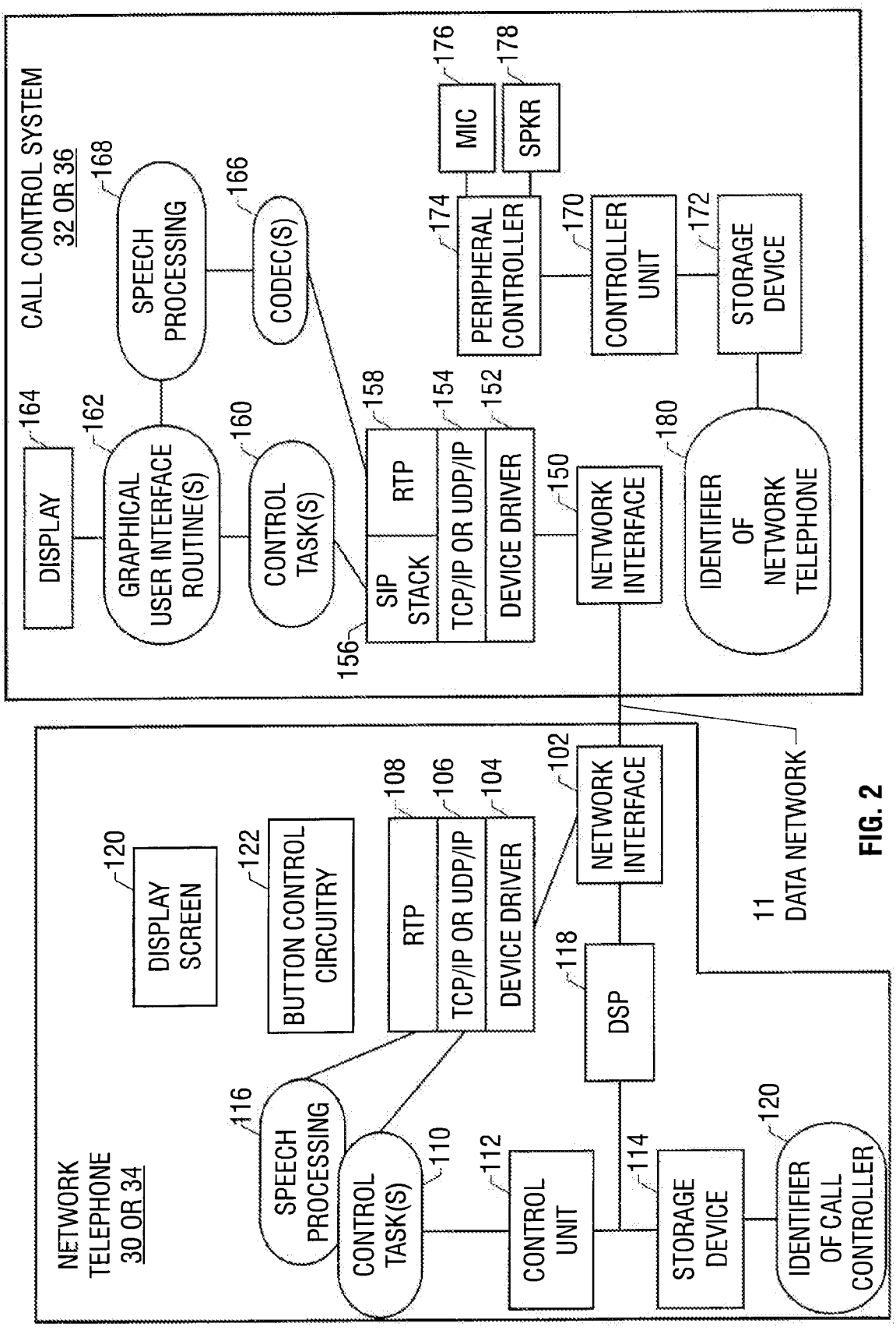

CALL CONTROL SYSTEM
32 OR 36
DISPLAY
GRAPHICAL USER INTERFACE ROUTINE(S)
CONTROL TASK(S)
SIP STACK
RTP
TCP/IP OR UDP/IP
DEVICE DRIVER
NETWORK INTERFACE
IDENTIFIER OF NETWORK TELEPHONE
SPEECH PROCESSING
CODEC(S)
MIC
SPKR
PERIPHERAL CONTROLLER
CONTROLLER UNIT
STORAGE DEVICE
NETWORK TELEPHONE
30 OR 34
DISPLAY SCREEN
BUTTON CONTROL CIRCUITRY
RTP
TCP/IP OR UDP/IP
DEVICE DRIVER
NETWORK INTERFACE
DSP
SPEECH PROCESSING
CONTROL TASK(S)
CONTROL UNIT
STORAGE DEVICE
IDENTIFIER OF CALL CONTROLLER
11
DATA NETWORK

FIG. 2

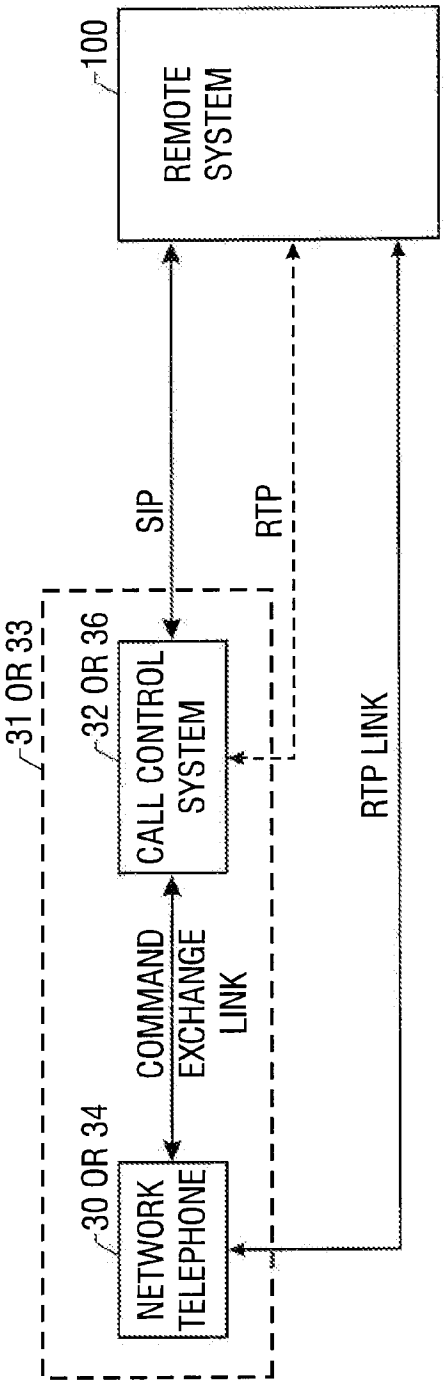

100
REMOTE SYSTEM
SIP
RTP
31 OR 33
32 OR 36
CALL CONTROL SYSTEM
RTP LINK
COMMAND EXCHANGE LINK
30 OR 34
NETWORK TELEPHONE

FIG. 3

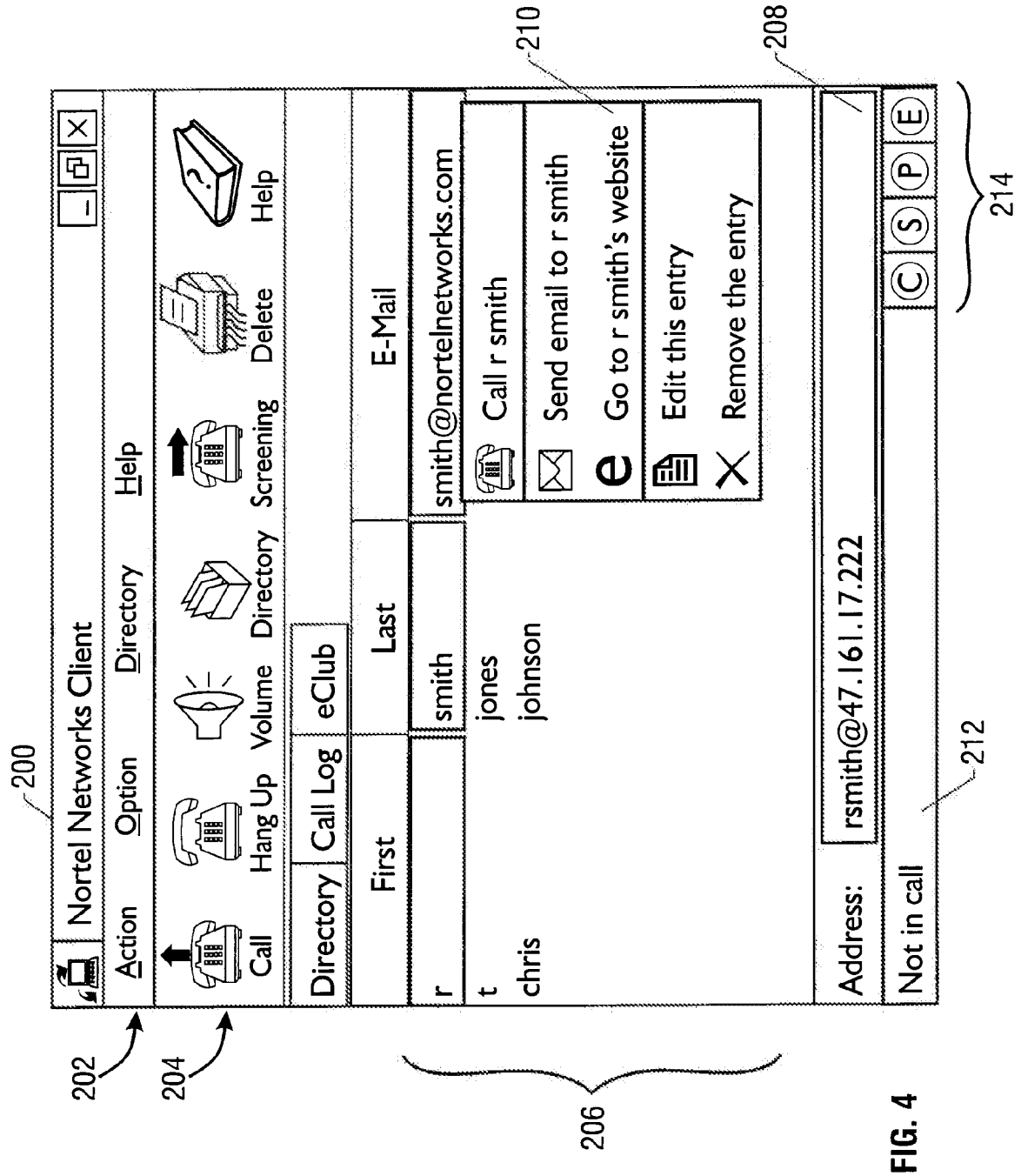

200
Nortel Networks Client
Action
Option
Directory
Help
202
Call
Hang Up
Volume
Directory
Screening
Delete
Help
204
Directory
Call Log
eClub
First
Last
E-Mail
r
smith
smith@nortelnetworks.com
t
jones
chris
johnson
Call r smith
Send email to r smith
Go to r smith's website
Edit this entry
Remove the entry
206
210
208
Address:
rsmith@47.161.17.222
Not in call
212
C
S
P
E
214

FIG. 4

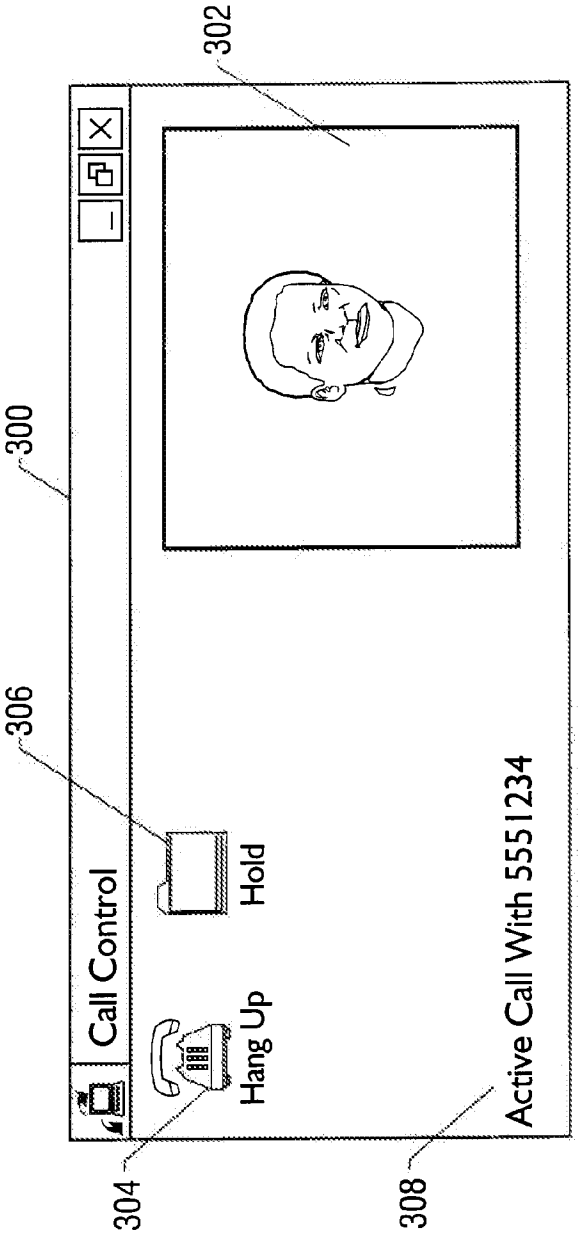

302
300
306
Call Control
Hold
Hang Up
Active Call With 5551234
304
308

FIG. 5

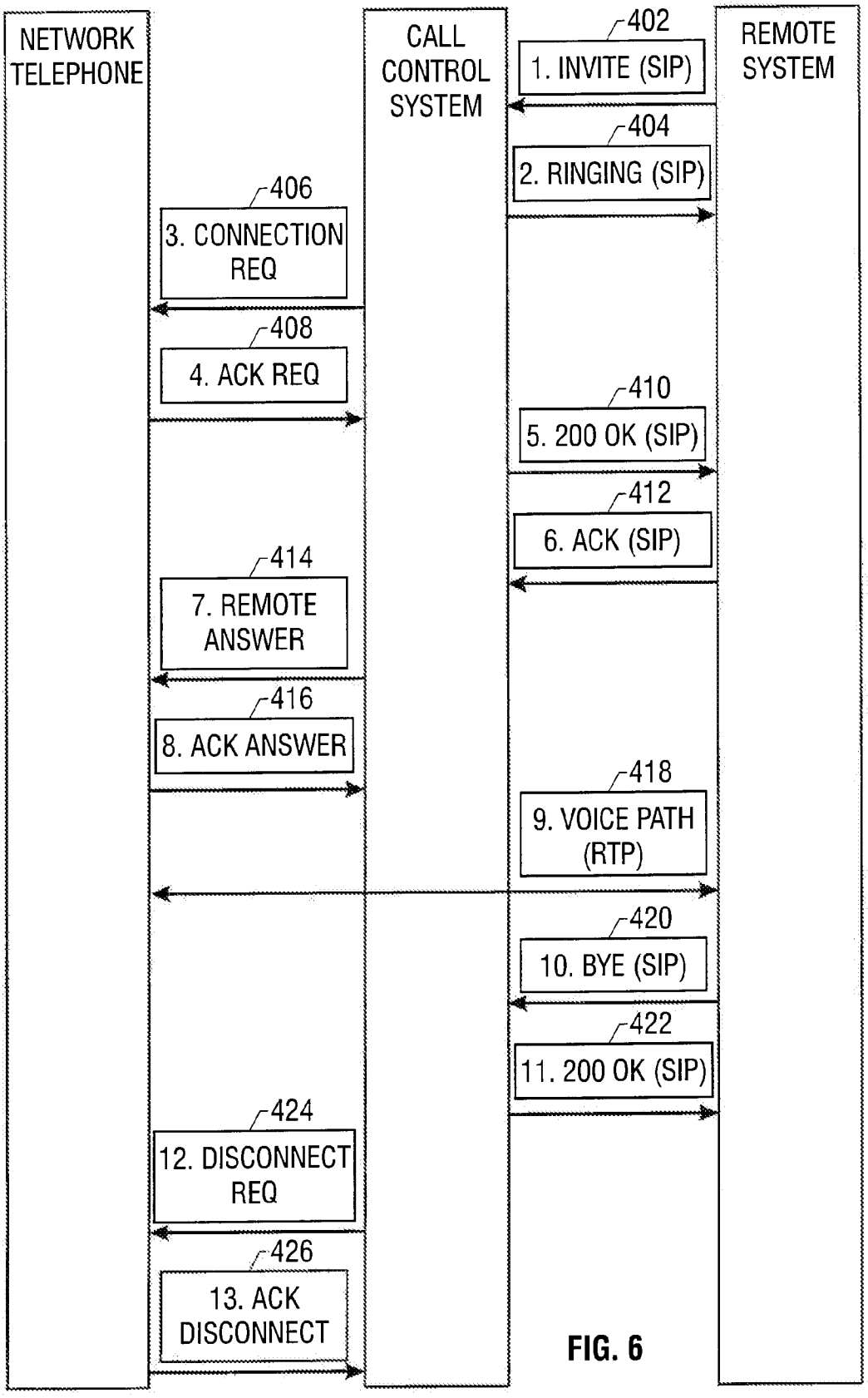

NETWORK TELEPHONE
CALL CONTROL SYSTEM
REMOTE SYSTEM
402
1. INVITE (SIP)
404
2. RINGING (SIP)
406
3. CONNECTION REQ
408
4. ACK REQ
410
5. 200 OK (SIP)
412
6. ACK (SIP)
414
7. REMOTE ANSWER
416
8. ACK ANSWER
418
9. VOICE PATH (RTP)
420
10. BYE (SIP)
422
11. 200 OK (SIP)
424
12. DISCONNECT REQ
426
13. ACK DISCONNECT

FIG. 6

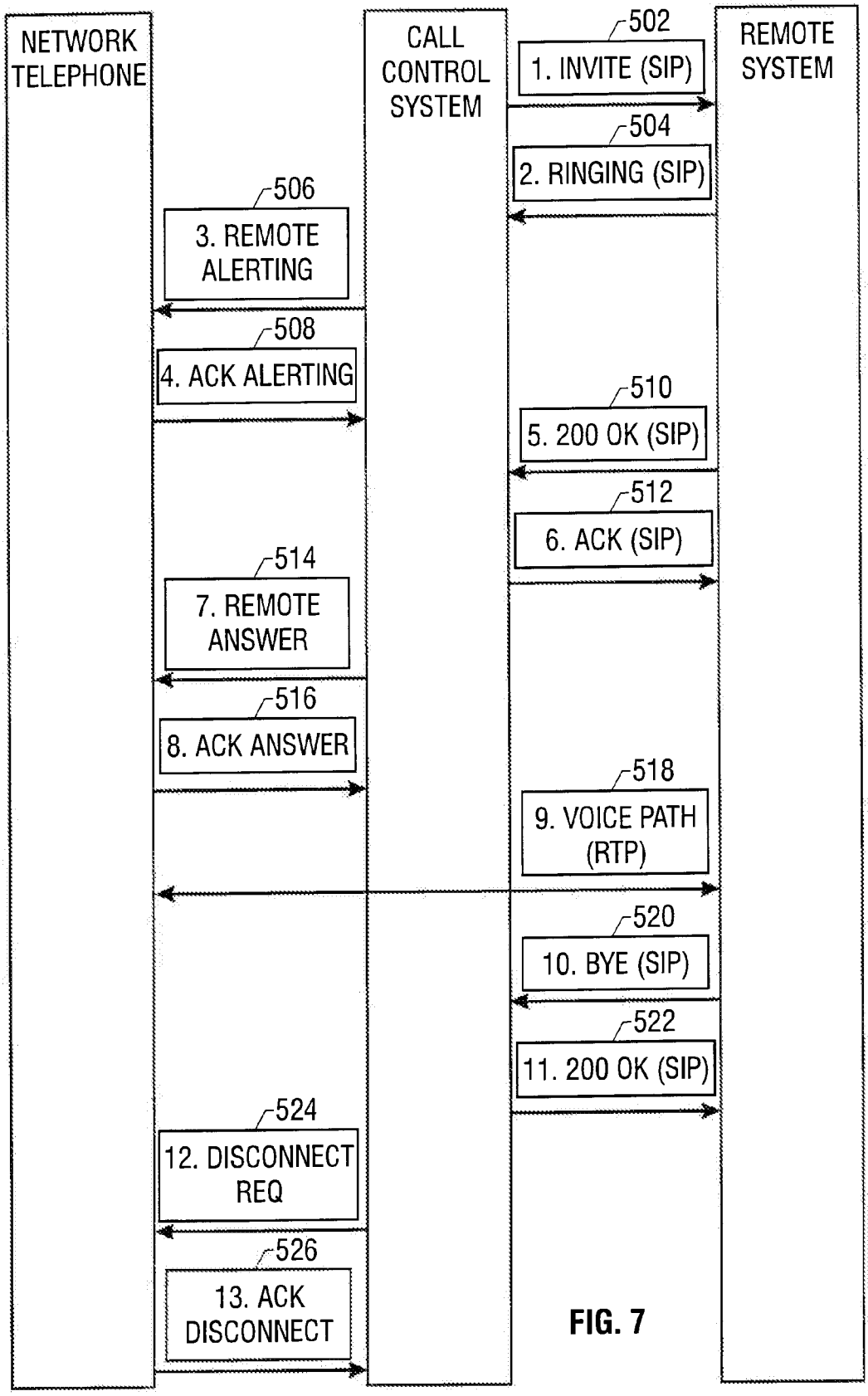

NETWORK TELEPHONE
CALL CONTROL SYSTEM
REMOTE SYSTEM
502
1. INVITE (SIP)
504
2. RINGING (SIP)
506
3. REMOTE ALERTING
508
4. ACK ALERTING
510
5. 200 OK (SIP)
512
6. ACK (SIP)
514
7. REMOTE ANSWER
516
8. ACK ANSWER
518
9. VOICE PATH (RTP)
520
10. BYE (SIP)
522
11. 200 OK (SIP)
524
12. DISCONNECT REQ
526
13. ACK DISCONNECT

FIG. 7

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/069899 A3

(51) International Patent Classification[7]: H04M 7/00, 1/253, 3/42

(21) International Application Number: PCT/US01/07686

(22) International Filing Date: 12 March 2001 (12.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/524,342 13 March 2000 (13.03.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/524,342 (CON)
Filed on 13 March 2000 (13.03.2000)

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

(72) Inventors; and

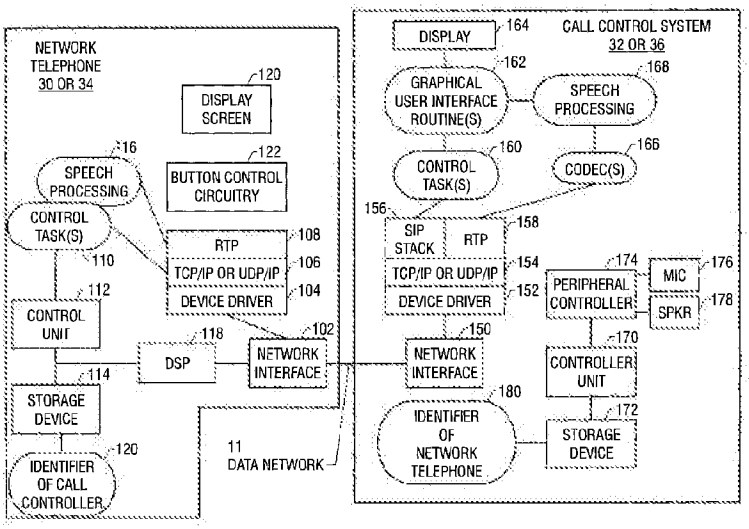
(75) Inventors/Applicants *(for US only)*: **SOLLEE, Patrick, N.** [US/US]; 2708 Garden Springs, Richardson, TX 75082 (US). **CREECH, David, R.** [US/US]; 2526 Fallview Lane, Carrollton, TX 75007 (US). **OSTERHOUT, Gregory, T.** [US/US]; 313 Falcon Court, Coppell, TX 75019 (US). **JESSEN, Christopher, L.** [US/US]; 107 Ledgenest, McKinney, TX 75070 (US).

(74) Agent: **HU, Dan, C.**; Trop, Pruner & Hu, P.C., 8554 Katy Freeway, Suite 100, Houston, TX 77024 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, 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, US, UZ, VN, YU, ZA, ZW.

[Continued on next page]

(54) Title: CONTROLLING VOICE COMMUNICATIONS OVER A DATA NETWORK



(57) Abstract: Recently, network telephones have been developed that are capable of being connected directly to a data network, such as an IP network. These network telephones are capable of placing telephony calls over a data network. The voice quality offered by such telephones are typically superior to those that can be offered by computer systems, since such network telephones typically include dedicated digital signal processors (DSPs) that perform the data intensive calculations involved in speech processing. However, the existing network telephones do not provide desired multimedia presentation capabilities such as those offered by displays of computer systems. Thus, while networks telephones offer superior speech capabilities, it does have the desired multimedia capabilities. On the other hand, computer systems have superior multimedia capabilities, but they suffer from relatively poor speech processing performance. A need thus exists for an improved method and apparatus for controlling voice communications over data networks. A method and apparatus of communicating over a data network (11) includes providing a user interface (200) in a control system (32, 36) for call control and to display information relating to a call session. The control system (32, 36) communicates one or more control messages (e.g., Session Initiation Protocol or SIP messages) over the data network (11) to establish a call session with a remote device in response to receipt of a request through the user interface. One or more commands are transmitted to a voice device (30, 34) associated with the control system (32, 36) to establish the call session between the voice device (30, 34) and the remote device over the data network (11). A Real-Time Protocol (RTP) link may be established between the voice device (30, 34) and the remote device.

WO 01/069899 A3

(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).

Declaration under Rule 4.17:

..... *of inventorship (Rule 4.17(iv)) for US only*

Published:

..... *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
29 August 2002

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.

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 01/07686

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M7/00 H04M1/253 H04M3/42

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC, COMPENDEX, EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 721 266 A (NCR INT INC) 10 July 1996 (1996-07-10) column 4, line 21 - line 35	1,12,25, 32,36 2-11, 13-24, 26-31, 33-35
A	THOM G A: "H. 323: THE MULTIMEDIA COMMUNICATIONS STANDARD FOR LOCAL AREA NETWORKS" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER. PISCATAWAY, N.J, US, vol. 34, no. 12, 1 December 1996 (1996-12-01), pages 52-56, XP000636454 ISSN: 0163-6804 the whole document	1-36

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 June 2002	03/07/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Schweitz, M

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 05590 A (HARBISON ROBERT W ;LO MING C (US); STARVOX INC (US); BARRY RICHARD) 4 February 1999 (1999-02-04) page 3, line 23 -page 12, line 13 ---	1-36
A	EP 0 836 295 A (IBM) 15 April 1998 (1998-04-15) page 2, line 3 -page 3, line 38 ---	1-36
A	EP 0 829 995 A (SPHERE COMMUNICATIONS INC) 18 March 1998 (1998-03-18) the whole document -----	1-36

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/US 01/07686

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0721266 A	10-07-1996	US 5742670 A	21-04-1998
		EP 0721266 A2	10-07-1996
		JP 8321889 A	03-12-1996
WO 9905590 A	04-02-1999	AU 8576798 A	16-02-1999
		EP 1021757 A1	26-07-2000
		WO 9905590 A2	04-02-1999
		US 2002018308 A1	14-02-2002
EP 0836295 A	15-04-1998	EP 0836295 A2	15-04-1998
		KR 259409 B1	15-06-2000
		US 6181691 B1	30-01-2001
EP 0829995 A	18-03-1998	US 5892764 A	06-04-1999
		AU 728479 B2	11-01-2001
		AU 3757097 A	19-03-1998
		CA 2215863 A1	16-03-1998
		EP 0829995 A2	18-03-1998
		JP 10145397 A	29-05-1998

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80587 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/EP01/04181

(22) International Filing Date: 11 April 2001 (11.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0009290.8 15 April 2000 (15.04.2000) GB

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

(72) Inventors: LINDGREN, Hans, Åke; Ringvägen 11F 4tr, S-118 43 Stockholm (SE). STILLE, Mats, Ola; Åsögatan 116, S-116 24 Stockholm (SE).

(74) Agent: O'CONNELL, David, Christopher; Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD (GB).

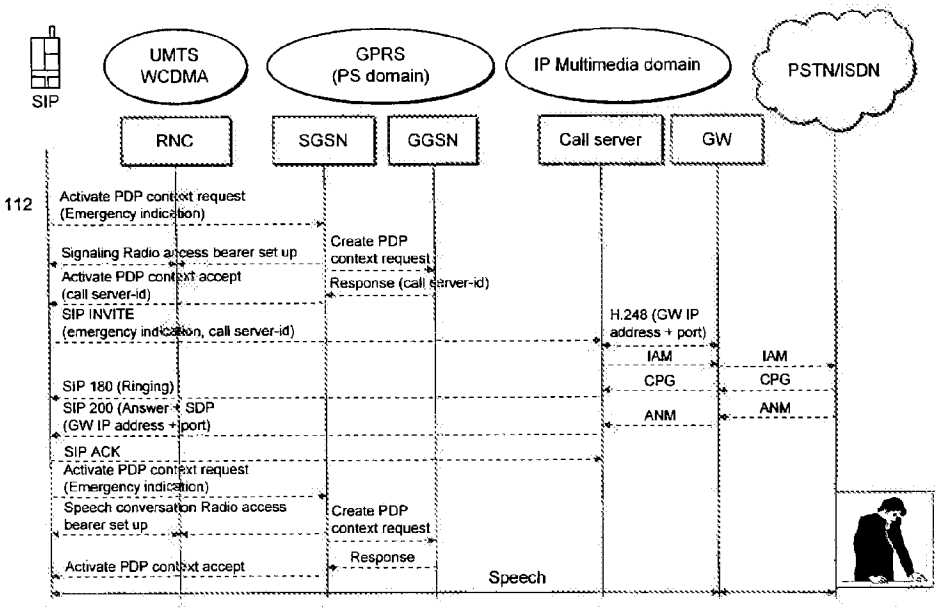
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, 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, SK (utility model), 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:
..... *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR EMERGENCY CALL HANDLING IN A MOBILE PACKET SWITCHED NETWORK



(57) Abstract: There is described a system which, in a voice over IP radiotelecommunications system, allows a mobile station to make an emergency call, even though other calls would not be allowed at that time. The mobile station includes an emergency call indication in the session activation request, and this is recognised by the network nodes, which then allow call set up.

WO 01/80587 A1

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.

SYSTEM AND METHOD FOR EMERGENCY CALL HANDLING IN A MOBILE PACKET SWITCHED NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates to a telecommunications system, and to a method of operation thereof. More particularly, the invention relates to a telecommunications network using Internet Protocol (IP), and specifically to a system for handling emergency calls in such a network.

BACKGROUND OF THE INVENTION

In mobile communication systems, there are situations in which a call request may not be allowed. For example the user may not have paid a bill, or the mobile system may have no information at all about the user, or there may be congestion on the network, or the mobile phone may be reported stolen.

In the GSM system, emergency calls may be allowed even when one of these factors apply.

It is expected that 3rd generation (3G) mobile phones will allow voice over IP. That is, the Internet Protocol (IP) will be used for the whole call from the mobile phone to the network gateway which is the connection to the public switched telephone network (PSTN) which includes the emergency services operator. Therefore, all calls will send the voice signals as packet data, rather than as circuit switched data.

The document "GSM on the Net", by Granberg, Ericsson Review No. 4, 1998 pages 184-191, describes a voice over IP system, based on the recommendation ITU H.323. The H.323 protocol separates call control (signalling in the call setup phase) from connection control (the actual data flows).

However, it provides no mechanism to allow for special treatment of emergency calls.

SUMMARY OF THE INVENTION

The present invention is concerned with allowing

special treatment of emergency calls, so that such a call can be successful even though another voice call would not be allowed.

According to one aspect of the invention, a mobile communication device analyses a dialled number and, in the case of an emergency call, sends a session activation request which includes an emergency call indication.

According to another aspect of the invention, a node in a packet data communication network detects an emergency call indication in a session activation request, and allows call setup, even though a call without such an indication would fail.

According to another aspect of the invention,

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a diagram illustrating message flows during call setup in accordance with the invention.

Figure 2 is a flow chart showing a method carried out in a mobile phone in accordance with the invention.

Figure 3 is a schematic representation of a mobile phone in accordance with the invention.

Figure 4 is a diagram illustrating message flows during call setup in accordance with a second embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In accordance with the invention, when a mobile phone wishes to place an emergency call, it sets a special emergency call indication when requesting mobile system and radio resources.

Figure 1 shows the network components required to connect a 3rd generation mobile phone to an emergency services operator. A radio network controller (RNC) controls the air interface with a mobile station 10, and operates in the Universal Mobile Telephony System (UMTS) or using Wideband Code Division Multiple Access

(WCDMA). The network operates using the General Packet Radio System (GPRS), and includes a Serving GPRS Service Node (SGSN) and a Gateway GPRS Service Node (GGSN). The GGSN is connected to a call server in the IP multimedia domain, and this is further connected to a gateway, which is connected to the public telephone network, operating for example as a Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN) system. The emergency services operator is connected to the public telephone network.

The call setup procedure is also shown in Figure 1, while Figure 2 shows the procedure in the phone, and Figure 3 is a representation of a phone 10. The procedure is described further with reference to the Session Initiation Protocol (SIP), described in IETF document IETF/RFC 2543. This protocol is part of the IETF multimedia data and control architecture, and can be used to set up calls between parties.

As shown in Figure 1, a user enters a dialled number, for example via a keypad 12, which is sent to a controller 14, which then forms a message to be sent via transceiver circuitry 16 through an antenna 18.

In the controller 14, the dialled number is received (step 20 in Figure 2), and the controller recognises from the dialled digits (for example, the numbers 112, 911 or 999), that the call is an emergency call. The session activation request which is then sent (step 24, and also see Figure 1) is then handled accordingly.

The mobile phone has to activate a packet (IP) data communication session with the mobile GPRS system over the air interface. A first PDP activation (Activate PDP Context Request, according to the GSM recommendation 24.008) is sent from the mobile station to the SGSN to get a signalling radio bearer. When

this has been obtained, the mobile station sends a second PDP activation to the SGSN, stipulating the need for a voice communication, allowing the user to speak to an operator at an emergency centre. The second PDP activation includes the requested bandwidth, delay and other quality of service parameters. These two radio bearers remain in parallel until the call is dropped.

In the illustrated embodiment of the invention, the two activation messages each include an indication that this is an emergency call. In the context of the GSM recommendation 24.008, the emergency indicator could for example be set by setting the Access Point Name (APN) to "EMERGENCY", Or something similar.

Thus, in more detail, the first session activation request is received by the 3G GPRS SGSN element. The SGSN recognises the received emergency call indication, and the SGSN will then not stop the call setup process, even if it would normally fail, for example because it cannot obtain user profile data or if unsuccessful authentication occurs.

The SGSN will send a Create PDP context request to the GGSN of the same network as the SGSN, to create a packet session with it. The context request will contain the special indication about an emergency call, received from the mobile phone as described above. This opens a communication path between the SGSN and the GGSN for this particular emergency call.

Since the GGSN has received the emergency call indication from the SGSN, the GGSN will determine the identity of the locally geographical VoIP call server that should receive forthcoming call control signals from the mobile phone. This can be done by software in the GGSN. This has the advantage that the call is routed out from the mobile system and to the public network emergency centre as fast as possible. This

avoids the possibility that the call could be routed to the call server belonging to the home network of the user. If the user is roaming, this could conceivably be in another country.

This call server identity is thereafter returned by the GGSN to the SGSN in the acknowledgement message which relates to the first activation message. The call server identity can be an IP address in conventional format.

The SGSN then returns the call server identity back to the mobile phone, for example in the acknowledgement signal to the first Activate PDP context request message.

When the mobile phone gets a successful session activation acknowledgement from the mobile system, the mobile phone can start the voice over IP (VoIP) related call control signalling over the session. In this described embodiment, this call control signalling is as described in the IETF Session Initiation Protocol (SIP). The first signal, that is, the INVITE signal in SIP, will include the VoIP call server identity determined by the GGSN and received from the SGSN. When the mobile terminal receives the call server identity in the format of an IP address, the mobile terminal should set this address in the IP packet header "destination address" field at all times when sending SIP messages, including the INVITE message. In this way, network routers will route IP packets that are carrying such SIP messages, directed to the call server, correctly to the call server.

The call server can also typically be the same as handling all the normal VoIP calls as well. The initial message, for example the SIP INVITE message, includes an emergency indication as well, either the number dialled by the user e.g. 112 in a 3G UMTS

European system or 911 in a 3G UMTS North America system, or a separate emergency indication. Alternatively, a new message could be defined, for example a SIP EMERGENCY INVITE message. Including the emergency indication avoids the possibility that the call server could treat the call as a normal voice call, with the possibility that it could stop the call process in the event of a failure to continue.

The call server then places an ISUP call to the appropriate PSTN signalling/media gateway for the emergency services operator using ISUP/IP, which routes the call using ISUP/SS7 to the operator. Then, as is conventional, a ringing response is sent using ISUP to the gateway, and using SIP to the call server and then to the mobile station. The response includes the address of the gateway.

This can then be used by the mobile station to create the required voice bearers to carry speech to the emergency services operator with the desired parameters, using the gateway address so that speech packets can reach the gateway. Thus, the mobile terminal sends a second Activate PDP Context request message, including an emergency indication, to the SGSN, which sets up a radio access bearer with the mobile terminal, and also sends a Create PDP Context request to the GGSN.

The GGSN responds to this message, and the SGSN sends an Activate PDO Context accepr message to the mobile terminal, after which a speech path is established between the mobile terminal and the emergency services operator.

Figure 4 illustrates a second call setup process according to the invention.

In the same way as Figure 1, Figure 4 also shows the network components required to connect a 3rd

generation mobile phone to an emergency services operator, namely a radio network controller (RNC) controlling the air interface with a mobile station 10. The network operates using the GPRS system, and includes a SGSN and a GGSN. The GGSN is connected to a call server in the IP multimedia domain, and this is further connected to a gateway, which is connected to the public telephone network, operating for example as a PSTN or ISDN system. The emergency services operator is connected to the public telephone network.

Figure 4 shows the set up of an emergency call from a mobile station, when the mobile station does not contain a Subscriber Identity Module (SIM) card. In that case, it is conventionally not possible to initiate a call.

As in the procedure described with reference to Figure 1, the mobile phone has to activate a packet (IP) data communication session with the mobile GPRS system over the air interface. In this case, when the mobile phone is without a SIM, it is permitted to form a limited attach. Thus, the mobile station sends an attach request via the RNC to the SGSN. In the attach request, the International Mobile Station Equipment Identity (IMEI) is transmitted as the mobile identity, and there is no Routing Area Indentification (RAI) or Ciphering Key Sequence Number (CKSN). An alternative is that the attach request should be allowed to be sent without any mobile identity.

In this embodiment of the invention, the only service allowed after formation of a limited attach is an emergency call. Therefore, the receipt by the SGSN of an attach request with the IMEI as the only identifier is a preliminary indication that an emergency call is required.

The formation of a limited attach is allowed in

some situations where a normal attach would not be allowed, including in this case where no SIM is available. A normal attach should be used if possible. In the procedure illustrated in Figure 4, the SGSN accepts the formation of the limited attach, and returns an attach accept message to the mobile station, with a Temporary Mobile Station Identifier (P-TMSI), and a Random Access Identifier (RAI).

The SGSN does not need to contact the Home Location Register (HLR) of the mobile station subscriber. Moreover, the SGSN does not perform any authentication or ciphering.

Thereafter, a request is sent from the mobile station to the SGSN to get a signalling radio bearer. When this has been obtained, the mobile station sends a second PDP activation request to the SGSN, stipulating the need for a voice communication, allowing the user to speak to an operator at an emergency centre. The second PDP activation includes the requested bandwidth, delay and other quality of service parameters. These two radio bearers remain in parallel until the call is dropped.

Preferably, the two activation messages each include an indication that this is an emergency call. In the context of the GSM recommendation 24.008, the emergency indicator could for example be set by setting the Access Point Name (APN) to "EMERGENCY", Or something similar.

Thus, in more detail, the first session activation request is received by the 3G GPRS SGSN element. The SGSN recognises the received emergency call indication, and the SGSN will then not stop the call setup process, even if it would normally fail, for example because it cannot obtain user profile data or if unsuccessful authentication occurs.

The SGSN will send a Create PDP context request to the GGSN of the same network as the SGSN, to create a packet session with it. The context request will contain the special indication about an emergency call, received from the mobile phone as described above. This opens a communication path between the SGSN and the GGSN for this particular emergency call.

Since the GGSN has received the emergency call indication from the SGSN, the GGSN will determine the identity of the locally geographical VoIP call server that should receive forthcoming call control signals from the mobile phone. This can be done by software in the GGSN. This has the advantage that the call is routed out from the mobile system and to the public network emergency centre as fast as possible. This avoids the possibility that the call could be routed to the call server belonging to the home network of the user. If the user is roaming, this could conceivably be in another country.

This call server identity is thereafter returned by the GGSN to the SGSN in the acknowledgement message which relates to the first activation message. The call server identity can be an IP address in conventional format.

The SGSN then returns the call server identity back to the mobile phone, for example in the acknowledgement signal to the first Activate PDP context request message.

When the mobile phone gets a successful session activation acknowledgement from the mobile system, the mobile phone can start the voice over IP (VoIP) related call control signalling over the session. In this described embodiment, this call control signalling is as described in the IETF Session Initiation Protocol (SIP). The first signal, that is, the INVITE signal in

SIP, will include the VoIP call server identity determined by the GGSN and received from the SGSN. When the mobile terminal receives the call server identity in the format of an IP address, the mobile terminal should set this address in the IP packet header "destination address" field at all times when sending SIP messages, including the INVITE message. In this way, network routers will route IP packets that are carrying such SIP messages, directed to the call server, correctly to the call server.

The call server can also typically be the same as handling all the normal VoIP calls as well. The initial message, for example the SIP INVITE message, includes an emergency indication as well, either the number dialled by the user e.g. 112 in a 3G UMTS European system or 911 in a 3G UMTS North America system, or a separate emergency indication. Alternatively, a new message could be defined, for example a SIP EMERGENCY INVITE message. Including the emergency indication avoids the possibility that the call server could treat the call as a normal voice call, with the possibility that it could stop the call process in the event of a failure to continue.

The call server then places an ISUP call to the appropriate PSTN signalling/media gateway for the emergency services operator using ISUP/IP, which routes the call using ISUP/SS7 to the operator. Then, as is conventional, a ringing response is sent using ISUP to the gateway, and using SIP to the call server and then to the mobile station. The response includes the address of the gateway.

This can then be used by the mobile station to create the required voice bearers to carry speech to the emergency services operator with the desired parameters, using the gateway address so that speech

packets can reach the gateway. Thus, the mobile terminal sends a second Activate PDP Context request message, including an emergency indication, to the SGSN, which sets up a radio access bearer with the mobile terminal, and also sends a Create PDP Context request to the GGSN.

The GGSN responds to this message, and the SGSN sends an Activate PDO Context accepr message to the mobile terminal, after which a speech path is established between the mobile terminal and the emergency services operator.

It should be noted that, although the invention has been described with particular reference to a GPRS based mobile telephone system using the IETF SIP, it is applicable to any mobile communication system, which offers real-time packet (IP) data communication, with any type of call control protocol, including for example ITU-T H.323.

There is thus described a method which allows an emergency call to be placed even when other calls would not be allowed.

CLAIMS

1. A mobile communications device, capable of operating in a packet data communications network, the device comprising:

means for analysing a dialled number,

the device being adapted, in the event that a dialled number is indicative of an emergency call, to send a session activation request which includes an emergency call indication.

2. A mobile communications device as claimed in claim 1, the device being adapted to send the session activation request, in the event that a dialled number is indicative of an emergency call, even if the device has no SIM.

3. A method of handling an emergency call in a mobile device capable of operating in a packet data communication network, the method comprising:

analysing a dialled number; and

if the dialled number is indicative of an emergency call, sending a session activation request which includes an emergency call indication.

4. A method as claimed in claim 3, comprising sending the session activation request if the dialled number is indicative of an emergency call, even if the mobile device has no SIM.

5. A network node for use in a pocket data communications network, the node comprising means for detecting an emergency call indication in a received session activation request, and being adapted, in the event that an emergency call indication is detected, to set up a call even if normal call setup criteria are not met.

6. A node as claimed in claim 5, wherein the mode is a SGSN element.

7. A node as claimed in claim 6, wherein the

node is adapted, in the event that an emergency call indication is detected, to set up a call even if the received session activation request includes no mobile station identifier.

8. A node as claimed in claim 6, adapted, in the event that an emergency call indication is detected, to create a packet session with a GGSN, including a further emergency call indication.

9. A node as claimed in claim 5, wherein the mode is a GGSN element.

10. A node as claimed in claim 7, adapted, in the event that an emergency call is detected, to return a message indicating a call server local to a calling device.

11. A method of operation of a node in a packet data communications network, the method comprising:

detecting an emergency call indication in a received session activation request, and

if an emergency call indication is detected, setting up a call even if normal call setup criteria are not met.

12. A method as claimed in claim 11, wherein the mode is a SGSN element, and the method further comprises:

if an emergency call indication is detected, creating a packet session with a GGSN, including a further emergency call indication.

13. A method as claimed in claim 11, wherein the mode is a SGSN element, and the method further comprises, in the event that an emergency call indication is detected, setting up a call even if the received session activation request includes no mobile station identifier.

14. A method as claimed in claim 11, wherein the mode is a GGSN element, and the method further

comprises:

if an emergency call indication is detected, returning a message indicating a call server local to a calling device.

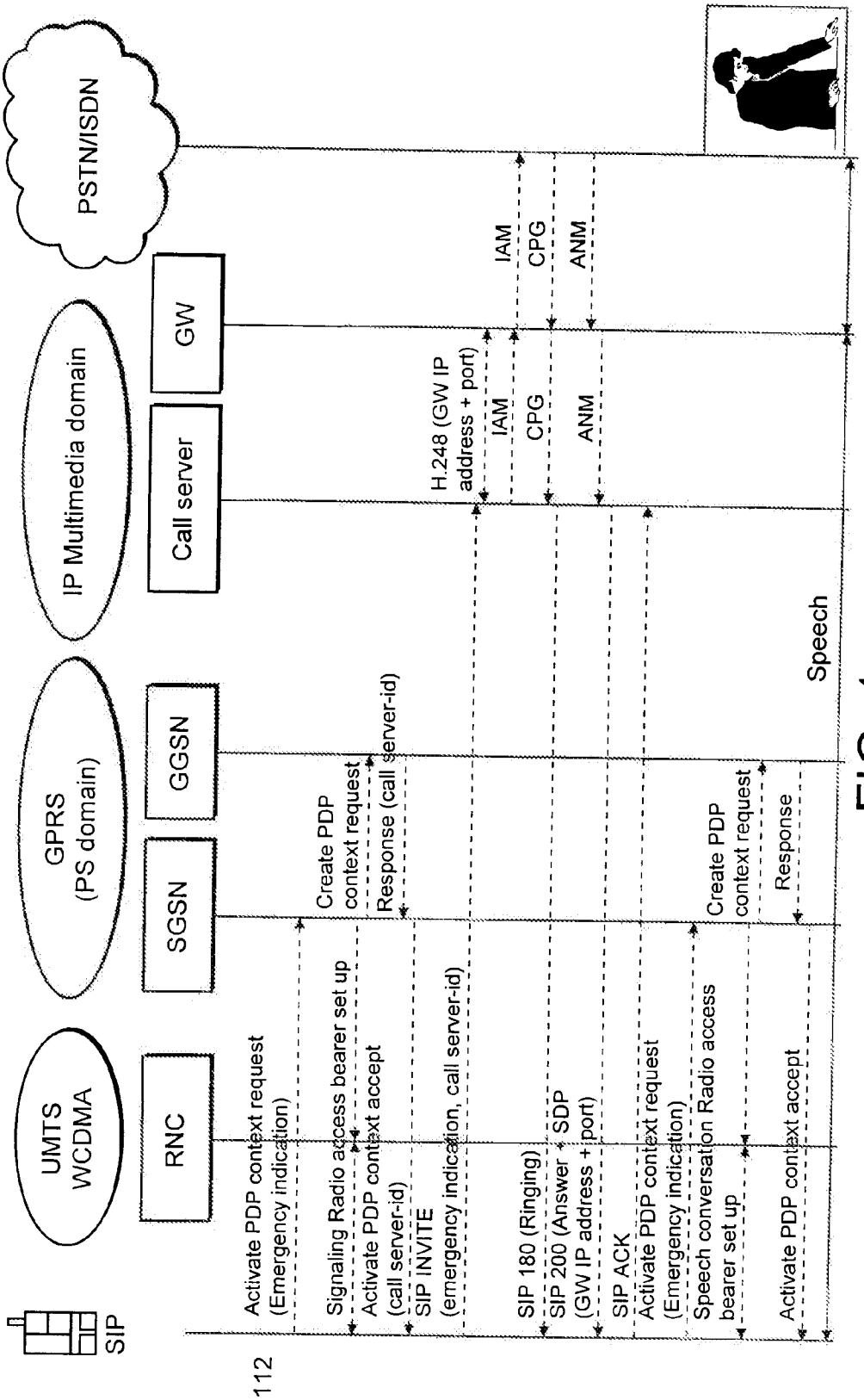

SIP
UMTS WCDMA
GPRS (PS domain)
IP Multimedia domain
PSTN/ISDN
RNC
SGSN
GGSN
Call server
GW
112
Activate PDP context request (Emergency indication)
Create PDP context request
Response (call server-id)
Signaling Radio access bearer set up
Activate PDP context accept (call server-id)
SIP INVITE (emergency indication, call server-id)
H.248 (GW IP address + port)
IAM
CPG
ANM
SIP 180 (Ringing)
SIP 200 (Answer + SDP (GW IP address + port)
IAM
CPG
ANM
SIP ACK
Activate PDP context request (Emergency indication)
Create PDP context request
Response
Speech conversation Radio access bearer set up
Activate PDP context accept
Speech

FIG. 1

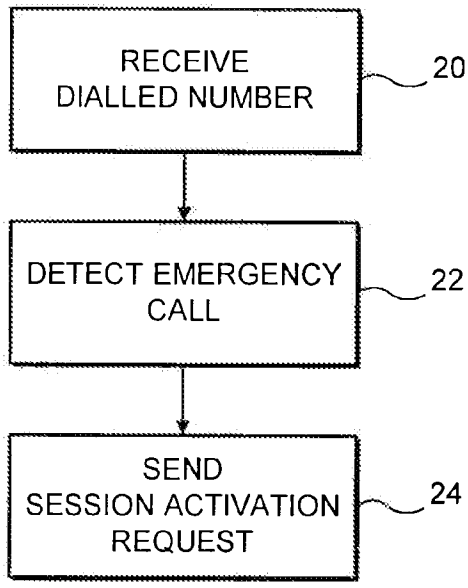

RECEIVE DIALLED NUMBER
20
DETECT EMERGENCY CALL
22
SEND SESSION ACTIVATION REQUEST
24

FIG. 2

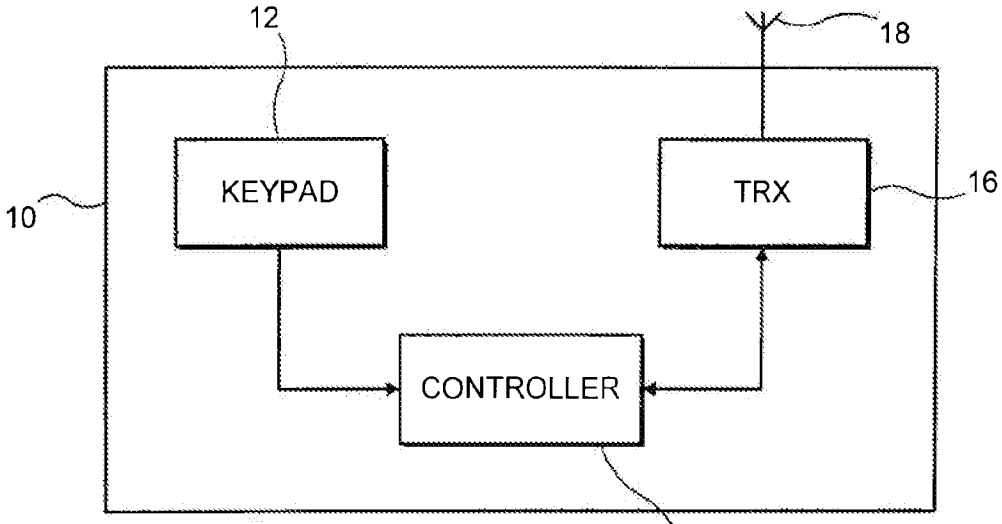

12
18
KEYPAD
TRX
16
10
CONTROLLER
14

FIG. 3

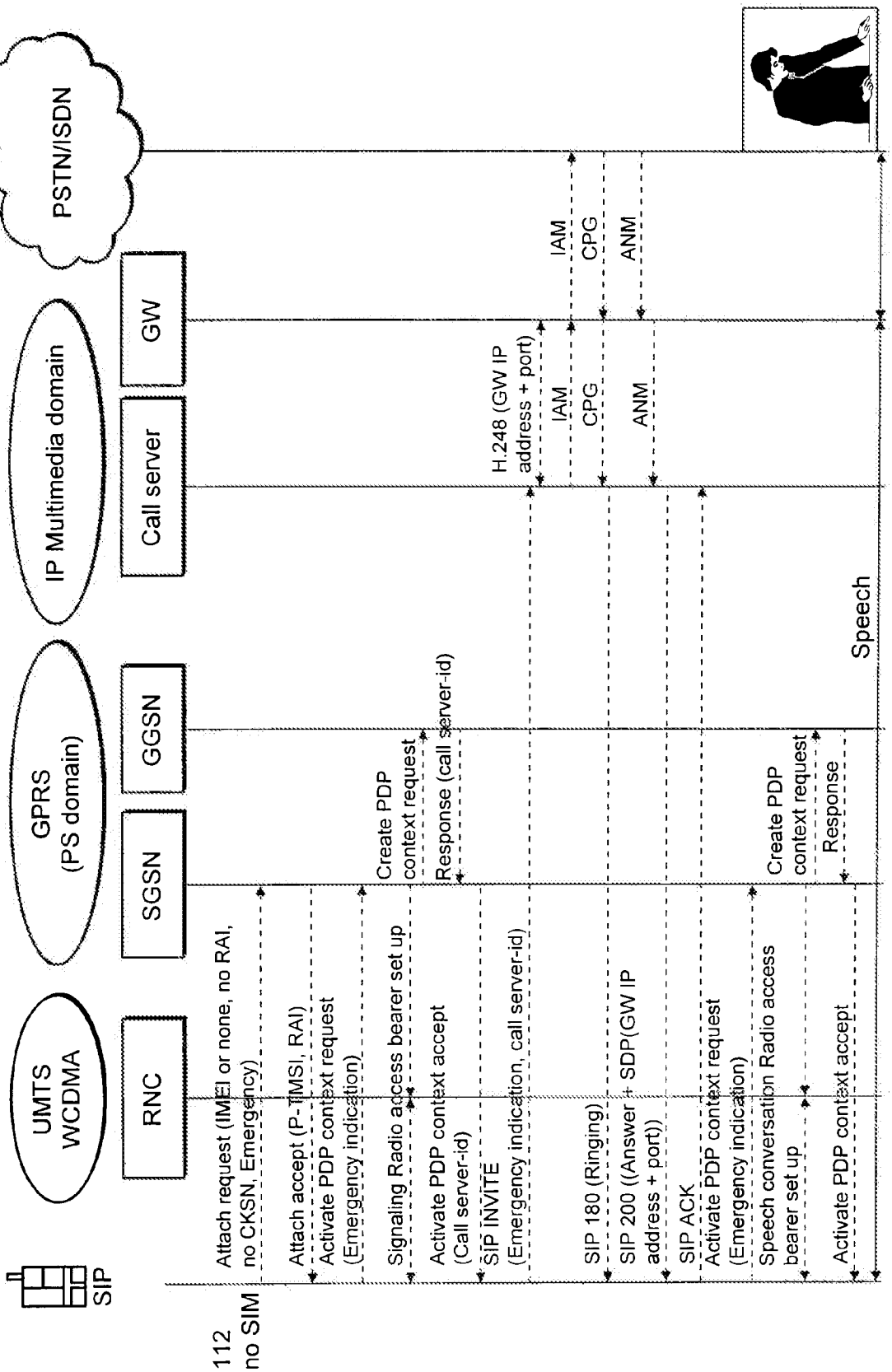

SIP
UMTS WCDMA
GPRS (PS domain)
IP Multimedia domain
PSTN/ISDN
RNC
SGSN
GGSN
Call server
GW
112 no SIM
Attach request (IMEI or none, no RAI, no CKSN, Emergency)
Attach accept (P-TMSI, RAI)
Activate PDP context request (Emergency indication)
Signaling Radio access bearer set up
Create PDP context request
Response (call server-id)
Activate PDP context accept (Call server-id)
SIP INVITE (Emergency indication, call server-id)
H.248 (GW IP address + port)
IAM
CPG
ANM
SIP 180 (Ringing)
SIP 200 ((Answer + SDP(GW IP address + port))
SIP ACK
Activate PDP context request (Emergency indication)
Create PDP context request
Response
Speech conversation Radio access bearer set up
Activate PDP context accept
Speech

FIG. 4

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 01/04181

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SATYABRATA CHAKRABARTI ET AL: "A NETWORK ARCHITECTURE FOR GLOBAL WIRELESS POSITION LOCATION SERVICES" VANCOUVER, CA, JUNE 6 - 10, 1999,NEW YORK, NY: IEEE,US, 6 June 1999 (1999-06-06), pages 1779-1783, XP000903675 ISBN: 0-7803-5285-8	1,3
Y	page 1779, left-hand column, paragraph 1 page 1782, left-hand column, paragraph 5 -right-hand column figures 1-3	2,4-7, 11-13
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 July 2001	14/08/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kreppel, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 01/04181

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	REED J H ET AL: "AN OVERVIEW OF THE CHALLENGES AND PROGRESS IN MEETING THE E-911 REQUIREMENT FOR LOCATION SERVICE" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 36, no. 4, 1 April 1998 (1998-04-01), pages 30-37, XP000752568 ISSN: 0163-6804 page 30, left-hand column, last paragraph -right-hand column, paragraph 3 ---	2,4-7, 11-13
E	EP 1 109 416 A (NORTEL NETWORKS LTD) 20 June 2001 (2001-06-20) column 17, line 29 -column 20, line 46 figure 6 ---	1-14
A	SCHULZRINNE HENNING G ET AL: "The Session Initiation Protocol: Providing Advanced Telephony Services Across the Internet" BELL LABS TECHNICAL JOURNAL, October 1998 (1998-10), XP002164648 the whole document ---	1-14
A	KORPI M ET AL: "SUPPLEMENTARY SERVICES IN THE H.323 IP TELEPHONY NETWORK" IEEE COMMUNICATIONS MAGAZINE,US,IEEE SERVICE CENTER. PISCATAWAY, N.J, vol. 37, no. 7, July 1999 (1999-07), pages 118-125, XP000835313 ISSN: 0163-6804 the whole document ---	1-14
A	WANG J ET AL: "WIRELESS VOICE-OVER-IP AND IMPLICATIONS FOR THIRD-GENERATION NETWORK DESIGN" BELL LABS TECHNICAL JOURNAL,US,BELL LABORATORIES, vol. 3, no. 3, 1 July 1998 (1998-07-01), pages 79-97, XP000782375 ISSN: 1089-7089 the whole document -----	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/EP 01/04181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1109416 A	20-06-2001	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

Espacenet

Bibliographic data: WO02082728 (A1) — 2002-10-17

METHOD AND TELECOMMUNICATIONS SYSTEM FOR MONITORING A DATA FLOW IN A DATA NETWORK

Inventor(s): STIFTER HELMUT [DE]; PFAEHLER WOLFGANG [DE]; KREUSCH NORBERT [DE] + (STIFTER, HELMUT, ; PFAEHLER, WOLFGANG, ; KREUSCH, NORBERT)

Applicant(s): SIEMENS AG [DE]; STIFTER HELMUT [DE]; PFAEHLER WOLFGANG [DE]; KREUSCH NORBERT [DE] + (SIEMENS AKTIENGESELLSCHAFT, ; STIFTER, HELMUT, ; PFAEHLER, WOLFGANG, ; KREUSCH, NORBERT)

Classification: **- international:** ***H04L12/26; H04L29/06; H04L29/08; H04M3/22;*** (IPC1-7): H04L12/26; H04L29/06

- cooperative: **H04L12/2602**; **H04L29/06**; **H04L43/00**; **H04L63/00**; **H04L63/30**; **H04L65/103**; **H04L65/1046**; **H04L65/80**; **H04L67/2814**; **H04L67/306**; **H04M3/2281**; H04L29/06027; H04L67/2819; H04L67/2842; H04L69/329; H04M7/006

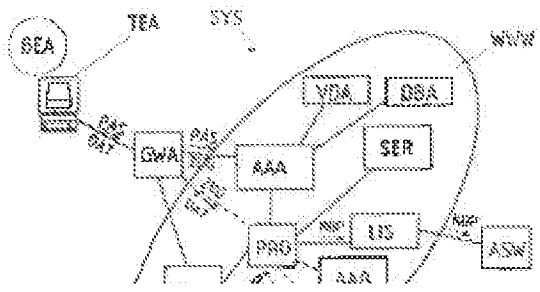
Application number: WO2002EP02524 20020307

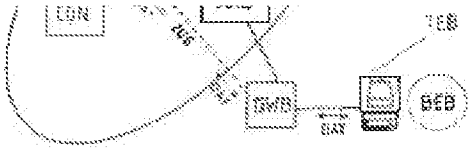
Priority number(s): EP20010107063 20010321

Also published as: EP1244250 (A1) US2004181599 (A1) US7979529 (B2) RU2003130974 (A) RU2280331 (C2) EP1371173 (A1) EP1371173 (B1) CN1498482 (A) CN1274114 (C) BR0208272 (A) less

Abstract of WO02082728 (A1)

The invention relates to a method and telecommunications system (SYS) for monitoring a data flow (DAT) in a data network (WWW) between at least two telecommunications terminals (TEA, TEB), which are connected to the data network via at least one access server





(AAA, AAB). When monitoring, the data flow (DAT) between the telecommunications terminals (TEA, TEB) is rerouted from the access server (AAA, AAB) via a monitoring server (PRO), which makes a copy (KOP) of the data flow (DAT) and transmits it to an evaluation unit (ASW).

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
17. Oktober 2002 (17.10.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/082728 A1

(51) Internationale Patentklassifikation[7]: H04L 12/26, 29/06

(21) Internationales Aktenzeichen: PCT/EP02/02524

(22) Internationales Anmeldedatum:
7. März 2002 (07.03.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
01107063.8 21. März 2001 (21.03.2001) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **STIFTER, Helmut** [DE/DE]; Taulerstr. 12, 81739 München (DE). **PFÄHLER, Wolfgang** [DE/DE]; Veltenstr. 16, 85221 Dachau (DE). **KREUSCH, Norbert** [DE/DE]; Ammerseestr. 4, 82061 Neuried (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

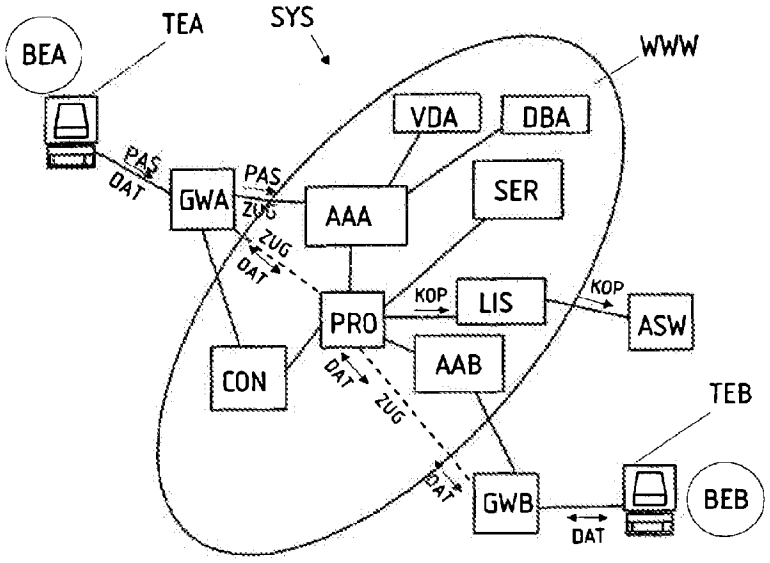
(81) Bestimmungsstaaten *(national)*: BR, CN, RU, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND TELECOMMUNICATIONS SYSTEM FOR MONITORING A DATA FLOW IN A DATA NETWORK

(54) Bezeichnung: VERFAHREN UND TELEKOMMUNIKATIONSSYSTEM ZUR ÜBERWACHUNG EINES DATENSTROMS IN EINEM DATENNETZ



(57) Abstract: The invention relates to a method and telecommunications system (SYS) for monitoring a data flow (DAT) in a data network (WWW) between at least two telecommunications terminals (TEA, TEB), which are connected to the data network via at least one access server (AAA, AAB). When monitoring, the data flow (DAT) between the telecommunications terminals (TEA, TEB) is rerouted from the access server (AAA, AAB) via a monitoring server (PRO), which makes a copy (KOP) of the data flow (DAT) and transmits it to an evaluation unit (ASW). .

[Fortsetzung auf der nächsten Seite]

WO 02/082728 A1

Erklärungen gemäß Regel 4.17:

hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten BR, CN, RU, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR)

..... *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

..... *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Ein Verfahren und ein Telekommunikationssystem (SYS) zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest zwei Telekommunikationsendgeräten (TEA, TEB), die über zumindest einen Zugangsserver (AAA, AAB) mit dem Datennetz verbunden sind, wobei von dem Zugangsserver (AAA, AAB) in einem Überwachungsfall der Datenstrom (DAT) zwischen den Telekommunikationsendgeräten (TEA, TEB) über einen Überwachungsserver (PRO) umgeleitet wird, der eine Kopie (KOP) des Datenstroms (DAT) erstellt und an eine Auswerteeinheit (ASW) übermittelt.

Beschreibung

Verfahren und Telekommunikationssystem zur Überwachung eines Datenstroms in einem Datennetz

Die Erfindung betrifft ein Verfahren zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

Weiters betrifft die Erfindung ein Telekommunikationssystem, welches zur Überwachung eines Datenstroms in einem Datennetz zwischen zumindest einem Telekommunikationsendgerät, welches über zumindest ein Gateway mit dem Datennetz verbunden ist und zumindest einer weiteren Telekommunikationseinrichtung eingerichtet ist, wobei zumindest ein Authentifikationsserver vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle zum Datennetz durchzuführen.

Von Gesetzgebern wird in zunehmenden Maß verlangt, dass Betreiber von Datennetzen Funktionen zur Verfügung stellen, die es ermöglichen im Bedarfsfall den Datenaustausch einzelner Benutzer zu überwachen.

Das legale Abhören von Datenströmen die sogenannte „Lawful Interception" in Datennetzen, beispielsweise dem Internet, wird zur Zeit unterschiedlich gelöst.

Eine bekannte Methode besteht darin, externe Sniffer (Analysatoren) in einem LAN-Segment des zu Überwachenden anzuordnen, welche den gesamten Paket-Datenstrom analysieren und den Verkehr des Überwachten ausfiltern, vervielfältigen und dem Bedarfsträger zustellen. Nachteilig an dieser Methode ist vor allem, dass ein zeitlich befristeter, physikalischer Eingriff

in das Netz erforderlich ist. Bei erhöhter Mobilität des zu Überwachenden ist diese Methode praktisch nicht verwendbar.

Eine andere Methode, die vor allem zum Abhören/Überwachen des e-Mailverkehrs dient, sieht vor, dass an einem oder mehreren e-Mailservern eine automatische Weiterleitungsfunktion implementiert ist, die sowohl ankommende als auch abgehende e-Mails dem Bedarfsträger, beispielsweise eine Behörde, zustellt. Ähnliches gilt für Voice-Mail etc. Bei dieser Methode ist es erforderlich, dass alle e-Mailserver dazu eingerichtet sein müssen, einen Abhör/Überwachungsfall zu erkennen und an die zuständige Behörde weiterzuleiten, was mit einem hohen administrativen Aufwand verbunden sein kann.

Aus der WO 0042742 sind eine Überwachungsmethode und ein Überwachungssystem zur Durchführen eines gesetzlichen Abhorchens in einem paketorientierten Netz, wie dem GPRS- oder dem UMTS-Netz beschrieben. Hierzu ist ein erst Netzelement mit Überwachungsfunktionalität für Datenpakete vorgesehen, welches durch ein zweites Netzelement gesteuert wird. Die abgefangenen (überwachten) Daten werden über ein Gateway, welches eine Schnittstelle zu einer zum Abhören berechtigten Behörde darstellt. Nachteilig an dieser Methode ist vor allem, dass auch Datenströme von Benutzern, die nicht abgehört werden sollen durch das Netzelement geführt werden, wodurch sich der technische und administrative Aufwand dieser Methode wesentlich erhöht.

Zur „Lawful Interception" im Internet siehe beispielsweise ETSI TR 101 750 V1.1.1.

Nicht außer Acht zu lassen sind die sehr hohen Kosten, die üblicherweise für einen Netzbetreiber bei zur Verfügungstellung der oben erwähnten Abhör/Überwachungsfunktionalität anfallen, die vor allem durch einen hohen administrativen Aufwand verursacht werden.

Es ist daher eine Aufgabe der Erfindung einen Weg zu schaffen, der es auf einfache und kostengünstige Weise ermöglicht, eine Abhör/Überwachungsfunktion in einem Datennetz zu implementieren und anzubieten.

Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art dadurch gelöst, dass von dem zumindest einem Authentifikationsserver überprüft wird, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei in einem Überwachungsfall eine Kopie des Datenstroms erstellt wird, welcher eine Identifikationskennzeichnung beigefügt wird, und die Kopie samt Identifikationskennzeichnung hierauf an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit übermittelt wird.

Es ist ein Verdienst der Erfindung, eine Abhörfunktionalität von seiten des Netzes zur Verfügung zu stellen, wodurch ein Eingriff mittels externer Abhörgeräte in das Netz vermieden werden kann. Weiters ist ein Zugriff auf einen Datenstrom eines zu Überwachenden auch dann möglich, wenn er mobil ist und seinen Standort ändert, da er sich über den Authentifizierungsserver eines Providers, der die Maßnahmen zur Überwachung setzt, einwählen muss.

In einer Variante der Erfindung wird die Kopie von dem Gateway erstellt.

Eine andere Variante der Erfindung sieht vor, dass die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver erstellt wird.

Vorteilhafterweise stellt der LI-Server anhand einer Identifikationskennzeichnung fest, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll(en).

Günstigerweise erstellt der LI-Server die zumindest eine Sekundärkopie, d.h. der LI-Server vervielfältigt die Kopie entsprechend der Anzahl der berechtigten Stellen.

Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server eine Schnittstellenanpassung zu der Auswerteeinheit durchführt.

Der Authentifizierungsserver kann anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwachungskennzeichnung feststellen, ob ein Überwachungsfall vorliegt.

Die verborgene Datenbank steht mit einer Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet wird.

Im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank werden auch die zugeordneten Überwachungskennzeichnungen in der verborgenen Datenbank gelöscht.

In einer weiteren Variante der Erfindung wird der Datenstrom als Voice over IP-Datenstrom übertragen, wobei ein Call-Controller den Datenstrom über den Überwachungsserver, der die Kopie erstellt, umleitet.

Eine andere Möglichkeit besteht darin, dass der Authentifizierunsserver in einem Überwachungsfall den Datenstrom über den Überwachungsserver umleitet.

Eine Variante des Umleitens besteht darin, dass der Datenzugang von dem Gateway zu dem Überwachungsserver durchgetunnelt wird.

Um einen Datenverlust zu vermeiden, falls die Kopie nicht sofort an einen Bedarfsträger zugestellt werden kann, kann die Kopie des Datenstroms auf dem Überwachungsserver und/oder auf dem LI-Server zwischengespeichert werden.

In einer bevorzugten Ausführungsform der Erfindung steuert der Controller sowohl das Gateway als auch den Überwachungsserver.

Eine weitere sehr vorteilhafte Ausführungsform der Erfindung sieht vor, dass der zumindest eine Authentifizierungsserver den Überwachungsserver steuert.

Zur Durchführung des erfindungsgemäßen Verfahrens eignet sich insbesondere ein Telekommunikationssystem der eingangs genannten Art, bei welchem der Authentifikationsserver dazu eingerichtet ist, zu überprüfen, ob der Datenstrom zwischen dem zumindest einem Telekommunikationsendgerät und der zumindest einen weiteren Telekommunikationseinrichtung überwacht werden soll, wobei das Telekommunikationssystem dazu eingerichtet ist, in einem Überwachungsfall eine Kopie des Datenstroms zu erstellen und der Kopie eine Identifikationskennzeichnung hinzuzufügen und die Kopie samt Identifikationskennzeichnung an zumindest einen LI-Server und/oder direkt an eine Auswerteeinheit zu übermitteln.

In einer ersten Variante der Erfindung ist das Gateway dazu eingerichtet, die Kopie des Datenstroms zu erstellen.

Bei einer zweiten Variante der Erfindung ist ein Überwachungsserver vorgesehen, der dazu eingerichtet ist, die Kopie zu erstellen.

Weiters ist der LI-Server dazu eingerichtet, anhand der Identifikationskennzeichnung festzustellen, ob zumindest eine Sekundärkopie der Kopie erstellt werden soll, und an wen die

Kopie und/oder die zumindest eine Sekundärkopie zugestellt werden soll(en).

Günstiger Weise ist der LI-Server dazu eingerichtet, die zumindest eine Sekundärkopie zu erstellen.

Weitere Vorteile lassen sich dadurch erzielen, dass der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit durchzuführen.

Der Authentifizierungsserver kann dazu eingerichtet sein, anhand einer dem zumindest einen Telekommunikationsendgerät in einer verborgenen Datenbank zugeordneten Überwachungskennzeichnung festzustellen, ob ein Überwachungsfall vorliegt.

Die verborgene Datenbank und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten sind dazu eingerichtet, Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung in der verborgenen Datenbank zugeordnet ist.

Das Telekommunikationssystem kann dazu eingerichtet sein, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank zugeordnete Überwachungskennzeichnungen in der verborgenen Datenbank zu löschen.

In einer vorteilhaften Variante der Erfindung, ist der Datenstrom ein Voice over IP-Datenstrom, wobei ein Call-Controller vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

Eine andere günstige Variante sieht vor, dass der Authentifizierungsserver dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom über den Überwachungsserver umzuleiten.

Weitere Vorteile lassen sich dadurch schaffen, dass das Telekommunikationssystem dazu eingerichtet ist, den Datenzugang von dem Gateway zu dem Überwachungsserver durchzutunneln.

Um einem Datenverlust vorzubeugen können der Überwachungsserver und/oder der LI-Server dazu eingerichtet sein, die Kopie des Datenstroms zwischenzuspeichern.

Weiters kann der Call-Controller dazu eingerichtet sein, sowohl das Gateway als auch den Überwachungsserver zu steuern.

In einer anderen Variante ist der Authentifizierungsserver dazu eingerichtet, den Überwachungsserver zu steuern. Günstigerweise weist der Überwachungsserver die Funktionalität eines Proxy-Servers auf.

Die Erfindung samt weiterer Vorteile ist im folgenden anhand einiger nicht einschränkender Ausführungsbeispiele, die in der Zeichnung veranschaulicht sind dargestellt, in dieser zeigen schematisch:

Fig. 1 ein erfindungsgemäßes Telekommunikationssystem,

Fig. 2a eine Kopie eines Datenstroms mit einer Identifikationskennzeichnung,

Fig. 2b die Identifikationskennzeichnung aus Fig. 2a im näheren Detail und

Fig. 3 einen beispielsweisen Ablauf des erfindungsgemäßen Verfahrens.

Gemäß Fig. 1 muss sich jeder Benutzer BEA, BEB, eines erfindungsgemäßen Telekommunikationssystems SYS der über sein Telekommunikationsendgerät TEA bzw. Telekommunikationseinrichtung TEB Zugang zu einem Datennetz WWW, beispielsweise dem Internet, haben will, über ein Gateway GWA, GWB einwählen bzw. sich bei einem Zugangsserver AAA anmelden. Unter einer

Telekommunikationsvorrichtung wird in diesem Dokument jede Art von Telekommunikationsendgerät, wie beispielsweise ein mit dem Datennetz verbundener PC, bzw. auch Server, die in dem Datennetz WWW stehen können, verstanden.

Der Zugangsserver AAA, AAB kann als AAA-Server oder als Remote Authentication Dial-In User Service Server kurz RADIUS-Server ausgebildet sein. Um einen Datenzugang ZUG dem Datennetz WWW zu erlangen, ist es für einen Benutzer erforderlich sich zu authentifizieren.

Die Authentifikation eines Benutzers BEA, BEB kann dabei über Eingabe eines Passwortes PAS bzw. einer Benutzeridentifikation, beispielsweise des Namens des Benutzers, erfolgen.

Anhand des Identifikationsergebnisses entscheidet der Zugangsserver AAA, AAB, ob einen Datenzugang ZUG zu dem Datennetz WWW gewährt oder verweigert wird.

Die Authentifikation des Benutzers BEA, BEB kann von seiten des Zugangsservers AAA mittels Abfrage einer Verwaltungsdatenbank VDA, in der die Benutzerdaten verwaltet werden erfolgen.

Liegt ein positives Authentifizierungsergebnis vor, so wird eine verborgene Datenbank abgefragt, in der jedem in der Verwaltungsdatenbank eingetragenen Benutzer eine Überwachungskennzeichnung UWD zugeordnet ist. Besagt die Überwachungskennzeichnung UWD, dass ein Datenstroms DAT zwischen dem Telekommunikationsendgerät TEA des Benutzer BEA und einem weiteren Telekommunikationsendgerät durchgeführt werden soll, so wird eine Kopie KOP des Datenstromes DAT angefertigt.

Die Kopie KOP des originalen Datenstromes DAT kann beispielsweise von dem Gateway GWA, welches dem Telekommunikationsendgerät TEA zugeordnet ist, oder von einem eigens hierfür vorgesehenen Überwachungsserver PRO erstellt werden.

Für den Fall, dass der Überwachungsserver PRO die Kopie des originalen Datenstromes DAT erstellt, wird der Datenstrom DAT zwischen über den Überwachungsserver PRO umgeleitet. Bevorzugter Weise weist dieser Server Proxyfunktionalität auf. Der Überwachungsserver PRO unterscheidet sich von einem Proxy-Server lediglich dadurch, dass der Überwachungsserver PRO dazu eingerichtet ist, die Kopie KOP eines über ihn laufenden (umgeleiteten) Datenstroms DAT zu erstellen und diese Kopie mit einer mitgelieferten Identifikationskennzeichnung IDK (Fig. 2), beispielsweise der IP-Adresse oder einer verschlüsselten Kennzeichnung des abzuhörenden Benutzers, zu versehen und an einen „Lawful Interception"-Server oder kurz LI-Server LIS zu übermitteln, wobei der originale Datenstrom an die durch den Benutzer bestimmte Zieladresse weitergeroutet wird.

Erstellt das Gateway GWA die Kopie KOP, so ist die soeben beschriebene Funktionalität des Kopierens und Weiterleitens der Kopie KOP an den LI-Server bzw. des Routens des originalen Datenstromes DAT gemäß der benutzerbestimmten Zieladresse in dem Gateway GWA realisiert.

Ein Datenzugang ZUG zu dem Datennetz WWW kann im Überwachungsfall für den zu überwachenden Benutzer BEA direkt über das Gateway und den Überwachungsserver PRO erfolgen.

Die Umleitung des Datenstromes DAT an den Überwachungsserver PRO kann mittels Tunneling, beispielsweise gemäß dem in der RFC 2661 spezifizierten L2T-Protokolls erfolgen.

Eine andere Möglichkeit den Datenstrom DAT über den Überwachungsserver PRO umzuleiten besteht darin, dass dem Überwachungsserver PRO eine Adresse in dem Datennetz zugeordnet wird, im Fall des Internet eine IP-Adresse. Diese Adresse kann in einer Speichereinheit des Zugangsservers AAA, AAB abgelegt sein, wobei im Überwachungsfall der Datenstrom DAT, beispielsweise gemäß dem TCP/IP-Protokolls, an die Adresse des Überwachungsservers PRO weitergeleitet wird.

Der Überwachungsserver PRO erstellt sodann, wie bereits oben erwähnt, eine Kopie KOP des über ihn umgeleiteten Datenstroms DAT und übermittelt diese Kopie KOP an einen LI-Server, der anhand der Identifikationskennzeichnung IDK, welche der Kopie beigefügt ist, entscheidet was mit der Kopie KOP zu geschehen hat, beispielsweise ob weitere Kopien d.h. Sekundärkopien WKO der Kopie erstellt werden sollen bzw. an welche Auswerteeinheit(en) die Kopie(n) zu übermitteln ist (sind).

Die weitere Verarbeitung und Auswertung der Kopie KOP erfolgt dann in der Auswerteeinheit ASW, beispielsweise einem dazu eingerichteten PC einer Behörde.

Der LI-Server LIS ist üblicherweise eine Anordnung mehrerer Workstations. Seine Aufgabe ist es, wie bereits oben erwähnt, die Kopie KOP des Datenstromes DAT zu empfangen, die der Kopie KOP von dem Überwachungsserver beigefügte Identifikationskennzeichnung IDK auszuwerten, gegebenenfalls weitere Kopien WKO der Kopie KOP herzustellen und an die Bedarfsträger zuzustellen.

Auch ist der LI-Server dazu eingerichtet, eine Schnittstellenanpassung zu unterschiedlichen Auswerteeinheiten ASW der Bedarfsträger durchzuführen. So kann es beispielsweise notwendig sein für eine Überwachung zwei H.323 Verbindungen zu einem bekannten Time Division Multiplex oder kurz TDM-Übergabe-Interface der überwachenden Behörde herzustellen. Eine andere Möglichkeit besteht darin, die Kopie über ein IP-Übergabe Interface an die überwachende Behörde zuzustellen.

Die Informationen, die der LI-Server LIS benötigt, um die Kopie an den Bedarfsträger bzw. die Auswerteeinheit ASW weiterzuleiten, können von Seiten der Bedarfsträger in einer Datenbank LID abgelegt werden.

Eine weitere Möglichkeit besteht darin, dass die Kopie KOP samt der Identifikationskennzeichnung IDK von dem Überwachungsserver PRO bzw. Gateway GWA direkt an die Auswerteeinheit ASW zugestellt wird.

Nach dem Erstellen der Kopie KOP des Datenstroms DAT, wird der originale Datenstrom DAT von dem Überwachungsserver PRO auf die herkömmliche Weise, beispielsweise gemäß dem TCP/IP-Protokoll, an den zweiten Benutzer BEB bzw. die Telekommunikationseinrichtung TEB, SER weitergeroutet.

Nach Fig. 2a wird der Kopie KOP des Datenstromes DAT eine Identifikationskennzeichnung IDK als Header vorangestellt. Die Identifikationskennzeichnung kann zumindest einen IP-Header IPH aufweisen, beispielsweise die IP-Adresse des überwachten Benutzers BEA. Weiters kann ein spezieller LI-Header LIH vorgesehen sein (Fig. 2b), der Informationen betreffend die weitere Datenübermittlung für den LI-Server enthält. So kann beispielsweise die erste Zeile die Art TYP der Nachricht enthalten, ob es zum Beispiel um eine Sprachnachricht oder eine „abgehörte" e-Mail handelt. Eine nächste Zeile kann die Länge LEN des Headers enthalten, während in einer dritten Zeile eine Operator-ID OID gemäß dem Standard ETSI ES 201671 enthalten kann. Eine Rufidentifizierungsnummer CIN kann zur Identifizierung eines „abgehörten" Benutzers BEA dienen, während eine Behördenidentifizierung LID dazu dient den Bedarfsträger, an den die Kopie KOP zugestellt werden soll, zu identifizieren. Weitere Informationen SUP können an die soeben genannten im Bedarfsfall angehängt werden.

Gemäß Fig. 3 wird im Fall einer Sprachübertragung gemäß dem Voice over IP-Protokoll eine entsprechende Applikation APP auf dem Telekommunikationsendgerät TEA des Anrufers BEA gestartet, welches daraufhin eine Verbindung über ein erstes Gateway GWA zu einem ersten Zugangsserver AAA aufbaut. Dieser Zugangsserver AAA überprüft, welcher Teilnehmer den Dienst zur Sprachübertragung in Anspruch nehmen will, und ob dieser zur Inanspruchnahme dieses Dienstes berechtigt ist. Zu diesem Zweck findet eine H.323 oder RADIUS-Kommunikation zwischen dem Gateway GWA und dem Zugangsserver AAA statt.

Ist der anrufende Benutzer BEA zur Benutzung des Sprachdienstes berechtigt, so überprüft der Zugangsserver AAA anhand der Authentifizierung dieses Benutzers BEA, ob der Datenaustausch

zwischen dem Anrufer und einem Angerufenen überprüft werden soll.

Nach erfolgreicher Zugangsprüfung ermittelt der Call-Controller CON durch Kommunikation mit einem zweiten Zugangsserver AAB die IP-Adresse des angerufenen Telekommunikationsendgerätes TEB und veranlasst den Signalisierungsverkehr über ein weiteres Gateway GWB zu diesem Telekommunikationsendgerät TEB.

Ist nun der Anrufer zu überwachen, dann baut der Controller CON die Verbindung vom Gateway GWA nicht direkt zu dem angerufenen Telekommunikationsendgerät TEB auf, wie es üblicherweise der Fall ist, sondern schleift den Überwachungsserver PRO ein. D. h. die Verbindung von dem ersten Telekommunikationsendgerät TEA zu dem zweiten Telekommunikationsendgerät TEB wird in zwei Strecken zerlegt, nämlich in die Strecke von dem ersten Telekommunikationsendgerät TEA zum Überwachungsserver PRO und in die Strecke von dem Überwachungsserver PRO zu dem zweiten Telekommunikationsendgerät TEB.

Der Controller CON steuert im Normalfall das erste Gateway GWA. Da aber nun wegen der Überwachung der Zugang zum Datennetz WWW bis zu dem Überwachungsserver PRO verlängert wird und dort eigentlich erst das normale Routing für den Datenstrom DAT des Benutzers BEA anfängt, ist der Controller CON dazu eingerichtet, einen „Handover" vom Gateway zu dem Überwachungsserver durchführen. D. h. der Controller CON wird durch den ersten Zugangsserver AAA informiert, dass ein Überwachungsfall vorliegt und der Datenzugang ZUG des zu überwachenden Telekommunikationsendgerätes TEA zu einem Überwachungsserver PRO durchzutunneln ist. Der Controller betrachtet den Überwachungsserver PRO von nun an als „neues" erstes Gateway GWA und steuert diesen Server als ob es das Gateway GWA wäre. Im Überwachungsfall verhält sich der Call-Controller CON also so, als ob der Überwachungsserver PRO das Gateway GWA wäre, dies gilt sowohl für die rufende als auch die gerufene Seite.

Der Überwachungsserver PRO erstellt dann, wie bereits oben erwähnt, eine Kopie KOP des Datenstromes DAT zwischen den beiden Telekommunikationsendgeräten TEA, TEB. Zur Erstellung der Kopie KOP wird der ursprüngliche Datenstrom DAT in dem Überwachungsserver PRO verdoppelt. Der ursprüngliche Datenstrom DAT wird nach der Verdoppelung von dem Überwachungsserver PRO an das zweite Telekommunikationsendgerät TEB weitergeroutet, während die Kopie KOP des Datenstromes DAT, wie bereits oben erwähnt, an einen LI-Server oder eine Auswerteeinheit ASW übermittelt wird.

Der Überwachungsserver PRO als auch der LI-Server LIS können dazu eingerichtet sein, die Kopie KOP zwischenzuspeichern, um für den Fall, dass eine unmittelbare Zustellung an die Auswerteeinheit ASW nicht möglich ist, einen Datenverlust zu vermeiden.

Um ein Abhören ohne merkliche Beeinträchtigung der Qualität und der Geschwindigkeit des ursprünglichen Datenstroms DAT zu verwirklichen, sollte die Strecke zwischen dem Überwachungsserver PRO und dem Gateway GWA gering sein, weshalb es vorteilhaft ist, wenn eine große Anzahl von Überwachungsservern PRO in dem Datennetz WWW angeordnet sind.

Soll der angerufene Benutzer BEB überwacht werden erfolgt das Verfahren im wesentlichen so wie oben beschrieben, wobei der zweite Zugangsserver AAB anhand der IP-Adresse des gerufenen Teilnehmers BEB die Authentifizierung durchführen kann und den Datenstrom DAT über den Überwachungsserver PRO umleitet.

Zu Zweck der Authentifizierung des gerufenen Teilnehmers BEB anhand seiner IP-Adresse kann der zweite Zugangsserver AAB eine Datenbank DAB aufweisen, welche die IP-Adresse des gerufenen Teilnehmers und einen Eintrag ob dieser abgehört werden soll enthält.

Der Befehl zur Überwachung des Benutzers BEA von einer zur Überwachung berechtigten Behörde gegeben und in der versteckten Datenbank DBA eingetragen.

Wenn der überwachte Benutzer BEA eine Applikation zur Datenübertragung in dem Datennetz WWW auf seinem Telekommunikationsendgerät startet, erfolgt die Authentifizierung des Benutzers und die Feststellung ob ein Überwachungsfall vorliegt, wie bereits oben erwähnt.

Der A-Seite wird in einem Überwachungsfall anstelle der Adresse des gerufenen Benutzers BEB bzw. einer Telekommunikationseinrichtung TEB SER, wie beispielsweise einem Server, auf dem eine Homepage oder andere Daten abgelegt sind, die Adresse des Überwachungsservers PRO übermittelt. Das B-seitige Gateway GWB erhält von dem Authentifizierungsserver AAA oder Call-Controller CON anstelle der Netzwerkadresse des rufenden Benutzers BEA die Netzwerkadresse des Überwachungsservers PRO.

Der Überwachungsserver PRO wird von dem Authentifizierungsserver AAA oder Call Controler CON informiert, dass eine Überwachung stattfinden soll. Alle zur Überwachung und Verbindung notwendigen Informationen, z. B. „Verbinde die A-Seite mit der B-Seite" und ähnliche Informationen, können mittels H.248 Übertragung von dem Authentifizierungsserver AAA bzw. Call-Controler CON an den Überwachungsserver PRO übertragen werden.

In dem Überwachungsserver wird, wie bereits oben erwähnt,der Datenstrom DAT zwischen dem A-seitigen und B-seitigen Benutzer bzw. Server verdoppelt, wobei die verdoppelten Daten mit einer Identifikationskennzeichnung IDK versehen werden. Die so erstellte Kopie KOP wird in weiterer Folge an den LI-Server übermittelt.

Für den originalen Datenstrom funktioniert der Überwachungsserver wie ein Proxyserver und verbindet lediglich die A-Seite mit der B-Seite.

Eine andere Variante der Erfindung sieht vor, dass die A-Seite von dem Authentifizierungsserver AAA oder Call-Controler CON die Netzwerkadresse der B-Seite erhält, wobei das A-seitige Gateway mittels H.248-Übertragung dazu aufge-

fordert wird, den gesamten Datenverkehr, der von dem Benutzer BEA stammt, zu dem Überwachungsserver zu tunneln. Hierbei wird der B-Seite, deren Netzwerkadresse bekannt ist anstelle der Netzwerkadresse der A-Seite von dem Call-Controler die Adresse des Überwachungsservers PRO übermittelt.

Der Überwachungsserver PRO erhält von dem Call-Controler die entsprechenden Informationen für das Tunnneln und verbindet die A-Seite mit der B-Seite.

Die Vorteile des Tunnelns bestehen darin, dass für den überwachten Benutzer BEA die für das Umleiten des Datenstroms über den Überwachungsserver PRO notwendigen Adressänderungen nicht sichtbar sind.

Wenn der Überwachungsserver PRO von dem Authentifizierungsserver AAA, AAB oder dem Call-Controler über eine H.248 Kommunikation informiert wird, dass ein Datenstrom DAT umgeleitet wird, so kann er eine Startnachricht an den LI-Server übermitteln, sodass dieser die notwendigen Daten aus der LI-Datenbank LID abfragt und diese bei eintreffen der Kopie KOP schon zur Verfügung stehen.

Wenn der zu überwachende Datenaustausch beendet wird, dann informiert der Call-Controler CON den Überwachungsserver PRO, dass er die Kommunikation bezüglich der konkreten Überwachung mit dem LI-Server abbrechen soll. Nach Erhalt einer von dem Überwachungsserver PRO stammenden Beendigungsnachricht kann der LI-Server die aus LI-Datenbank stammenden Daten wieder löschen und die Kommunikation mit den Bedarfsträgern einstellen.

Patentansprüche

1. Verfahren zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB), wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
dadurch gekennzeichnet, dass von dem zumindest einem Authentifikationsserver (AAA, AAB) überprüft wird, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) erstellt wird, welcher eine Identifikationskennzeichnung (IDK) beigefügt wird, und die Kopie samt Identifikationskennzeichnung (IDK) hierauf an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) übermittelt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass die Kopie (KOP) von dem Gateway (GWA, GWB) erstellt wird.

3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass die Kopie von einem eigens hierfür vorgesehenen Überwachungsserver (PRO) erstellt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass der LI-Server anhand der Identifikationskennzeichnung (IDK) feststellt, ob zumindest eine Sekundärkopie (WKO) der Ko-

pie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll(en).

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der LI-Server (LIS) die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der LI-Server (LIS) eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchführt.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) anhand einer dem zumindest einem Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB) zugeordneten Überwachungskennzeichnung (UWD) feststellt, ob ein Überwachungsfall vorliegt.

8. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass die verborgene Datenbank (DBA, DBB) mit einer Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten in Verbindung steht und jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenem Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet wird.

9. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwa-

chungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) gelöscht werden.

10. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Datenstrom (DAT) als Voice over IP-Datenstrom übertragen wird.

11. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass ein Call-Controller (CON) den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet, der die Kopie (KOP) erstellt.

12. Verfahren nach Anspruch 3 bis 10, dadurch gekennzeichnet, dass der Authentifizierunsserver (AAA, AAB) in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umleitet.

13. Verfahren nach einem der Ansprüche 3 bis 11, dadurch gekennzeichnet, dass der Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchgetunnelt wird.

14. Verfahren nach einem der Ansprüche 3 bis 12, dadurch gekennzeichnet, dass die Kopie (KOP) des Datenstroms (DAT) auf dem Überwachungsserver (PRO) zwischengespeichert werden.

15. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Kopie des Datenstroms (DAT) auf dem LI-Server zwischengespeichert wird.

16. Verfahren nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, dass der Controller

(CON) sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) steuert.

17. Verfahren nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass der zumindest eine Authentifizierungsserver (AAA, AAB) den Überwachungsserver steuert.

18. Telekommunikationssystem, welches zur Überwachung eines Datenstroms (DAT) in einem Datennetz (WWW) zwischen zumindest einem Telekommunikationsendgerät (TEA), welches über zumindest ein Gateway(GWA, GWB) mit dem Datennetz (WWW) verbunden ist, und zumindest einer weiteren Telekommunikationseinrichtung (SER, TEB) eingerichtet ist, wobei zumindest ein Authentifikationsserver (AAA, AAB) vorgesehen ist, der dazu eingerichtet ist, eine Zugangskontrolle (ZUG) zum Datennetz (WWW) durchzuführen,
dadurch gekennzeichnet, dass der Authentifikationsserver (AAA, AAB) dazu eingerichtet ist, zu überprüfen, ob der Datenstrom (DAT) zwischen dem zumindest einem Telekommunikationsendgerät (TEA) und der zumindest einen weiteren Telekommunikationseinrichtung (SER, TEB) überwacht werden soll, wobei das Telekommunikationssystem (SYS) dazu eingerichtet ist, in einem Überwachungsfall eine Kopie (KOP) des Datenstroms (DAT) zu erstellen und der Kopie (KOP) eine Identifikationskennzeichnung (IDK) hinzuzufügen und die Kopie (KOP) samt Identifikationskennzeichnung (IDK) an zumindest einen LI-Server (LIS) und/oder direkt an eine Auswerteeinheit (ASW) zu übermitteln.

19. Telekommunikationssystem nach Anspruch 17, dadurch gekennzeichnet, dass das Gateway (GWA, GWB) dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zu erstellen.

20. Telekommunikationssystem nach Anspruch 17, dadurch gekennzeichnet, dass ein Überwachungsserver (PRO) vorgesehen ist, der dazu eingerichtet ist die Kopie (KOP) zu erstellen.

21. Telekommunikationssystem nach einem der Ansprüche 17 bis 19, dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, anhand der Identifikationskennzeichnung (IDK) festzustellen, ob zumindest eine Sekundärkopie (WKO) der Kopie (KOP) erstellt werden soll, und an wen die Kopie (KOP) und/oder die zumindest eine Sekundärkopie (WKO) zugestellt werden soll(en).

22. Telekommunikationssystem nach Anspruch 21, dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, die zumindest eine Sekundärkopie (WKO) der Kopie (KOP) zu erstellen.

23. Telekommunikationssystem nach einem der Ansprüche 17 bis 22, dadurch gekennzeichnet, dass der LI-Server, dazu eingerichtet ist eine Schnittstellenanpassung zu der Auswerteeinheit (ASW) durchzuführen.

24. Telekommunikationssystem nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, anhand einer dem zumindest einen Telekommunikationsendgerät (TEA) in einer verborgenen Datenbank (DBA, DBB) zugeordneten Überwachungskennzeichnung (UWD) festzustellen, ob ein Überwachungsfall vorliegt.

25. Telekommunikationssystem nach Anspruch 24, dadurch gekennzeichnet, dass die verborgene Datenbank (DBA, DBB) und eine dem Authentifizierungsserver zugeordnete Verwaltungsdatenbank (VDA, VDB) zur Verwaltung von Benutzerprofilen und Benutzerauthentifikationsdaten dazu eingerichtet sind Daten miteinander auszutauschen, wobei jedem in der Verwaltungsdatenbank (VDA, VDB) eingetragenen Benutzer (BEA, BEB) eine Überwachungskennzeichnung (UWD) in der verborgenen Datenbank (DBA, DBB) zugeordnet ist.

26. Telekommunikationssystem nach Anspruch 25, dadurch gekennzeichnet, dass es dazu eingerichtet ist, im Fall einer Löschung von Benutzerauthentifikationsdaten in der Verwaltungsdatenbank (VWA, VWB) zugeordnete Überwachungskennzeichnungen (UWD) in der verborgenen Datenbank (DBA, DBB) zu löschen.

27. Telekommunikationssystem nach einem der Ansprüche 17 bis 26, dadurch gekennzeichnet, dass der Datenstrom (DAT) ein Voice over IP-Datenstrom ist.

28. Telekommunikationssystem nach Anspruch 27, dadurch gekennzeichnet, dass ein Call-Controller (CON) vorgesehen ist, der dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

29. Telekommunikationssystem nach einem der Ansprüche 20 bis 28, dadurch gekennzeichnet, dass der Authentifizierunsserver (AAA, AAB) dazu eingerichtet ist, in einem Überwachungsfall den Datenstrom (DAT) über den Überwachungsserver (PRO) umzuleiten.

30. Telekommunikationssystem nach einem der Ansprüche 20 bis 29,
dadurch gekennzeichnet, dass es dazu eingerichtet ist, den Datenzugang (ZUG) von dem Gateway (GWA, GWB) zu dem Überwachungsserver (PRO) durchzutunneln.

31. Telekommunikationssystem nach einem der Ansprüche 20 bis 30,
dadurch gekennzeichnet, dass der Überwachungsserver dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

32. Telekommunikationssystem nach einem der Ansprüche 17 bis 31,
dadurch gekennzeichnet, dass der LI-Server dazu eingerichtet ist, die Kopie (KOP) des Datenstroms (DAT) zwischenzuspeichern.

33. Telekommunikationssystem nach einem der Ansprüche 28 bis 32,
dadurch gekennzeichnet, dass der Call-Controller (CON) dazu eingerichtet ist, sowohl das Gateway (GWA, GWB) als auch den Überwachungsserver (PRO) zu steuern.

34. Telekommunikationssystem nach einem der Ansprüche 29 bis 32,
dadurch gekennzeichnet, dass der Authentifizierungsserver (AAA, AAB) dazu eingerichtet ist, den Überwachungsserver zu steuern.

35. Telekommunikationssystem nach einem der Ansprüche 20 bis 34,
dadurch gekennzeichnet, dass der Überwachungsserver (PRO) die Funktionalität eines Proxy-Servers aufweist.

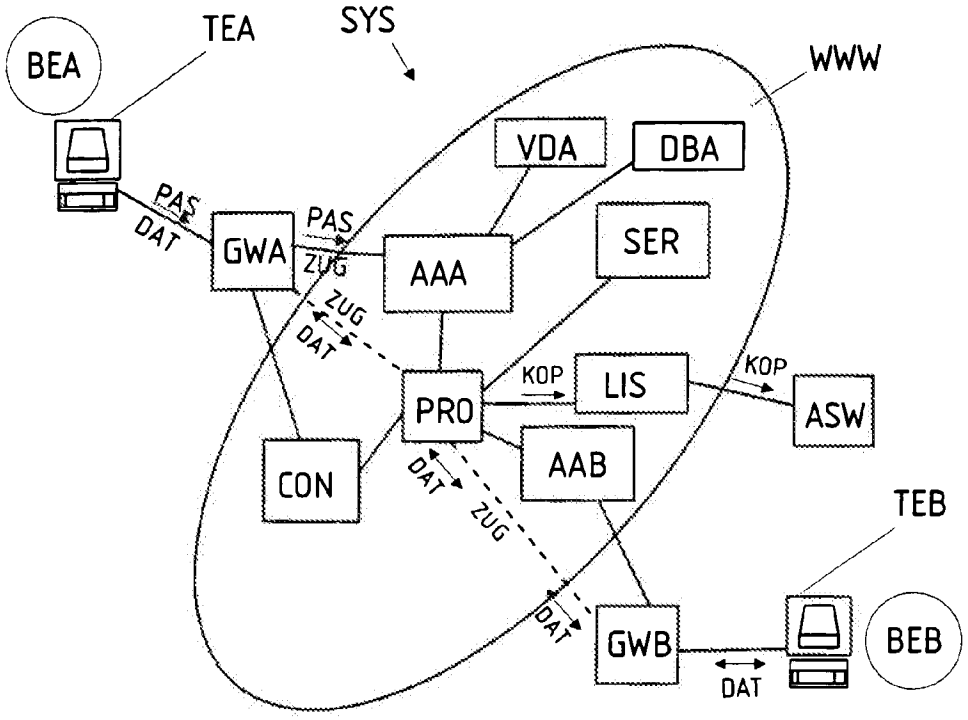

BEA
TEA
SYS
WWW
VDA
DBA
PAS
DAT
GWA
PAS
ZUG
AAA
SER
ZUG
DAT
KOP
LIS
KOP
ASW
PRO
AAB
CON
DAT
ZUG
TEB
DAT
GWB
BEB
DAT

Fig. 1

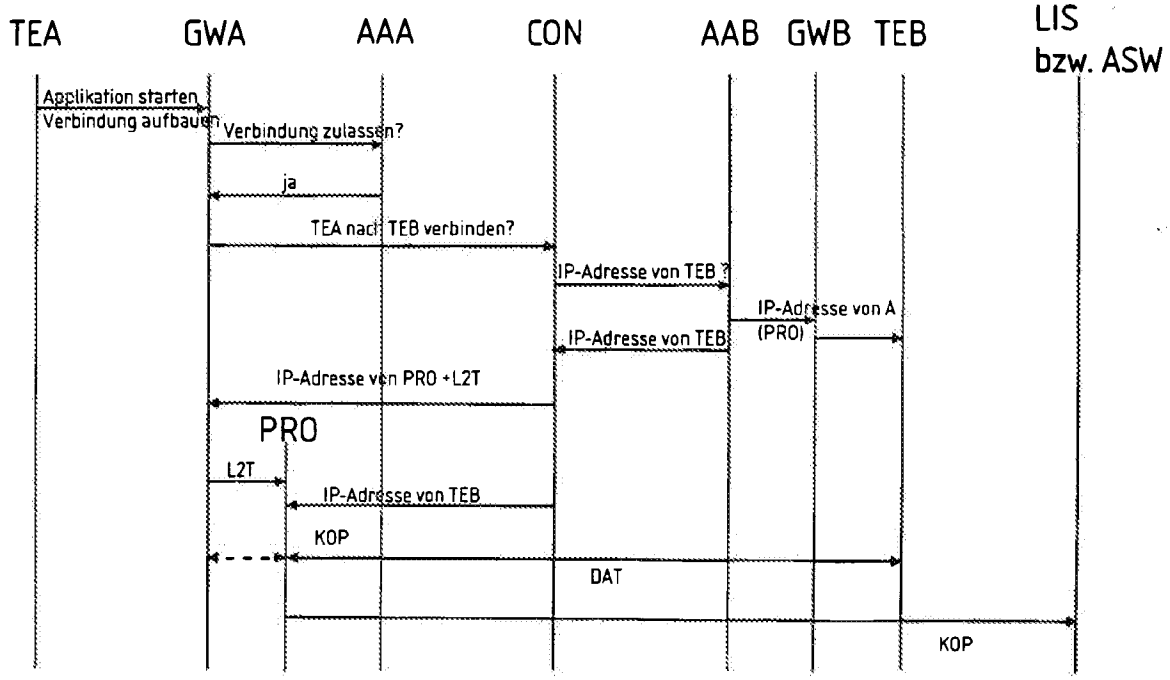

TEA
GWA
AAA
CON
AAB
GWB
TEB
LIS
bzw. ASW
Applikation starten
Verbindung aufbauen
Verbindung zulassen?
ja
TEA nach TEB verbinden?
IP-Adresse von TEB ?
IP-Adresse von A
(PRO)
IP-Adresse von TEB
IP-Adresse von PRO +L2T
PRO
L2T
IP-Adresse von TEB
KOP
DAT
KOP

Fig. 3

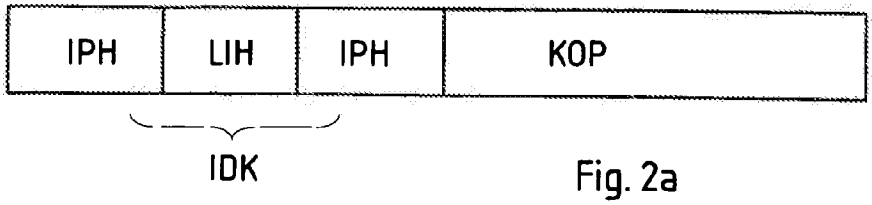


Fig. 2a

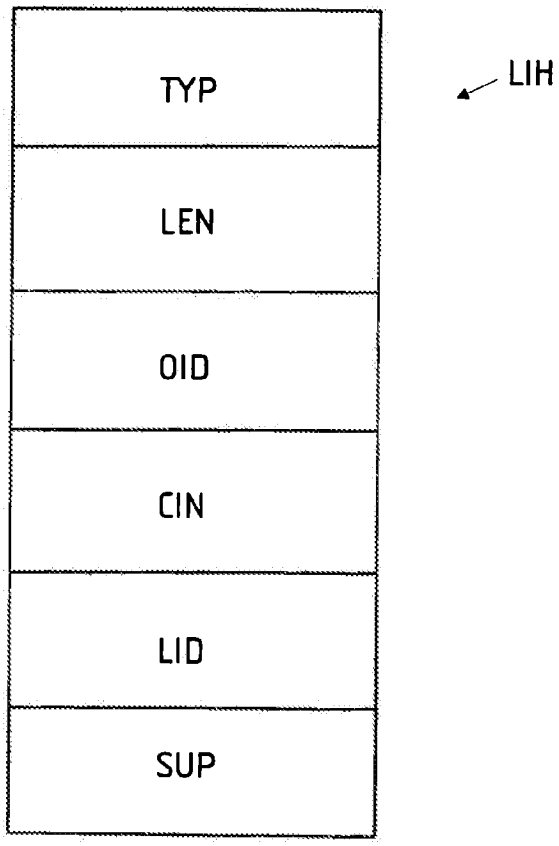


Fig. 2b

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/02524

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/26 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 56019 A (NOKIA NETWORKS OY ;ELORANTA JAANA (FI)) 21 September 2000 (2000-09-21) page 1, line 5 -page 1, line 19 page 7, line 27 -page 10, line 16 figures 1,2,4 --- -/--	1-3,7-9, 11-16, 18-20, 24-26, 28,30-33

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 August 2002	12/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Körbler, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 42742 A (NOKIA NETWORKS OY ;HIPPELAEINEN LASSI (FI)) 20 July 2000 (2000-07-20) page 2, line 18 -page 3, line 6 page 4, line 7 -page 4, line 32 page 6, line 4 -page 8, line 21 page 10, line 28 -page 11, line 14 figures 1-4	1-3,6-9, 11-16, 18-20, 23-26, 28,30-33
A	WO 99 55062 A (GTE GOVERNMENT SYST) 28 October 1999 (1999-10-28) page 3, line 3 -page 3, line 6	10,27
A	METZ CHRISTOPHER: "AAA Protocols: Authentication, Authorization, and Accounting for the Internet" IEEE INTERNET COMPUTING, 1999, pages 75-79, XP002176948 the whole document	1,7,8, 12,17, 18,24, 25,29,34

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 02/02524

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0056019 A	21-09-2000	WO 0056019 A1	21-09-2000
		AU 3035399 A	04-10-2000
		US 2002051457 A1	02-05-2002
WO 0042742 A	20-07-2000	WO 0042742 A1	20-07-2000
		AU 2617399 A	01-08-2000
		EP 1142218 A1	10-10-2001
		US 2002078384 A1	20-06-2002
WO 9955062 A	28-10-1999	AU 3865599 A	08-11-1999
		WO 9955062 A1	28-10-1999

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 02/02524

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L12/26 H04L29/06

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, IBM-TDB

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 00 56019 A (NOKIA NETWORKS OY ;ELORANTA JAANA (FI)) 21. September 2000 (2000-09-21) Seite 1, Zeile 5 -Seite 1, Zeile 19 Seite 7, Zeile 27 -Seite 10, Zeile 16 Abbildungen 1,2,4 --- -/--	1-3,7-9, 11-16, 18-20, 24-26, 28,30-33

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
1. August 2002	12/08/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Körbler, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 00 42742 A (NOKIA NETWORKS OY ;HIPPELAEINEN LASSI (FI)) 20. Juli 2000 (2000-07-20) Seite 2, Zeile 18 -Seite 3, Zeile 6 Seite 4, Zeile 7 -Seite 4, Zeile 32 Seite 6, Zeile 4 -Seite 8, Zeile 21 Seite 10, Zeile 28 -Seite 11, Zeile 14 Abbildungen 1-4 ---	1-3,6-9, 11-16, 18-20, 23-26, 28,30-33
A	WO 99 55062 A (GTE GOVERNMENT SYST) 28. Oktober 1999 (1999-10-28) Seite 3, Zeile 3 -Seite 3, Zeile 6 ---	10,27
A	METZ CHRISTOPHER: "AAA Protocols: Authentication, Authorization, and Accounting for the Internet" IEEE INTERNET COMPUTING, 1999, Seiten 75-79, XP002176948 das ganze Dokument -----	1,7,8, 12,17, 18,24, 25,29,34

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 02/02524

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 0056019	A	21-09-2000	WO	0056019 A1	21-09-2000
			AU	3035399 A	04-10-2000
			US	2002051457 A1	02-05-2002
WO 0042742	A	20-07-2000	WO	0042742 A1	20-07-2000
			AU	2617399 A	01-08-2000
			EP	1142218 A1	10-10-2001
			US	2002078384 A1	20-06-2002
WO 9955062	A	28-10-1999	AU	3865599 A	08-11-1999
			WO	9955062 A1	28-10-1999

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082782 A2

(51) International Patent Classification[7]: H04M

(21) International Application Number: PCT/US01/31548

(22) International Filing Date: 9 October 2001 (09.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/239,048 10 October 2000 (10.10.2000) US

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

(72) Inventors; and

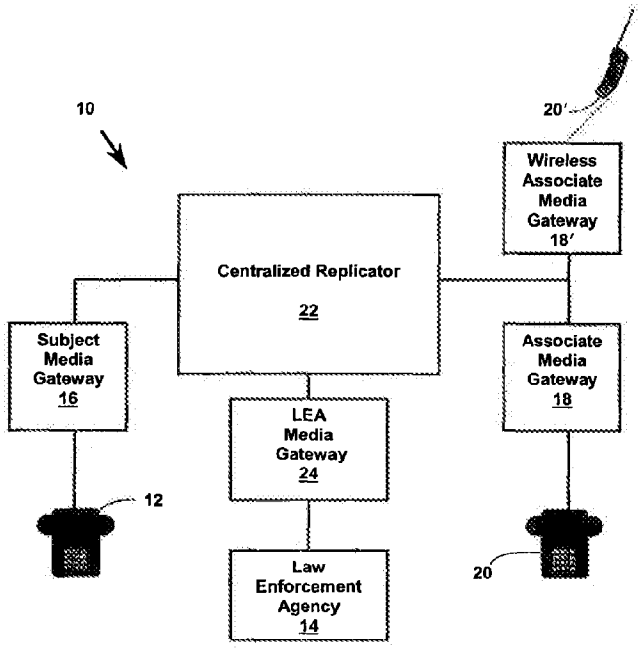
(75) Inventors/Applicants *(for US only)*: **PYKE, Craik, R.** [CA/CA]; 426A Moodie Drive, Nepean, ON K2H 8A6 (CA). **HERN, William** [GB/GB]; "Feliz" Whyteladyes Lane, Maidenhead, SL6 9LA (GB). **THOMPSON, Roger, L.** [US/US]; Dept. ND840, P.O. Box 13955, RTP, NC 27709 (US). **CARON, Serge, S.** [CA/CA]; 52 Limbour, Gatineau, PQ J8V 1X9 (CA). **MOUNJI, Halima, H.** [CA/CA]; 60 Hemlo Cres., Kanata, ON K2T 1E2 (CA). **EWOTI, Charles, B.** [DE/DE]; Oberer Garwiedenweg 2, 88677, Markdorf (DE). **GOERENS, Michael** [DE/DE]; Kenzelweg 17, 88045 Friedrichshafen (DE). **STRENG, Pete, J.** [CA/CA]; 5436 West River Drive, Manotick, ON K4M 1G5 (CA). **GOERTZEN, Christopher, J.** [CA/CA]; #10-1701 Blohm Drive, Ottawa, ON K1G 6N6 (CA). **KITTLITZ, Christian** [CA/CA]; 2-2418 Carlson Avenue, Ottawa, ON K1V 8G1 (CA). **TAYLOR, Richard, C.** [CA/CA]; P.O. Box 22, Manotick, ON K4M 1A2 (CA). **WELHAM, Michael** [DE/DE]; Bruckfelder Strasse 27, 88662 Lippertsreute (DE).

(74) Agent: **VYNALEK, John, H.**; Nortel Networks Inc., P.O. Box 13828, Research Triangle Park, NC 27709-3828 (US).

(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, EC, 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,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS



(57) Abstract: A system and method for intercepting a telecommunication signal are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload and adding a second header to replicated payload and directing the replicated payload to the address associated with the second.

WO 02/082782 A2

MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, 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, 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.

Cross Reference to Related Applications

This application claims priority to United States Provisional Patent Application serial number 60/239,048, filed October 10, 2000, entitled LAWFUL INTERCEPT VIA CENTRALIZED REPLICATOR and is incorporated herein by this reference.

Background of the Invention

In law enforcement, it is sometimes necessary to monitor an individual or group of individuals to support allegations of illegal activity. Indeed, many countries mandate that telecommunications service providers and equipment manufacturers provide a law enforcement agency the ability to perform lawful interception of telecommunications to and from a subject being monitored.

Historically, lawful intercept consisted of using alligator clips which a law enforcement agency would physically clip to, thereby tapping into, the telecommunication line of a subject (the monitored party) and monitor calls to or from an associate (a party calling or being called by the subject.)

There are two categories of intercept, call data and call content. Call data intercept includes monitoring call events, for example, monitoring if the subject originates a call, or if a call is terminated on the subject, or if a call is forwarded elsewhere. This type of monitoring, known as pen register, provides the phone number of both the person called and the person calling, along with call events and time-date stamps of when the events occurred. In contrast, call content includes the actual content of the call, i.e., the conversation that takes place, plus

call data. Call content is transmitted to the law enforcement agency in real time so that the law enforcement agency can monitor the conversation as it happens. This transmission must be transparent to the subject and the associates so that they are not aware that they are being monitored.

As telecommunications equipment evolved, modules were provided in the telecommunication switch that provided the law enforcement agency the ability to lawfully intercept telecommunications. For example in a Time Division Multiplexed (TDM) switch such as the Nortel Networks DMS -100, a switch network fabric provides an access point that allows a law enforcement agency to tap the subject's phone line. This type of centrally located access point is known as an Intercept Access Point (IAP). The resulting information is then provided to the law enforcement agency.

As telecommunications have evolved to packet based communications, to include Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) protocols, the changing architecture of the telecommunications switches has necessarily made the interception of content more difficult.

In September of 1998, the Federal Communications Committee (FCC) ruled that new TDM equipment must have lawful intercept capability built in. Moreover, in August of 1999 the FCC ruled that packet communications interception capability will be required by September 30, 2001.

Accordingly, there is a need to be able to intercept voice over packet communications in a manner that satisfies governmental requirements, is

transparent to the subject and the associate, in real time, and works with standard protocols such as IP and ATM applications.

Summary of the Invention

The invention results from the realization that a truly efficient and effective system and method for intercepting voice over packet communications is achieved in which a packet communication signal directed to or from a subject is received by a centralized replicator. The header is stripped from the packet leaving only the payload, the payload is replicated, a header is added to the replicated payload and the replicated payload is transmitted to a Law Enforcement Agency. A header is added to the original payload and the packet is retransmitted to the intended recipient. Alternatively, the entire packet can be replicated and the headers stripped off both the original packet and the replicated packet and a new header added to each payload. The payloads are then transmitted to the intended recipient and the Law Enforcement Agency.

In one embodiment, there is provided a method of intercepting a telecommunication signal including receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload, adding a new header to replicated payload and directing the replicated payload to the address associated with the new header.

It can be determined whether a telecommunication packet is to be monitored. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with the second predetermined header.

In another embodiment there is provided a system for intercepting a telecommunication signal. The system includes an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet comprising a predetermined header and a payload, a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to replicated payload and a relay point for directing the replicated payload to the address associated with the new header.

The new header can be associated with one of an intended recipient and a law enforcement agency. There can be a media gateway for directing the telecommunication signal to the audio server and also a media gateway controller, responsive to the media gateway, for determining that the telecommunication packet is to be intercepted. The media gateway controller can include a call discriminator, responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception. There can be a second termination point for adding a second predetermined header to

the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. There can be a second relay point for directing the payload to the address associated with the second predetermined header.

In yet another embodiment, there is provided a method for intercepting a telecommunication signal by receiving a telecommunication packet comprising a predetermined header and a payload, removing the predetermined header from the packet, replicating the payload, adding a new header to replicated payload and directing the replicated payload to the address associated with the new header.

It can be determined whether the telecommunication packet is to be intercepted. The new header can be associated with one of an intended recipient and a law enforcement agency. The predetermined header can be removed from the payload and replaced with a second predetermined header. This replacement can occur before or after replication of the payload. The second predetermined header can be associated with the other of the intended recipient and the law enforcement agency. The payload can be directed to the address associated with second predetermined header.

There is further provided a method of redirecting a telecommunication signal. The method includes receiving a telecommunication packet comprising a header and a payload, removing the predetermined header from the packet, adding a second predetermined header to payload and directing the replicated payload to the address associated with the second predetermined header.

It can be determined whether a telecommunication packet is to be redirected. The second predetermined header can be associated with one of an intended recipient and a law enforcement agency. The payload can be replicated. This replication can occur before or after the predetermined header is removed. A new header can be added to the replicated payload and the replicated payload can be directed to the address associated with second predetermined header. The new header can be associated with the other of the intended recipient and the law enforcement agency.

There is still further provided a method of monitoring a telecommunication signal to or from a subject being monitored from or to an associate. The method includes determining that a telecommunication signal is subject to being monitored, establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject, establishing a connection between the second gateway and a second termination point representing the first gateway and establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connection directly.

A connection can be established from at least one of the first termination point and the second termination point to a gateway associated with other than the subject and the associate concurrently with the connection between the first termination point and the second termination point.

There is provided even still further a method of redirecting a telecommunications signal intended for one of a subject and an associate by associating a first termination point with a first intended termination point of a first media gateway, associating a second termination point with a second intended termination point of a second media gateway, establishing a connection between the first intended termination point and the second termination point, establishing a connection between the second intended termination point and the first termination point and establishing a connection between the first termination point and the second termination point wherein the first intended termination point and the second termination point appear to be connected directly.

Brief Description of the Drawings

Figure 1 is a schematic block diagram generally representing a system for intercepting packet communications including a centralized replicator according to the present invention;

Figure 2 is a more detailed schematic block diagram, similar to Figure 1, including a media gateway controller associated with each media gateway for implementing the necessary connections to affect interception of packet communications;

Figure 3 is a schematic block diagram, similar to Figure 1, demonstrating the actual and ephemeral connections when implementing the call intercept according to one aspect of the present invention;

Figure 4 is a schematic block diagram demonstrating associated connections internal to the centralized replicator for affecting bearer channel tandeming for intercepting packet communications;

Figure 5 is a schematic block diagram representing bearer channel tandeming by the call discriminator in response to a requirement to intercept packet communications;

Figure 6 is a flow chart representing one method of intercepting packet communications according to the present invention;

Figure 7 is a schematic block diagram, similar to Figure 2, in which a second associate establishes a call to a subject being monitored and a call waiting feature is invoked;

Figure 8 is a schematic block diagram, similar to figure 4, demonstrating the connection topology within the centralized replicator when the call-waiting feature is invoked; and

Figure 9 is a schematic block diagram, similar to Figure 8, demonstrating the connection topology within the centralized replicator when a conference call feature is invoked.

Detailed Description

According to the present invention there is generally provided a system **10**, Figure 1, which can intercept a packet telecommunication signal to or from a subject **12** being monitored, for example, by a Law Enforcement Agency (LEA)

14. There is a first, or subject, media gateway **16** associated with subject **12** being monitored and a second, or associate, media gateway **18** associated with an associate **20** who is calling or being called by subject **12**. There can also be a wireless associate media gateway **18'** where an associate **20'** is communicating with subject **12** over a wireless phone.

A call is initiated between subject **12** and associate **20**. It is determined that the telecommunication signal is one targeted for monitoring and is to be intercepted. Accordingly, for a call from associate **20** to subject **18**, the telecommunication signal, rather than being sent directly to the intended associate media gateway **18**, is redirected from subject media gateway **16** to a centralized replicator **22** which may, for example, comprise a universal audio server associated with LEA **14**. When centralized replicator **22** receives the telecommunication signal, comprised of individual packets with each packet including a header and a payload, centralized replicator **22** removes the header from the packet leaving the payload intact. Centralized replicator **22** replicates the payload, adds a header to the replicated payload and transmits the replicated payload to a law enforcement agency gateway **24**. Once the payload has been replicated a header is added to the original payload and that packet is retransmitted by centralized replicator **22** to associate media gateway **18/18'** for delivery to associate **20/20'**.

Alternatively, the entire incoming packet can be replicated, including header and payload. Once the packet has been replicated, the headers of the original and replicated packets are removed. A new header is added to the

replicated payload for delivery to law enforcement agency **14** and a new header is added to the original payload for delivery to the respective intended recipient, subject **12** or associate **20.**

Referring now to Figure 2, associated with each media gateway **16**, **24** and **18**, can be a media gateway controller **26, 28** and **30**, respectively. As used herein, a media gateway controller refers to one or more devices whose functionality can include performing media gateway control signaling and call processing functions. Each associated gateway controller can include a call discriminator **32** comprising call processing software that determines that a call from or between associated gateways, for example subject media gateway **16** to associate media gateway **18**, is in fact subject to monitoring. There can be included within discriminator **32**, for example, a lawful intercept database that identifies subscribers, e.g., subject **12**, who are subject to a surveillance order.

Once it has been determined that the call is subject to monitoring, subject media gateway controller **26** sends a first message, for example using Media Gateway Control Protocol (MGCP) or H.248 protocol, to LEA media gateway **28** to effect a connection between subject media gateway **16** and centralized replicator **22** and another message to effect a connection between associate media gateway **18** and centralized replicator **22.** The redirection of the call through centralized replicator **22** is transparent to call processing and service functions and the call appears to be set up normally as if subject media gateway **16** and associate media gateway **18** were connected directly. The above example assumes that subject **12** and associate **20** do not share a common

gateway. However, a shared gateway would not change the operation of the subject invention as call discrimination and packet replication would take place in the same manner, transparent to the caller.

LEA Media gateway controller **28** effects redirection of the call from the intended recipient and instructs centralized replicator **22** to make internal connections, referred to as bearer channel tandeming, in order to facilitate packet replication as will be discussed further in reference to Figure 4. Once media gateway controller **28** has established the necessary connections between subject media gateway **16**, centralized replicator **22** and associate media gateway **18**, media gateway controller **28** initiates the connections between centralized replicator **22** and law enforcement agency media gateway **24** which is then connected to LEA **14.**

Accordingly, a call subject to monitoring will contain packets whose headers have been altered or substituted such that instead of the packets being transmitted to and from gateways **16** and **18** directly (the intended recipients), the packets are redirected to centralized replicator **22** for replication. Media gateway controller **28** alters the address information of the messages such that it appears to subject media gateway **16** that the message is coming from associate media gateway **18** and messages sent to associate media gateway **18** appear to come from subject media gateway **16**.

As shown in Figure 3, subject media gateway controller **26** sends a message **27** with the session description information, for example using a protocol such as the Session Description Protocol (SDP), of subject media

gateway **16** to LEA media gateway controller **28**. Media gateway controller **28** sends a message **29** including the session information of media gateway **16** to associate media gateway controller **30**, but with the address of centralized replicator **22**.

Similarly, associate media gateway controller **30** sends a message **31** acknowledging the session description of media gateway **16** with the session description of associate media gateway **18**. LEA media gateway controller **28** sends a message **33** acknowledging the session description of subject media gateway **16** with the session description of associate media gateway **18**, but with the address of centralized replicator **22**.

Accordingly, a communication path from subject media gateway **16** to associate media gateway **18** is tandemed through centralized replicator **22**, but is transparent to subject **12** or associate **20**.

Figure 4 further demonstrates how bearer channel tandeming can be accomplished through centralized replicator **22** by modifying the association between packet streams and endpoints to affect the connections and representations demonstrated in Figure 3.

Packet streams **34**, **36**, **38** and **40** originate from associated endpoints **42**, **44**, **46** and **48**, respectively. Accordingly, the respective transmit and receive streams **34/36** of endpoint **42**, while appearing to be associated with endpoint **46** (associate media gateway **18**), are associated with end point **44** within centralized replicator **22**. Similarly, respective transmit and receive streams **38/40** of endpoint **46** are associated with end point **48** while appearing to be

associated with end point **42** (subject media gateway **16**). Finally, internal streams **50** and **52** are associated with end points **44** and **48**. Connections to end points **42**, **44**, **46** and **48** are initiated from media gateway controller **28** (Figure 3) where endpoints **42** and **46** are the recognized originator and terminator endpoints.

Endpoints **42** and **46** are typically configured to convert the TDM information from subject **12** or associate **20** into, for example, IP or ATM packets or cells depending upon the fabric of centralized replicator **22**. Similarly, information received at these endpoints from centralized replicator **22** is converted from IP/ATM to TDM. In contrast, endpoints **44** and **48** within centralized replicator **22** are typically configured only as packet relay points and do not provide any transcoding or jitter correction in order to minimize latency and reduce the risk of detection by subject **12** or associate **20** of the monitoring. Flow control buffers (not shown) can be provided to avoid loosing packets.

Packet relay endpoints **44** and **48**, respectively, strip the header off incoming packet streams **34** and **38** that they receive from respective endpoints **42** and **46**, replicate the payload, add a new header to the replicated payload and transmit replicated packet streams **54** and **56** to law enforcement agency gateway **24** via endpoints **58** and **60**. Packet relay endpoints **44** and **48** also transmit the original payload via streams **50** and **52**, respectively, to each other, adding new headers directing the packets to respective gateways **16** and **18**. Alternatively, the entire packet may be replicated, then the replicated headers are

stripped off and new headers added to redirect the replicated packets to their respective gateways.

In order to ensure transparency to subject **12** and associate **20** of the intercept, streams **54** and **56** destined for law enforcement agency **14** should be unidirectional. Accordingly, endpoints **58** and **60** should be configured as send only in the direction of law enforcement agency gateway **24**. Endpoints **58**, **60** should be from the same resource pool as endpoints **44** and **48** so that the resource pools reflect what endpoints within centralized replicator **22** have internal connections between them so that media gateway controller **28** can send the appropriate connectivity messages to centralized replicator **22**. Accordingly, a resource manager **62** is provided. Moreover, endpoints **58** and **60**, as with packet relay endpoints **44** and **48**, should achieve a transmission time between endpoints that maintains low latency such that the total trip delay of the packets, including time to traverse centralized replicator 22, does not exceed the engineered threshold of the echo cancellers of the respective media gateways.

Resource manager **62** performs several basic functions to include allocation of resources, returning resources to a free pool and reporting on resources. Resource manager **62** can provide an interface to operating personnel to indicate what resources in centralized replicator **22** are to be used for bearer channel tandeming. The connection to law enforcement agency **14** can occur in several forms to include dedicated lines, switched local links, dedicated trunks or switched remote links without departing from the scope of the invention.

A monitoring point **64** within law enforcement agency **14**, which may include an audio device, can receive the call content via a TDM multiplexed mixing bridge **66**. Monitoring point **64** receives the call content in real time, thus at the same time subject **12** hears the ring from associate **20**, law enforcement agency **14** also hears the ring back. As will be apparent to those skilled in the art, law enforcement agency gateway **24** should be able to support all possible CODEC's that can be negotiated between a subject **12** and an associate **20**.

While system **10** has been described as only performing a single replication for a single law enforcement agency, it should be understood that this is not a limitation of the present invention, as the incoming packet streams can be replicated at endpoints **44** and **48** multiple times, depending on the number of law enforcement agencies monitoring subject **12**, by configuring the hardware comprising endpoints **44** and **48** for multiple replications.

Despite the changes in the connection messages as described above, neither subject **12** nor associate **20** are provided an indication that the call is being redirected through centralized replicator **22**.

When it is determined that a call is to be monitored, the standard connectivity message from the call server can either be altered to perform the appropriate connection or the message can be split into multiple messages to perform the requested connection.

By way of example, the connection operation from the call server requesting a connection between subject **12** and associate **20** is modified into three separate connectivity operations. This is done by requesting separate

connections from endpoints **42** and **44**, from endpoints **46** and **48** and from endpoints **44** to **48**.

As shown in Figure 5, a call agent or call processing **68**, in response to electronic surveillance software **69**, issues a connectivity message **70** to call discriminator **32** to make a subject to associate connection from a discriminator layer in connectivity software **72** to bearer channel tandeming connectivity software **74** which issues three separate media gateway control messages. A first message **76** can initiate a connection from subject media gateway **16** (Figure 4) to centralized replicator **22**. A second message **78** can initiate a connection from associate media gateway **18** to centralized replicator **22**. A third message **80** can instruct centralized replicator **22** to make an internal association between the centralized replicator **22** to subject media gateway **16** connection and the centralized replicator **22** to associate media gateway **18** connection.

Once the associated connection between subject **12** and associate **20** has been configured, media gateway controller **28** (Figure 3) initiates the respective connections to law enforcement media gateway **24** by requesting two connections from endpoints **44** to **58** and **48** to **60** (Figure 4) within centralized replicator **22** to law enforcement media gateway **24**, where endpoints **58** and **60** connect to law enforcement media gateway **24**, as illustrated in Figure 4 above.

A flowchart of the present invention is presented in Figure 6. A call is initiated between a subject and an associate, Block **82**. The media gateway controller associated with the subject being monitored determines that the call is to be monitored, Block **84**, and redirects the call to the media gateway controller

of the LEA by associating the LEA media gateway with the destination (associate) media gateway, Block **86**. The media gateway controller associated with the law enforcement agency effects bearer channel tandeming by associating the endpoints of the subject and associate media gateways with endpoints within the centralized replicator, Block **88**.

Once tandeming of the bearer channel has been affected, packets to and from the subject are redirected to the centralized replicator, Block **90**, where the payload is replicated, Block **92**, and new headers added to both the replicated payload and the original payload, Block **94**. The respective payloads are then transmitted to the recipient subject or associate and the LEA, Block **96**.

Figure 7 represents generally the situation where a call-waiting feature is invoked. For illustrative purposes, each agent is serviced by a different media gateway controller. A call is originated between subject **12** and first associate **20**, as discussed above, until subject **12** and first associate **20** enter the talking state as discussed above with the law enforcement agency **14** receiving the call content.

A second associate **20'** originates a call to subject **12**. Associate media gateway controller **30'** performs call processing routing the call to subject media gateway **16** and it is determined that the call is subject to interception. Centralized replicator **22** recognizes that subject **12** is engaged in an existing call. LEA media gateway controller **28** instructs media gateway **16** to play a call waiting tone to subject **12**.

Referring now to Figure 8, subject **12** invokes a feature flash to receive the call originated by second associate **20'**. Subject media gateway controller **26** (Figure 7) instructs centralized replicator **22** to break the connection between subject **12** and first associate **20**. However, Tandeming Connectivity software **74** (Figure 5) intercepts this message, and alters it to only break the connection between endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA **14** be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** remain in tact.

Tandeming Connectivity software **74** obtains two more endpoints **44'** and **48'** from resource manager **62** to tandem the call between subject **12**, second associate **20'** and LEA **14**. Tandeming Connectivity software **74** initiates a connection between end points **42** and **44'**. Tandeming Connectivity software **74** further initiates a connection between endpoints **44'** and **48'** within centralized replicator **22**. The session description information of endpoints **42** and **44'** are exchanged, and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel.

Subject media gateway controller **26** acknowledges endpoint **46'** and responds with the session information of endpoint **48'**, in order to facilitate the completion of the bearer channel configuration.

At this point a bearer channel is configured between end points **42** and **44'**, **44'** and **48'** and **48'**and **46'**. Subject **12** and second associate **20'** now enter

the talking state with law enforcement agency **14** receiving the call content. Second associate **20'** terminates the call and subject **12** invokes a feature flash to return to first associate **20**. Subject media gateway controller **26** sends a message to break the connection between subject **12** and the message is intercepted and altered to only break the connection between end points **42** and **44'**. The connection with Law enforcement agency **14** is also broken, but the connections between endpoints **44'** and **48'** and **48'** and **46'** remain intact. Second associate media gateway controller **30'** (not shown) passes a clear forward message to subject media gateway controller **26** instructing connectivity to break the connection with second associate **20'**. Tandeming Connectivity software **74** (Figure 5) intercepts the message and, determining that the other external agent has been removed from the bearer channel tandem, instructs a break of the connections between end points **44'** and **48'**, and **48'** and **46'**.

Endpoints **44'** and **46'** are returned to resource manager **62** to be reentered into the free pool. Subject media gateway controller **26** (Figure 7) sends a message to reestablish a connection between subject **12** and first associate **20**. Tandeming Connectivity software **74** (Figure 5) intercepts this message, determines the given communication is already associated with a tandemed connection, and retrieving the endpoints in use, issues connectivity messages to reestablish the connection between endpoints **42** and **44**.

The session information of end points **42** and **44** are exchanged as previously discussed completing the bearer channel tandem. Electronic Surveillance software **69** (Figure 5) requests notification of the endpoints being

used to tandem the bearer channel through centralized replicator **22**. Endpoints **58** and **60** are then connected to LEA media gateway **24** in order to provide capture of the call content. Subject **12** and associate **20** are again in a talking state through a bearer channel established via endpoints **42** and **44**, **44** and **48** and **48** and **46**.

Referring to Figure 7 once again, a conference call feature is established in a manner similar to call waiting. A call is originated between subject **12** and first associate **20**. Subject media gateway controller **26** determines that the call is subject to monitoring and bearer channel tandeming is initiated connecting subject media gateway **16** and associate media gateway **18** via centralized replicator **22** as discussed above by LEA media gateway controller **26** associating respective end points within centralized replicator **22** with subject media gateway **16** and associate media gateway **18**. A connection is then initiated between end points within centralized replicator **22**.

Associate media gateway **18** acknowledges the associated endpoint within centralized replicator **22**, as if it were acknowledging subject media gateway **16**, as discussed above with reference to Figure 3, and responds with the session description information of associate media gateway **18** and a bearer channel is configured between endpoints **42**, **44**, **46** and **48** (Figure 4).

A connection between law enforcement agency gateway **24** and end points within centralized replicator **22** as discussed in Figure 4 above, is established. Subject **12** and associate **20** now enter a talking state and law

enforcement agency **14** receives the replicated packet streams and monitors the call.

Referring again to Figure 8, subject **12** can invoke a flash feature and originate or receive a call with a second associate **20'**. Subject media gateway controller **26** (Figure 7) receives a message from the call agent of subject **12** to break the connection with first associate **20**, which is intercepted due to the bearer channel tandeming, and media gateway controller **28** sends a modified message to centralized replicator **22** (rather than to associate media gateway **18**) to break the connectivity of endpoints **42** and **44** (shown in phantom). Electronic Surveillance software **69** (Figure 5) further requests the connections with LEA 14 be broken and thus the connections between endpoint **44** and **58** and **48** and **60** are broken (shown in phantom), but the connection between endpoints **44** and **48** and **48** and **46** temporarily remain in tact.

With respect to the new caller, the media gateway determines that the call is subject to monitoring, and two more endpoints **44'** and **48'** within centralized replicator **22** are allocated by resource manager **62** and configured to tandem the call to second associate **20'**. A connection is then initiated between endpoints **42** and **44'** and media gateway controller **28** passes the endpoint of **48'** to the media gateway controller **30'** associated with second associate **20'**. A connection is then initiated between **44'** and **48'** within centralized replicator **22.** The session description information of **42** and **44'** are exchanged and the session description information of **44'** and **48'** are exchanged to facilitate the completion of the bearer channel tandeming.

At this point a bearer channel is configured between **42** and **44'**, **44'** and **48'**, and **48'** and **46'**. A connection is then initiated from centralized replicator **22** to LEA **14** via endpoints **44'**and **58'** and **48'** and **60'**. Subject **12** can now talk with second associate **20'** and LEA **14** can intercept the content. Subject **12** then invokes a feature flash to join first associate **20** in a three-way call. Connectivity software (Figure 5) requests that all connections associated with the previous legs be broken (shown in phantom) to enable the three-way call. Accordingly, the connection of end points **44** and **48**, **48** and **46** and **44'** and **48'** and **48'** and **46'** are broken along with the corresponding LEA connection and all resources are returned to the resource pool. Media gateway controller **28** requests a connection between subject **12**, first associate **20** and second associate **20'** through conferenced ports **98**, **100** and **102**, as shown in Figure 9.

Claims

What is claimed is:

1. A method of intercepting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a predetermined header and a payload;

(b) removing the predetermined header from the packet;

(c) replicating the payload;

(d) adding a new header to replicated payload; and

(e) directing the replicated payload to the address associated with the new header.

2. The method of claim 1 further comprising the step of determining that a telecommunication packet is to be monitored.

3. The method of claim 1 further comprising the step of associating the new header with one of an intended recipient and a law enforcement agency.

4. The method of claim 3 further comprising the step of replacing the predetermined header with a second predetermined header.

5. The method of claim 4 further comprising the step of associating the second predetermined header with the other of the intended recipient and the law enforcement agency.

6. The method of claim 4 in which the step of replacing occurs after the step of replicating.

7. The method of claim 5 further comprising the step of directing the payload to the address associated with the second predetermined header.

8. A system for intercepting a telecommunication signal, the system comprising:

(a) an audio server, responsive to a telecommunication signal, for receiving a telecommunication packet comprising a predetermined header and a payload;

(b) a termination point for removing the predetermined header from the packet, for replicating the payload and for adding a new header to replicated payload; and

(c) a relay point for directing the replicated payload to the address associated with the new header.

9. The system of claim 8 further comprising a media gateway for directing the telecommunication signal to the audio server.

10 The system of claim 8 in which the new header is associated with one of an intended recipient and a law enforcement agency.

11. The system of claim 9 further comprising a media gateway controller, responsive to a media gateway, for determining that a telecommunication packet is to be intercepted.

12. The system of claim 11 in which the media gateway controller includes a call discriminator, responsive to the telecommunications signal, for determining that the telecommunication signal is subject to interception.

13. The system of claim 12 further comprising a second termination point for adding a second predetermined header to the payload.

14. The system of claim 13 in which the second predetermined header is associated with the other of the intended recipient and the law enforcement agency.

15. The system of claim 14 further comprising a second relay point for directing the payload to the address associated with second predetermined header.

16. A method of intercepting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a predetermined header and a payload;

(b) removing the predetermined header from the packet;

(c) replicating the payload;

(d) adding a new header to replicated payload; and

(e) directing the replicated payload to the address associated with the new header.

17. The method of claim 16 further including the step of determining that a telecommunication packet is to be intercepted.

18. The method of claim 16 further comprising the step of associating the new header with one of an intended recipient and a law enforcement agency.

19. The method of claim 18 further including the step of replacing the predetermined header removed from the payload with a second predetermined header.

1 20. The method of claim 19 further comprising the step of associating the
2 second predetermined header with the other of the intended recipient and the law
3 enforcement agency.

1 21. The method of claim 19 in which the step of replacing occurs after the step
2 of replicating.

1 22. The method of claim 20 further comprising the step of directing the
2 payload to the address associated with second predetermined header.

23. A method of redirecting a telecommunication signal, the method comprising:

(a) receiving a telecommunication packet comprising a header and a payload;

(b) removing the predetermined header from the packet;

(c) adding a second predetermined header to payload; and

(d) directing the replicated payload to the address associated with the second predetermined header.

24. The method of claim 23 further comprising the step of determining that a telecommunication packet is to be redirected.

25. The method of claim 23 further comprising the step of replicating the payload.

26. The method of claim 25 wherein the step of replicating includes replicating the payload before the predetermined header is removed.

27. The method of claim 23 further comprising the step of associating the second predetermined header with one of an intended recipient and a law enforcement agency.

28. The method of claim 27 further comprising the step of adding a new header to the replicated payload.

29. The method of claim 28 further comprising the step of associating the new header with the other of the intended recipient and the law enforcement agency.

30. The method of claim 29 further comprising the step of directing the replicated payload to the address associated with the new header.

31. A method of monitoring a telecommunication signal to or from a subject being monitored from or to an associate, the method comprising the steps of:

(a) determining that a telecommunication signal is subject to being monitored;

(b) establishing a connection between a first gateway associated with one of a subject being monitored and an associate and a first termination point representing a second gateway associated with the other of the associate and the subject;

(c) establishing a connection between the second gateway and a second termination point representing the first gateway; and

(d) establishing a connection between the first termination point and the second termination point to establish a bearer channel between the subject and the associate wherein the first and second gateways appear to be connection directly.

32. The method of claim 31, further comprising the step of establishing a connection from at least one of the first termination point and the second termination point to a gateway associated with other than the subject and the associate concurrently with the connection between the first termination point and the second termination point.

33. A method of redirecting a telecommunications signal intended for one of a subject and an associate, the method comprising:

(a) associating a first termination point with a first intended termination point of a first media gateway;

(b) associating a second termination point with a second intended termination point of a second media gateway;

(c) establishing a connection between the first intended termination point and the second termination point;

(d) establishing a connection between the second intended termination point and the first termination point; and

(e) establishing a connection between the first termination point and the second termination point wherein the first intended termination point and the second termination point appear to be connected directly.

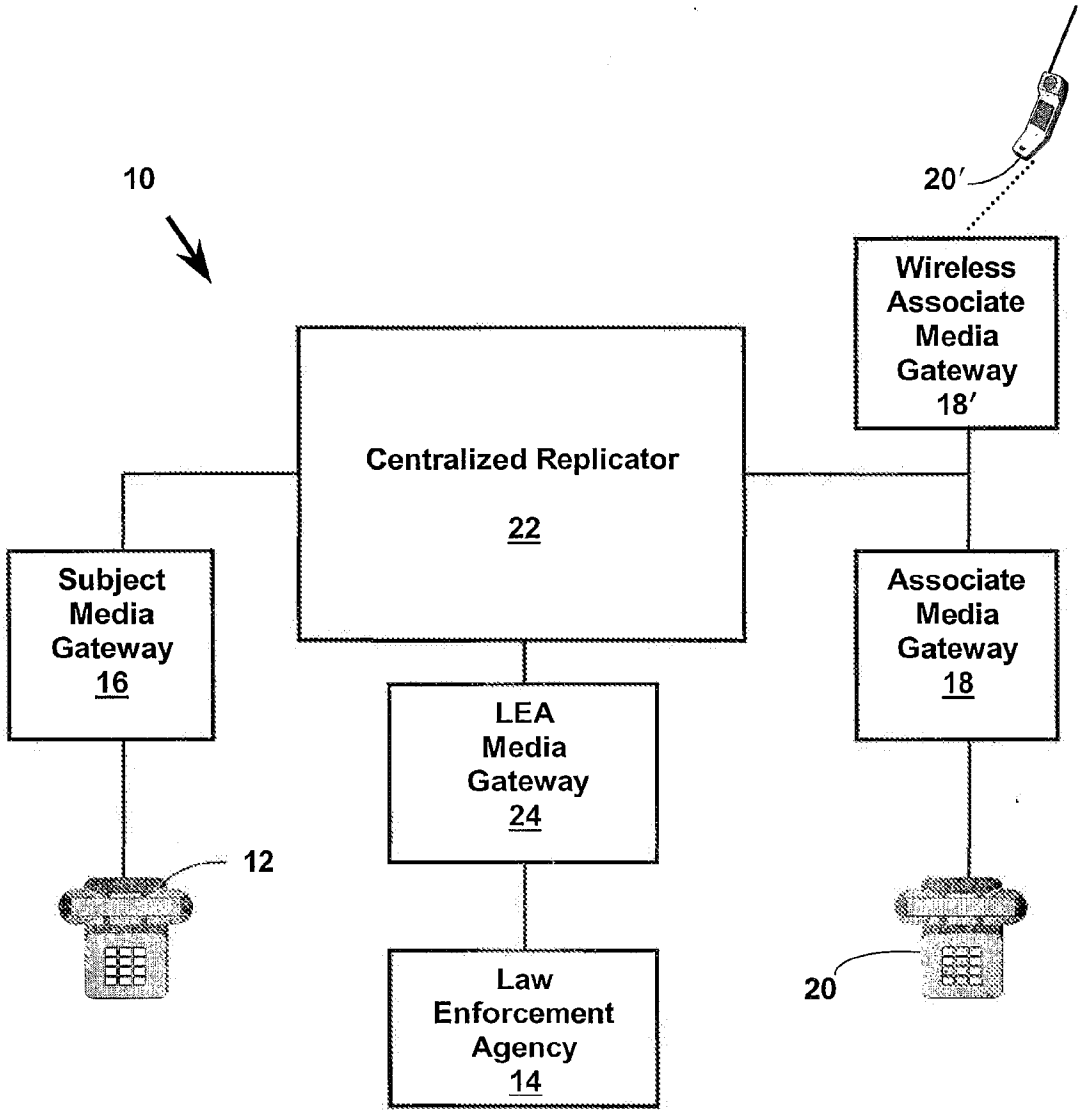

10
20′
Wireless Associate Media Gateway 18′
Centralized Replicator 22
Subject Media Gateway 16
Associate Media Gateway 18
LEA Media Gateway 24
12
20
Law Enforcement Agency 14

Figure 1

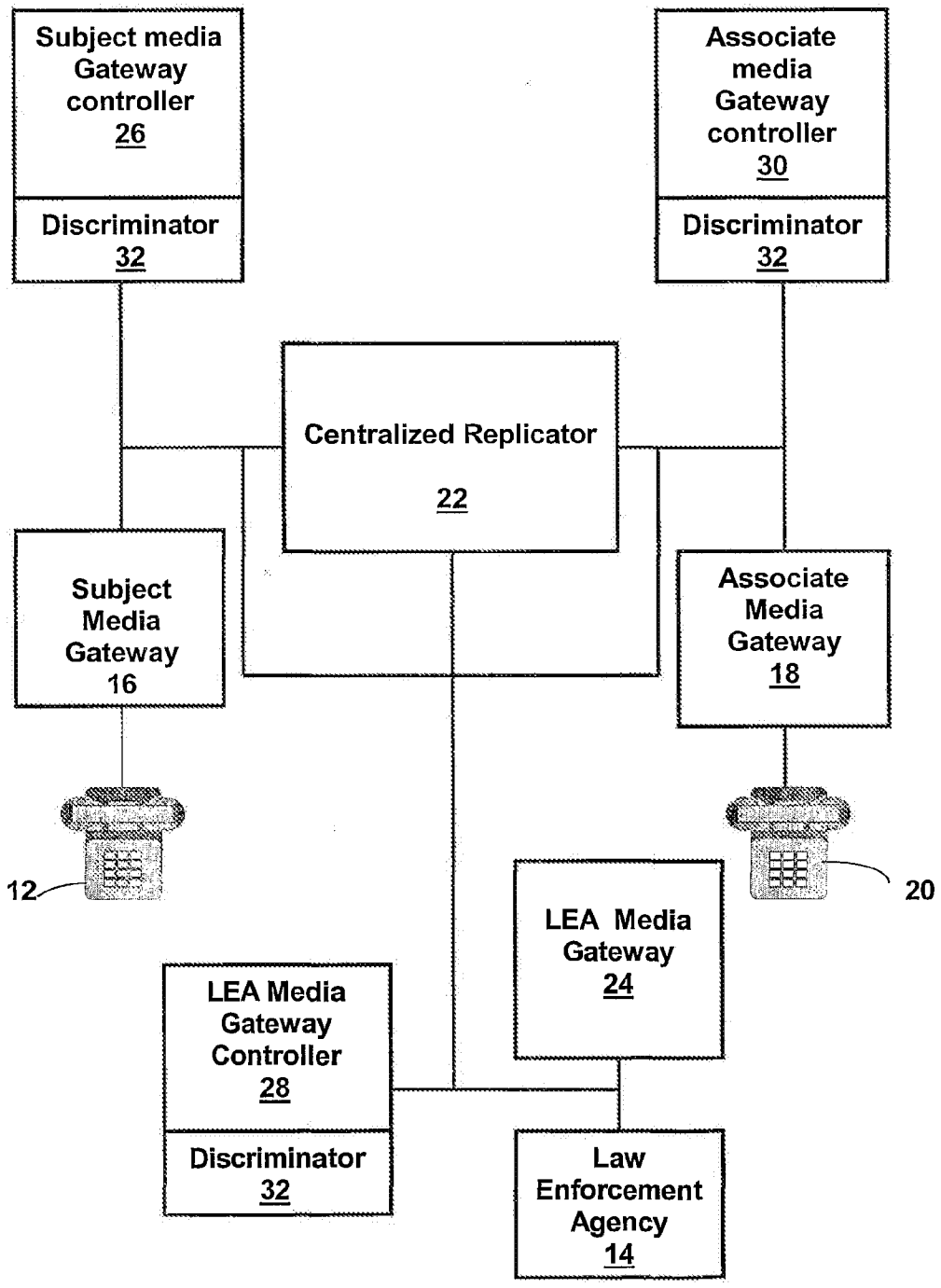

Subject media Gateway controller 26
Discriminator 32
Associate media Gateway controller 30
Discriminator 32
Centralized Replicator 22
Subject Media Gateway 16
Associate Media Gateway 18
12
20
LEA Media Gateway 24
LEA Media Gateway Controller 28
Discriminator 32
Law Enforcement Agency 14

Figure 2

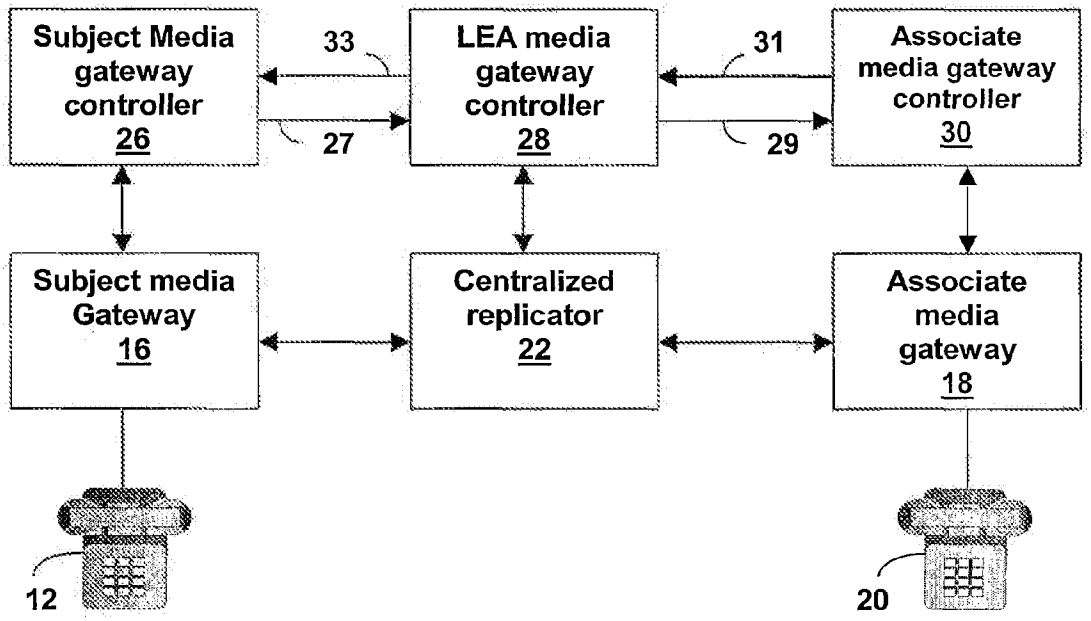

Subject Media gateway controller 26
33
27
LEA media gateway controller 28
31
29
Associate media gateway controller 30
Subject media Gateway 16
Centralized replicator 22
Associate media gateway 18
12
20

Figure 3

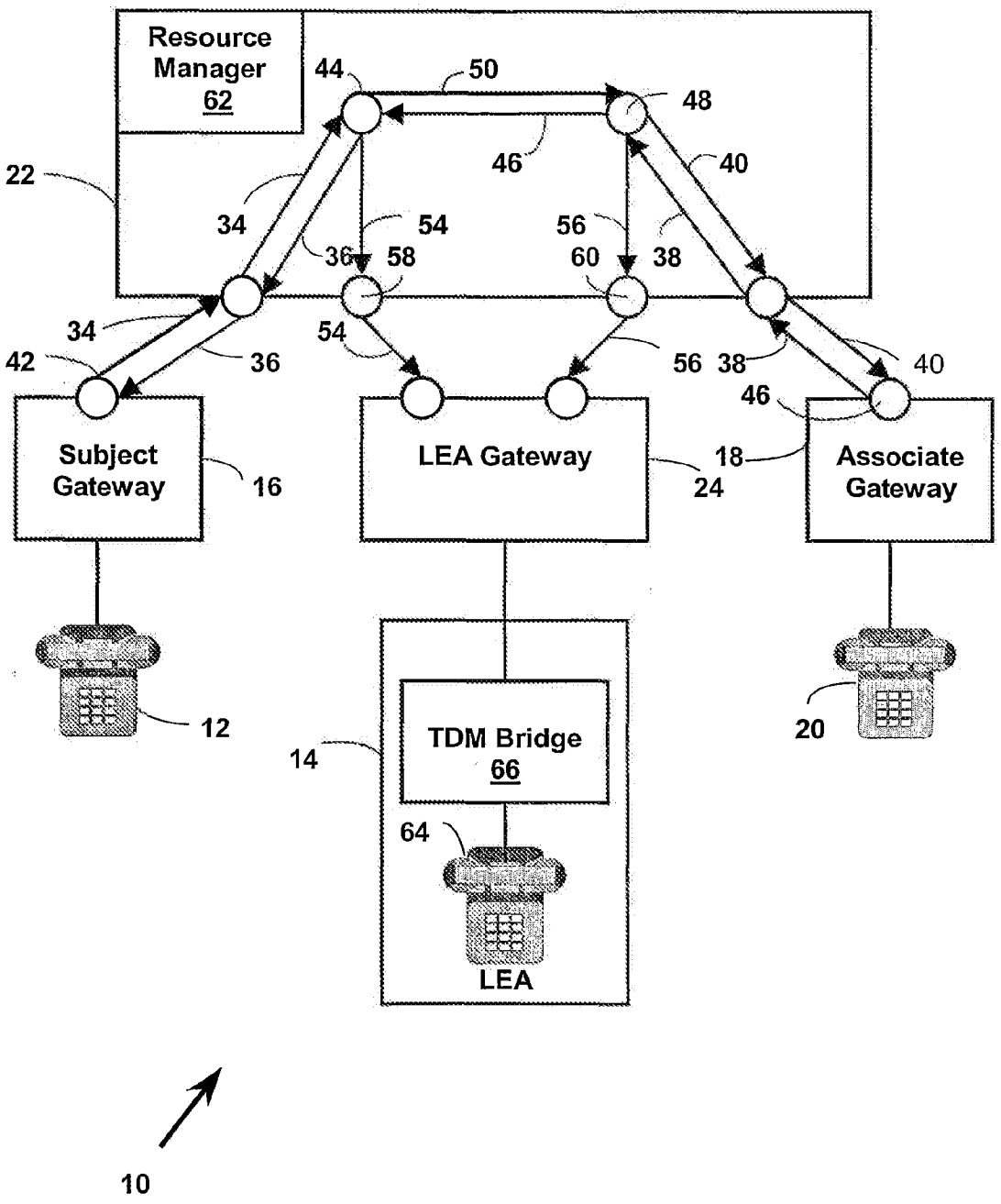

Resource Manager 62
44
50
48
46
40
22
34
54
56
36
58
60
38
34
54
42
36
56
38
40
46
Subject Gateway
16
LEA Gateway
18
24
Associate Gateway
12
20
14
TDM Bridge 66
64
LEA
10

Figure 4

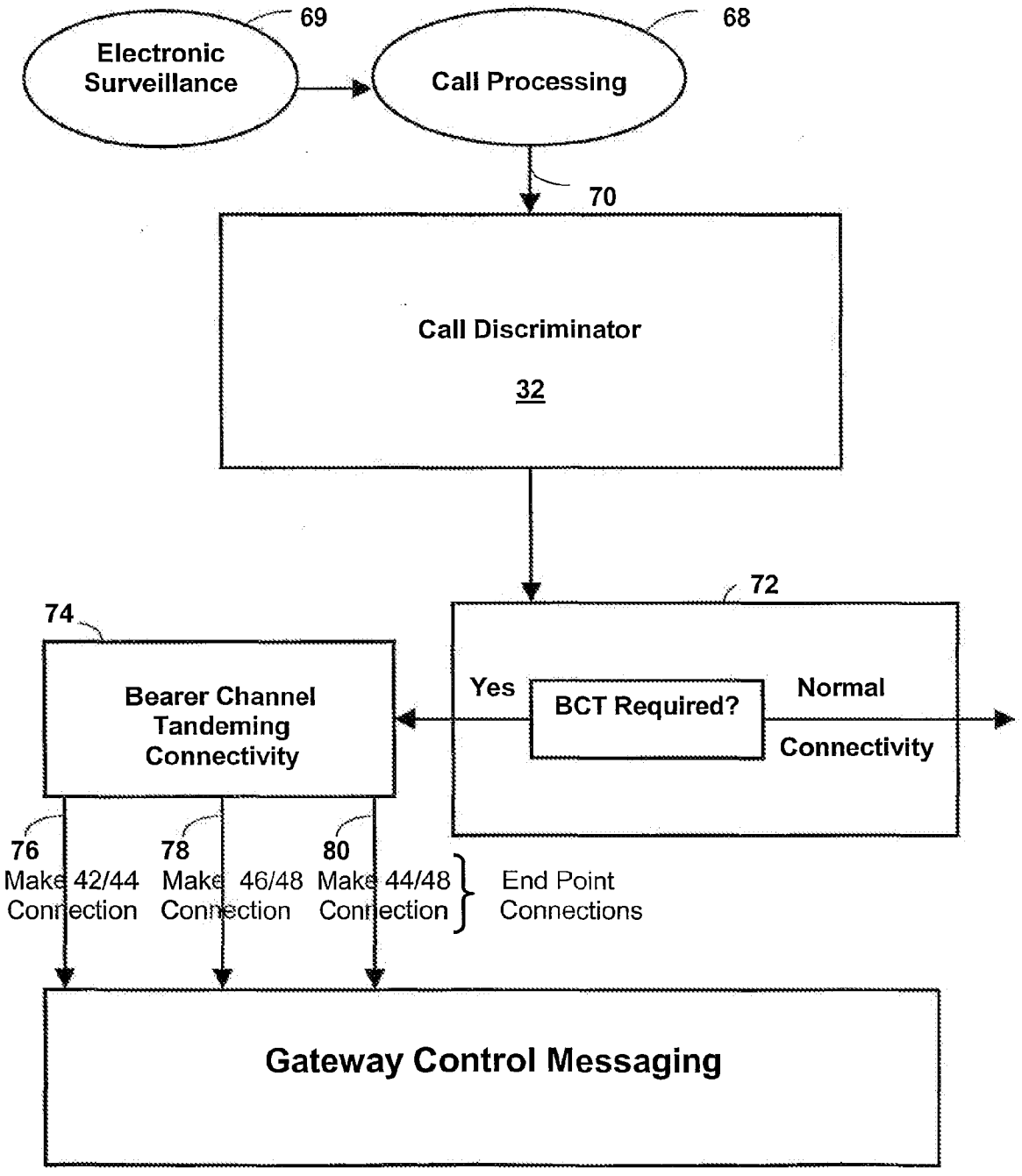

69
Electronic Surveillance
68
Call Processing
70
Call Discriminator
32
72
74
Bearer Channel Tandeming Connectivity
Yes
BCT Required?
Normal
Connectivity
76
Make 42/44 Connection
78
Make 46/48 Connection
80
Make 44/48 Connection
End Point Connections
Gateway Control Messaging

Figure 5

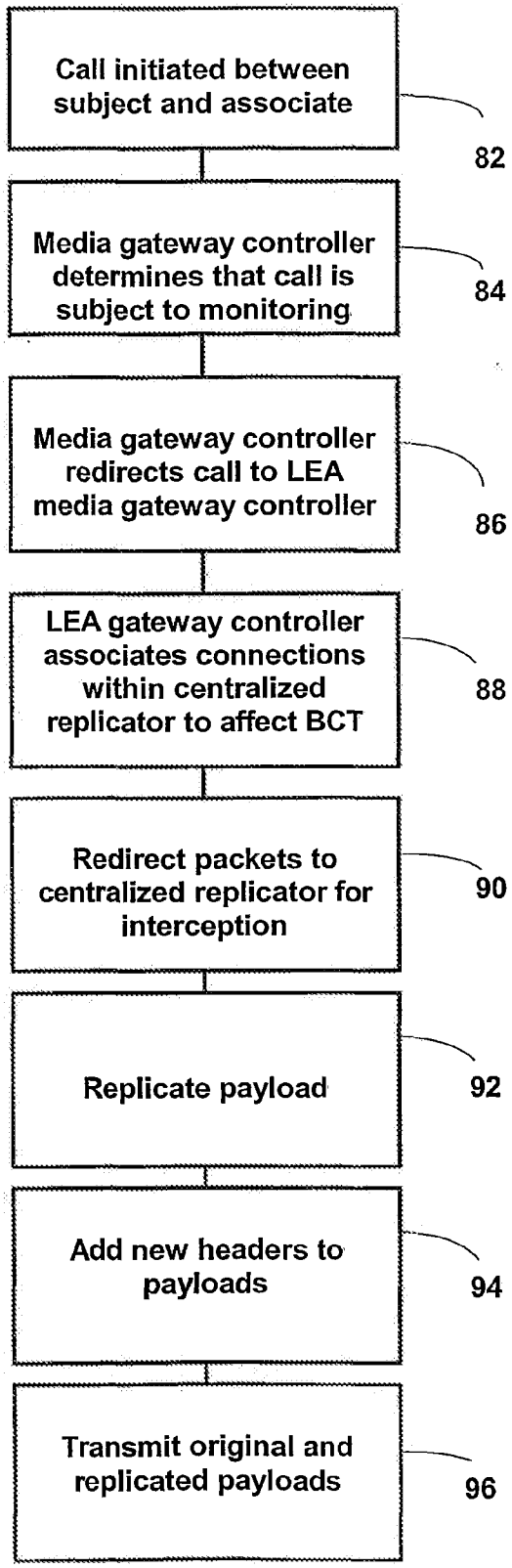

Call initiated between subject and associate
82
Media gateway controller determines that call is subject to monitoring
84
Media gateway controller redirects call to LEA media gateway controller
86
LEA gateway controller associates connections within centralized replicator to affect BCT
88
Redirect packets to centralized replicator for interception
90
Replicate payload
92
Add new headers to payloads
94
Transmit original and replicated payloads
96

Figure 6

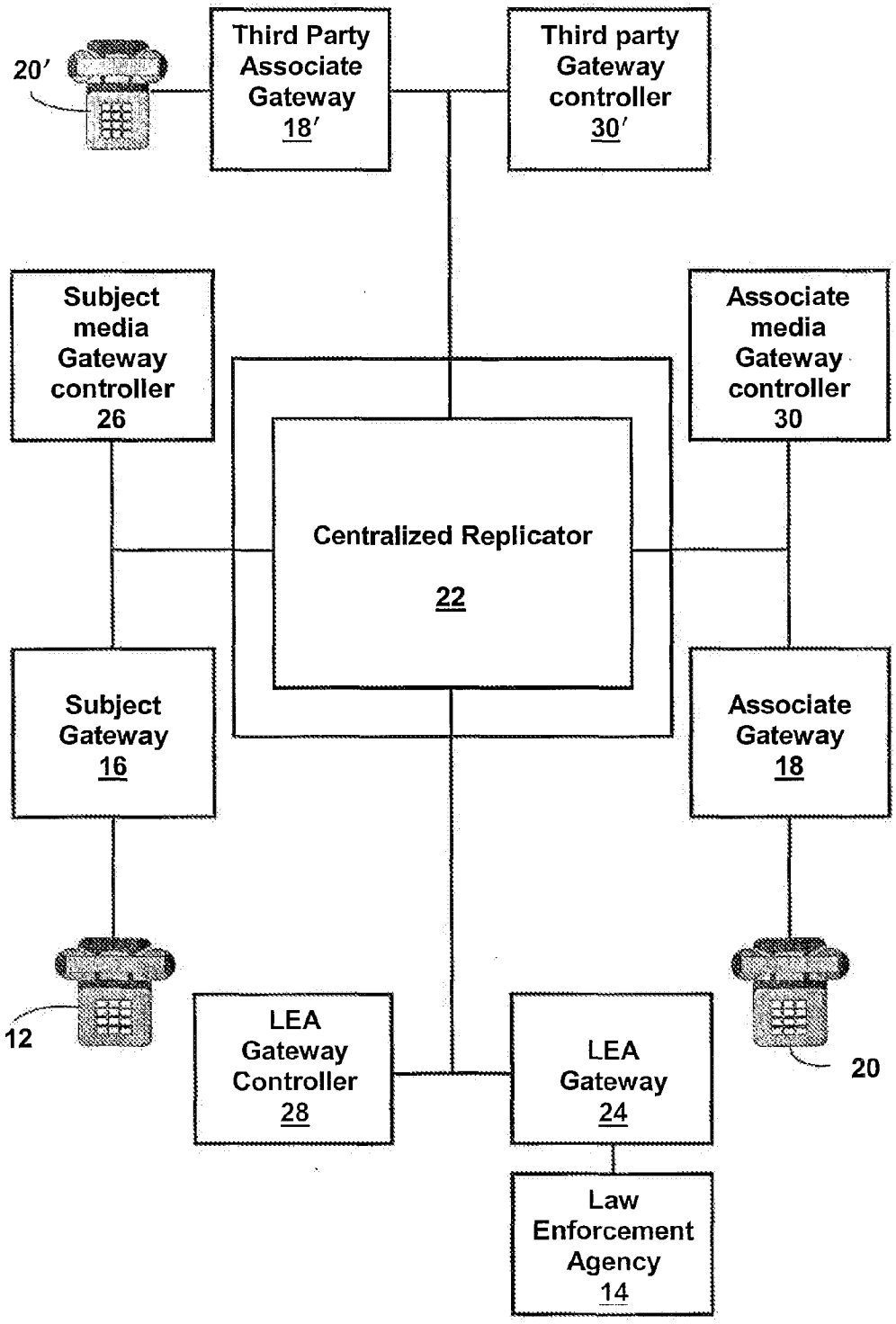

20′
Third Party Associate Gateway 18′
Third party Gateway controller 30′
Subject media Gateway controller 26
Associate media Gateway controller 30
Centralized Replicator 22
Subject Gateway 16
Associate Gateway 18
12
LEA Gateway Controller 28
LEA Gateway 24
20
Law Enforcement Agency 14

Figure 7

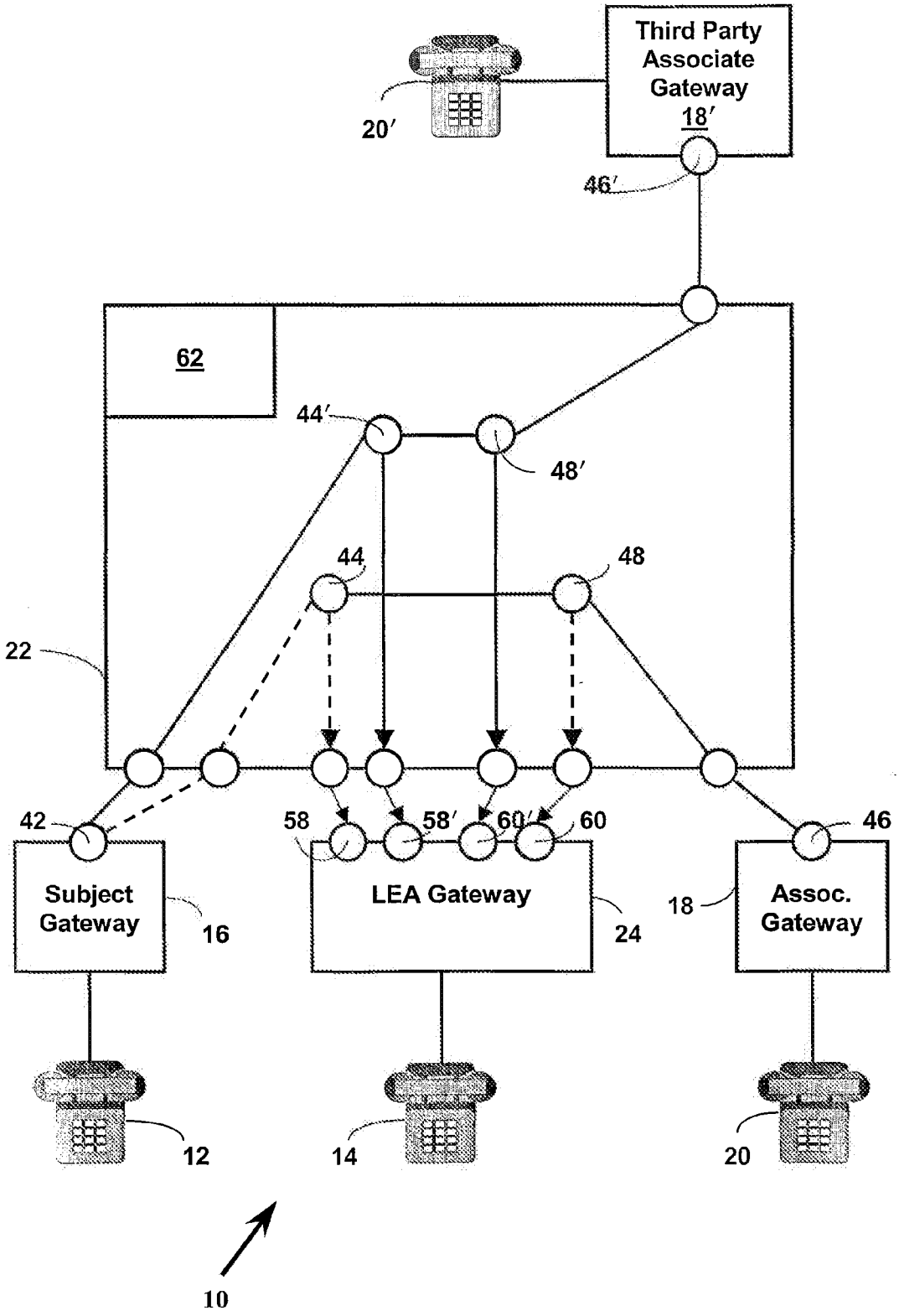

Third Party Associate Gateway 18′
20′
46′
62
44′
48′
44
48
22
42
58
58′
60′
60
46
Subject Gateway
16
LEA Gateway
24
18
Assoc. Gateway
12
14
20
10

Figure 8

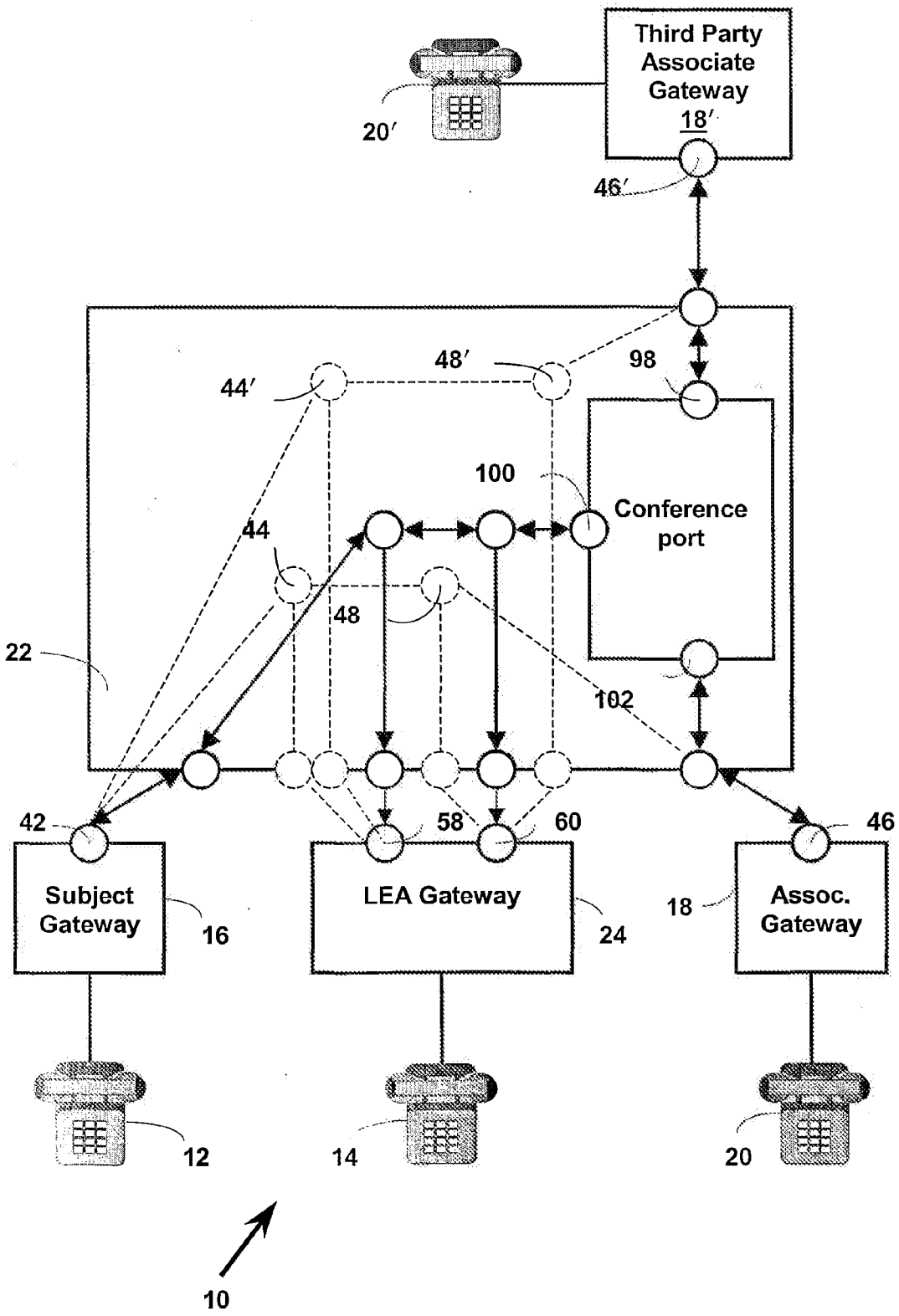

Third Party Associate Gateway 18′
20′
46′
48′
44′
98
100
Conference port
44
48
22
102
42
58
60
46
Subject Gateway
16
LEA Gateway
24
18
Assoc. Gateway
12
14
20
10

Figure 9

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 October 2002 (17.10.2002)

PCT

(10) International Publication Number
WO 02/082782 A3

(51) International Patent Classification[7]: H04L 12/56

(21) International Application Number: PCT/US01/31548

(22) International Filing Date: 9 October 2001 (09.10.2001)

(25) Filing Language: English

(26) Publication Language: English

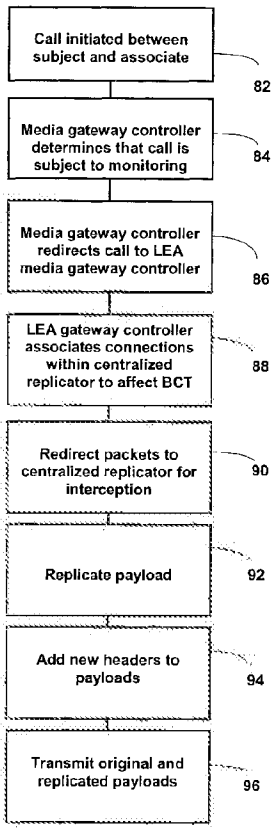
(30) Priority Data:
60/239,048 10 October 2000 (10.10.2000) US

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

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PYKE, Craik, R.** [CA/CA]; 426A Moodie Drive, Nepean, ON K2H 8A6 (CA). **HERN, William** [GB/GB]; "Feliz" Whyteladyes Lane, Maidenhead, SL6 9LA (GB). **THOMPSON, Roger, L.** [US/US]; Dept. ND840, P.O. Box 13955, RTP, NC 27709 (US). **CARON, Serge, S.** [CA/CA]; 52 Limbour, Gatineau, PQ J8V 1X9 (CA). **MOUNJI, Halima, H.** [CA/CA]; 60 Hemlo Cres., Kanata, ON K2T 1E2 (CA). **EWOTI, Charles, B.** [DE/DE]; Oberer Garwiedenweg 2, 88677, Markdorf (DE). **GOERENS, Michael** [DE/DE]; Kenzelweg 17, 88045 Friedrichshafen (DE). **STRENG, Pete, J.** [CA/CA]; 5436 West River Drive, Manotick, ON K4M 1G5 (CA). **GOERTZEN, Christopher, J.** [CA/CA]; #10-1701 Blohm Drive, Ottawa, ON K1G 6N6 (CA). **KITTLITZ, Christian** [CA/CA]; 2-2418 Carlson Avenue, Ottawa, ON K1V 8G1 (CA). **TAYLOR, Richard, C.** [CA/CA]; P.O. Box 22, Manotick, ON K4M 1A2 (CA). **WELHAM, Michael** [DE/DE]; Bruckfelder Strasse 27, 88662 Lippertsreute (DE).

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR INTERCEPTING TELECOMMUNICATIONS



(57) **Abstract:** A system and method for intercepting a telecommunication signal (fig. 6 box 86) are generally provided, in which the system and method affect receiving a telecommunication packet, comprising a header and a payload, removing a first header from the packet, replicating the payload (fig. 6 box 92) and adding a second header to the replicated payload (fig. 6 box 94) and directing the replicated payload to the address associated with the second (fig. 6 box 96).

WO 02/082782 A3

(74) Agent: VYNALEK, John, H.; Nortel Networks Inc., P.O. Box 13828, Research Triangle Park, NC 27709-3828 (US).

(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, EC, 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, US, 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, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

(88) Date of publication of the international search report:
24 April 2003

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/31548

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 12/56

US CL : 370/352

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/352,

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 6,147,994 A (DUREE ET AL. 14 NOVEMBER 2000, COL. 31, LINE 65 - COL. 32 LINE 8.	1, 3-10, 12-16, 18-23, 25-30
Y,E	US 6,356,546 B1 (BESHAI) 12 MARCH 2002, COL. 13 LINES 16-27.	1,3-10, 12-16,18-23,25-30
Y,P	US 6,246,688 B1 (ANGWIN ET AL.)12 JUNE 2001, COL. 3 LINES 11 - 58.	1,3-10,12-16,18-23,25-30

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 29 AUGUST 2002	Date of mailing of the international search report 18 DEC 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer RON ABELSON Telephone No. (703) 306-5622

Form PCT/ISA/210 (second sheet) (July 1998)★

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2005 (09.09.2005)

PCT

(10) International Publication Number
WO 2005/084002 A1

(51) International Patent Classification[7]: H04M 7/00, 3/42

(21) International Application Number:
PCT/GB2005/000612

(22) International Filing Date: 18 February 2005 (18.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/548,746 27 February 2004 (27.02.2004) US
10/861,194 4 June 2004 (04.06.2004) US

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

(71) Applicant *(for UZ only)*: NORTEL NETWORKS UK LIMITED [GB/GB]; Maidenhead Office Park, Westacott Way, Maidenhead Berkshire SL6 3QH (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DAWSON, Martin [AU/AU]; 10 Rosemont Street, West Wollongong, New South Wales 2500 (AU). LEWIS, Mark [US/US]; 3160 Wagner CT, Aurora, Illinois 60504 (US). BRODA, Maciej [CA/CA]; 22 Brookbend Cres, Ottawa, Ontario K2H 1E4 (CA).

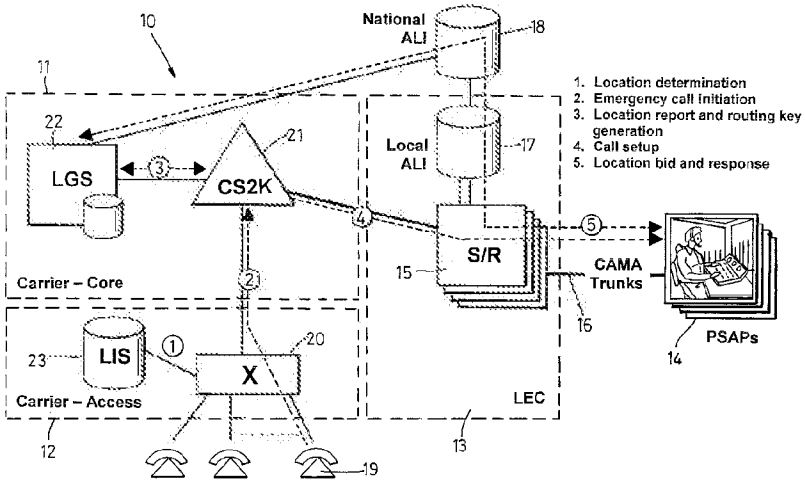
(74) Agent: HERMELE, Daniel; Nortel Networks Limited, London Road, Harlow Essex CM17 9NA (GB).

(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, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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,

[Continued on next page]

(54) Title: DETERMINING THE GEOGRAPHICAL LOCATION FROM WHICH AN EMERGENCY CALL ORIGINATES IN A PACKET-BASED COMMUNICATIONS NETWORK



(57) Abstract: In order that emergency service vehicles can be dispatched to the correct destination promptly, accurate information about the location of the caller is needed. Another problem concerns routing emergency calls to the correct destination. For emergency calls a universal code is used such as 911 in North America and 112 in Europe. This universal code cannot be used to identify the destination of the call. These problems are particularly acute for nomadic communications systems such as voice over internet protocol communications networks. That is because user terminals change network location. These problems are solved by enabling the geographical location of the emergency caller to be determined by entities within a packet-based network without the need for modification of existing emergency services network infrastructure.

WO 2005/084002 A1

FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, 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).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search 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.

DETERMINING THE GEOGRAPHICAL LOCATION FROM WHICH AN EMERGENCY CALL ORIGINATES IN A PACKET-BASED COMMUNICATIONS NETWORK

The present invention relates to a method and apparatus for determining the geographical location from which an emergency call originates in a packet-based communications network. The invention also relates to a method and apparatus for providing a routing key for routing an emergency call from a packet-based communications network node to an emergency services network node.

BACKGROUND TO THE INVENTION

There are a number of particular problems in dealing with emergency calls that do not arise for regular calls. For example, in order that emergency service vehicles or other assistance can be dispatched to the correct destination promptly, accurate information about the location of the caller is needed. Previously, in conventional switched telephone networks, it has been possible to provide the caller location information relatively easily because telephone handsets are typically fixed in particular locations. Static database entries can then be made in a database accessible to the emergency services associating for example, a subscribers' home address and telephone number. However, for mobile communication systems and also for nomadic systems use of such static database entries is not possible because the location of a communications terminal varies over time.

Another problem concerns routing emergency calls to the correct destination. For regular calls this is not such an issue because the caller enters specific details of the required call destination. However, for emergency calls a universal code is used such as 911 in North America and 112 in Europe. This universal code cannot be used to identify the destination of the call. Generally, an emergency call needs to be routed to a particular geographical answering point for servicing. This answering point is often referred to as a

Public Safety Answering Point (PSAP). The jurisdiction for emergency services answering points is typically quite small, for example, at the county level in the USA. This information about the location of the caller is needed to determine which emergency services answering point to route the call to. Misrouting of calls to the wrong answering point leads to costs in transferring calls, impacts reliability, and leads to delays which are significant in life threatening situations. Previously, in conventional switched telephone networks, this location information was relatively easy to obtain because static database entries could be used as mentioned above. However, this is not possible for mobile and nomadic communications systems.

One proposal has been to update or refresh the database entries every 24 hours. However, this approach cannot cope with situations where a user terminal changes location more than once a day. Also, changes to the existing emergency services network infrastructure are required in order to enable the database to be updated daily.

More detail about how existing voice networks interface to the emergency services network is now given. The primary existing voice networks that do interface to emergency services are the PSTN (public switched telephone network) as served by LECs (local exchange carriers) and the various mobile networks operated by the cellular carriers.

The emergency services network, from this perspective, can be regarded as being made up of Selective Routers (SRs), Automatic Location Identification (ALI) databases, both local and national, and the Public Safety Answering Points (PSAPs) themselves with their various CAMA (centralized automatic message accounting), and other, trunk connections and various data connections for querying the ALIs. Of course, beyond these network elements are the public safety organisations themselves (Police, Fire, Ambulance) and the communications networks that support them.

The location of the subscriber, who is dialing emergency services, is used for two key purposes. The first is routing of the call, ultimately to the right PSAP, and the second is in the delivery of the location, for display, to the PSAP operator in order that emergency response units can be dispatched to the correct location.

In wireline voice networks, there is an association between the phone number of the subscriber (The Calling Line Identifier - CLID) and that subscriber's location. This is generally, the home address of the subscriber as maintained by their local exchange carrier. In this case, the CLID becomes a ready-reference to location.

Similarly, the incoming line to the local exchange switch and the switch itself provides an explicit indication of the appropriate routing of 911 calls. This permits the local exchange to work from a static configuration in terms of selecting the outgoing trunk on which to place the call so it goes to the correct selective router. The selective router, in turn, can use the same static association and CLID information to ensure that the call is routed to the correct serving PSAP for the subscriber's address.

In cellular systems, the association between the subscriber's location and their CLID is lost. Being, by definition, mobile a cellular subscriber can be anywhere within the wireless network's area of coverage. Similarly, there is no physical wired line corresponding to the source of the call from which to associate a route to the correct destination. In cellular networks, however, there is a physical serving cell from which the call is initiated. The geographic granularity of these cell locations is generally sufficiently fine for the mobile switch to determine the correct trunk route to a corresponding selective router. In many cases, this also provides sufficient accuracy for the selective router to determine which PSAP the caller should be connected with.

It is an internal procedure for the mobile switch to associate an outgoing trunk route with a serving cell. However, some signaling is required for an MSC (mobile switching center) to pass this same information along to the selective router so that it can determine the correct PSAP. The TR45 standard, J-STD-036 "Enhanced Wireless 9-1-1 Phase 2", Telecommunications Industry Association, 2000, defines mechanisms for doing this. The routing information is passed to the selective router in the ISUP (ISDN user part) call setup signaling in one or other newly defined parameters called the Emergency Services Routing Digits (ESRD) or the Emergency Services Routing Key (ESRK). The selective router examines the value of the ESRD/ESRK parameter in the call setup signaling and routes the call to the correct PSAP based on this value.

Note that there are circumstances where cell boundaries can span the boundaries of PSAP catchment areas. In this case, and ESRD or ESRK determined from a serving cell may not provide a reliable indication of a route to the correct PSAP. Both ANSI-41 (generally TDMA, and CDMA) and 3GPP (generally GSM, EDGE, and UMTS) cellular networks have identified functionality to address this. In ANSI-41 networks a functional element known as a Coordinate Routing Database (CRDB) is defined. The network can consult the CRDB and, based on the geographic location of the caller (determined by different positioning technologies such as forward link trilateration, pilot strength measurements, time of arrival measurements, etc.), it will return an appropriate value of the routing parameter. As long as the geographic location is an improvement in accuracy over the cell location, this mitigates the problem of misrouted calls. Similarly 3GPP networks allow the switch to request a refined routing key value from the Gateway Mobile Location Center (GMLC) based on the geographic location of the caller.

The second, independent, area in which location comes into play in E911 calling is the display of the caller's location to the PSAP operator. The need for this is that the PSAP operator can facilitate more rapid despatch of the emergency service response units if the network can deliver the location rather than relying on getting this information from the caller - particularly where the caller may be unable to provide this information.

In a wireline voice network, necessary subscriber (or, at least, calling line) address information is stored in a database known as an Automatic Location Identification, or ALI, database. On receipt of an emergency call and, armed with the caller's CLID, the PSAP is able to query this database and receive, in return, the street address (also known as a civic address) information associated with the CLID. The physical interface over which the PSAP makes this query is variable. It may be an IP based interface over dial-up or broadband or it may be made over an X.25 packet interface. Similarly, the ALI may physically be co-located within the LEC and selective router, or it may be a remote national ALI handling the request directly or in tandem from the local ALI. Similarly, the protocol may vary but one known as PAM (PSAP to ALI message specification) is in common usage. These details are contained

within the emergency network itself and not generally a concern of the larger voice network on the far side of the selective router.

In a cellular network, the same level of detachment with respect to this function is not possible. To begin with, the location of the caller is variable both initially and during the period of an emergency call. It is no longer possible to rely on a static database of location information that can provide an address against a CLID. It now becomes necessary for the PSAP to be able to request a dynamic location both for the initial position of the caller but also for any changes during the call. In addition, a civic address may no longer be pertinent to the location of the caller. By nature, cellular networks cover wide and varying types of territory. A conventional street address may no longer apply to a caller's location. Indeed, they may not even be in or by a street as the term is commonly understood. For this reason, a more universal reference system for location needs to be used. The solution generally adopted and, once more defined in J-STD-036 as referenced above, is to use geospatial co-ordinates - or latitude and longitude - as defined in the WGS-84 coordinate system (Military Standard WGS84 Metric MIL-STD-2401 (11 January 1994): "Military Standard Department of Defence World Geodetic System (WGS)").

While J-STD-036 does define mechanism whereby this geospatial location can be delivered in the ISUP call setup signaling, it can be generally acknowledged that PSAPs do not support the necessary signaling interfaces nor customer premises equipment to receive and display this information. Also, there is no mechanism whereby an updated location can be delivered in the ISUP signaling. For these reasons, J-STD-036 identifies a new interface that the emergency network can use to query the cellular network. This interface is assigned the identifier of E2 and both J-STD-036 and NENA "NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface" define a protocol which can be used over this interface called the emergency services protocol.

On receipt of an emergency call arising from a cellular network, the PSAP can initiate, via the serving ALI, a request on the cellular network to provide the geodetic location of the caller. This request is made over the E2 interface in a message called the EPOSREQ (Emergency Position Request) with the

response message identified as the esposreq. The location of the caller is determined by positioning capabilities native to the cellular network itself and different systems of network measurement, triangulation, or special handset capabilities such as GPS (Global Positioning System) are used.

As described above, the network mechanisms and procedures defined in JSTD-036 are around the provision of a geodetic (latitude and longitude) type location for the caller. This obviously implies a capability on the part of the PSAP to display location information of this type to the PSAP operator. There is also consideration supported in the E2 interface messaging that allows the delivery of civic address type information.

One application of this facility is in the support of PSAPs which are not equipped with the capability to receive and display geodetic type location information. This is part of what is often referred to as a Phase 1 E911 capability for cellular networks. Enhanced 911 calling was introduced in two phases into the cellular and emergency services networks. Phase 2 defined the capabilities for delivering, generally more accurate, geodetic location information from the network. Phase 1 was generally targeted at providing location information to the accuracy of a serving base station location but, perhaps more importantly, that location information is delivered to the PSAP as a more conventional street, or civic, address associated with that base station. Depending on the nature of the PSAP, the ALI may provide the geodetic position and/or the phase1 civic address type information in response to the location bid.

Just as cellular networks have specific characteristics that result in new considerations for E911 compared to conventional wireline voice networks, so too do IP based voice (VoIP) networks. VoIP network users have much in common with cellular network users in that there is no specific physical point of connection which dictates their identity. Just as a cellular phone can attach to the network anywhere that there is a point of coverage, so too can an IP based phone client attach to an IP network at many and varied points and take advantage of the voice service. From this perspective, it becomes necessary to view VoIP clients as essentially nomadic or even fully mobile to ensure that all usage scenarios are covered. For certain, many VoIP clients may be relatively static in terms of location (for example, a conventional form

factor desktop phone with integrated VoIP client software will tend to be as stationary as any conventional wireline desktop phone) however, this situation is not explicitly predictable by the network, so an architecture that addresses mobility ensures that all usage scenarios are covered.

In terms of emergency call routing, the VoIP network introduces some additional challenges over wireline or cellular networks. In particular, the access network associated with a VoIP network can be highly distended. That is to say, in wireline the phone is tied to the specific local switch by the incoming line, in cellular the mobile switch has specific knowledge of the serving cell which has some degree of geographic association with that switch. But, in VoIP, the client may be attached to the network in another city, state, or, even, country than the one in which the serving call server is located. There is not an immediate association to location that the call server can use to directly determine a route to a selective router before, even, the correct PSAP can be selected.

Similarly, in terms of location delivery and display, a VoIP client may be appropriately identified by a street address, being on a relatively static access point, or it may be more appropriately identified against a geodetic location, as in the case of a VoIP client connected by a wide area broadband wireless network.

OBJECT TO THE INVENTION

The invention seeks to provide a method and apparatus for determining the geographical location from which an emergency call originates in a packet-based communications network which overcomes or at least mitigates one or more of the problems mentioned above.

The invention also seeks to provide a method and apparatus for providing a routing key for routing an emergency call from a packet-based communications network node to an emergency services network node which overcomes or at least mitigates one or more of the problems noted above.

Further benefits and advantages of the invention will become apparent from a consideration of the following detailed description given with reference to the

accompanying drawings, which specify and show preferred embodiments of the invention.

SUMMARY OF THE INVENTION

According to an aspect of the present invention there is provided a method of providing a routing key for routing an emergency call from a packet-based communications network node to an emergency services network node in a switched telephone network, said method comprising the steps of:

- receiving information about the geographical location from which the emergency call originates;
- generating a routing key on the basis of the received information and pre-specified information about geographical locations served by particular emergency service network nodes.

This provides the advantage that an emergency call can be routed using the routing key to an appropriate emergency services network node. This is achieved in a packet-based network without the need to access information from the emergency services network. Thus an existing emergency services network can be used without the need for modification.

Preferably the method comprises storing said generated routing key together with the received information about geographical location. The method also comprises providing the stored information to an automatic location identification (ALI) database. In this way the geographical location information is made available to an existing emergency services communications network comprising an ALI. The emergency services network is then able to display that information and use it to dispatch emergency services vehicles.

According to another aspect of the present invention there is provided a packet-based communications network node for providing a routing key for routing an emergency call from the packet-based communications network to an emergency services network node in a switched telephone network, said node comprising:

- an input arranged to receive information about the geographical location from which the emergency call originates;
- a processor arranged to generate a routing key on the basis of the received information and pre-specified information about geographical locations served by particular emergency service network nodes.

According to another aspect of the present invention there is provided a method of routing an incoming emergency call in a packet-based communications network to an appropriate emergency services answering point in a switched telephone network, said method comprising:

- at a call server, receiving the emergency call;
- at a location gateway server, receiving a geographical location from which the call originated and using that to generate a routing key;
- at the call server, routing the emergency call using the generated routing key.

Preferably a location information server is used to provide the geographical location information. This provides the advantage that the location gateway server need not be concerned with the particular methods used to determine the geographical location information.

Also, the routing key is determined and delivered dynamically within the life of the emergency call. This is achieved by using the location information server to provide the geographical location information as and when needed. This reduces and need for static information to be retained in the network including an emergency services network. In addition, it is possible to deal with nomadic entities and mobile entities whose geographical location changes over time.

In a preferred embodiment the location gateway server interfaces to the emergency services network using a known interface protocol. This enables the present invention to be used with existing emergency services equipment that already operates the specified interface protocol. This reduces costs and the need for modification of network equipment.

The invention also encompasses computer software for implementing any of the methods described above and herein.

The preferred features may be combined as appropriate, as would be apparent to a skilled person, and may be combined with any of the aspects of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to show how the invention may be carried into effect, embodiments of the invention are now described below by way of example only and with reference to the accompanying figures in which:

Figure 1 is a schematic diagram of a packet based communications network comprising a location gateway server;

Figure 2 is a flow diagram of a method of operating a call server to route an emergency call;

Figure 3 shows the communications network of Figure 1 with a connection between the location gateway server and location information sever;

Figure 4 is a schematic diagram of another embodiment of the communications network of Figure 1;

Figure 5 is a schematic diagram of a communications network comprising a DHCP (Dynamic Host Configuration Protocol) server suitable for use in an embodiment of the invention;

Figure 6 is a schematic diagram of an enterprise client and call server using a carrier Location Gateway Server (LGS) and Trunk Media Gateway (TMG) to route emergency calls into an emergency network;

Figure 7 is a schematic diagram of a carrier voice over internet protocol (VoIP) deployment serving enterprise customers with network based VoIP service from legacy clients connected via conventional managed switches;

Figure 8 is a message sequence chart for several embodiments of the invention.

DETAILED DESCRIPTION OF INVENTION

Embodiments of the present invention are described below by way of example only. These examples represent the best ways of putting the invention into practice that are currently known to the Applicant although they are not the only ways in which this could be achieved.

The term "geographical location information" is used to refer to information about the physical position of an entity in the physical environment as opposed to a communications network address. For example, it comprises a civic address, postal address, street address, latitude and longitude information or geodetic location information.

The term "nomadic communications system" is used to refer to a communications network in which user terminals can access the network from different, geographically separated, network access points without the need for modification of the terminal in order to access the network from those different access points.

Figure 1 is a schematic diagram of a packet-based communications network 10 with a core network region 11, an access network region 12, and a local exchange region 13.

A plurality of public safety answering points (PSAPs) 14 are shown, each being for serving a different geographical region as known in the art. Each PSAP has an associated selective router 15 which is a switch for routing calls, location information and other details to the PSAP. Each selective router 15 is connected to its associated PSAP by a trunk 16 or other suitable communications link as known in the art.

Each selective router 15 is linked via the communications network 10 to a local automatic location identification (ALI) database 17. This database comprises pre-specified information about a geographical address associated with each customer or user account and details of an identifier for a communications terminal for that customer account. Only information about customer accounts with geographic addresses local to the particular selective router 15 are stored in the local ALI 17.

A national ALI 18 is also provided. This comprises pre-specified information about which geographical regions each local ALI 17 serves. For example, details of every valid postal address in the USA are stored and each address is associated with a particular local ALI 17 and selective router 15.

The local ALIs 17, selective routers 15, national ALI 18, PSAPs 14 and trunks 16 are all known in the art of conventional switched telephone networks. An advantage of the present invention is that this emergency service network infrastructure is reused without the need for modification. The existing emergency service network infrastructure is integrated or connected to the packet-based communications network core 11 as using media gateways of any suitable type as known in the art.

Communications terminals 19, also referred to as clients, which are of any suitable type, are connected to a switch 20 in the access part 12 of the communications network 10. The terminals 19 are either physically connected to the network or connected via a wireless link. The switch is connected via the network to a call server 21 in the core of the network 11. Only one call server 21 and switch 20 are shown for reasons of clarity, however, many switches 20 are typically served by one call server 21 and there can be a plurality of call servers 21.

When a communications terminal connects to the network 10 on start-up of the terminal, or if the terminal is newly connected, then a registration request is sent to the call server 21 for that region of the network 10. This process is known in the art. The registration process involves the terminal sending, via the switch 20, details of its network address. The call server 21 is then able to keep track of all the terminals 19 under its remit.

In the present invention a location information server (LIS) 23 is provided. Figure 1 shows the LIS in the access part of the network 12 although it can also reside in an Enterprise network or an access network for residential services. The LIS can also be split into two entities: probes and a main server, with the probes in an Enterprise network for example and the main server in an access network.

The LIS is arranged to detect terminals connecting to the network and determine their geographic locations. The LIS passes this information to the terminals when requested and the terminals pass it on to the call server. In addition, the LIS is able to pass the geographic location information to another entity, a Location Gateway Server (LGS) as described in more detail below with reference to Figure 3. In that case the LGS polls the LIS for the location information.

As mentioned above the LIS determines geographic location of terminals. It does this in any suitable known manner. For example, it comprises or has access to a wiremap. This wiremap comprises details of network addresses of access ports in the access network served by the call server 21 and geographic location details associated with each network address. For example, a building address and a particular quadrant of that building. This information is pre-configured at the LIS, for example, by service providers or other network administrators. Thus when a terminal 19 is connected to a particular access port in the access portion of the network 12 there is a network address associated with that port and at the LIS geographic location details associated with the same port or network address. However, it is not essential for the LIS to use a wiremap. Any suitable type of positioning technology can be used. An advantage of using an LIS in this way is that the LGS need not be concerned with the nature of the positioning technology used.

The core network 11 also comprises a location gateway server (LGS) 22 connected to the call server 21 and also linked to the national ALI 18. The LGS is a novel network entity for use in the present invention. The LGS 22 is arranged to determine routing keys also known as emergency services routing keys (ESRKs). A routing key is used by the call server 21 to route an incoming emergency call to an appropriate selective router 15 and PSAP 14. In order to determine the routing keys the LGS operates in conjunction with the LIS 12 and national ALI 18.

In a first embodiment of the present invention the LIS is arranged to detect when a terminal newly starts up or connects to the network. The LIS determines a geographic location for that newly connected terminal using any suitable method as known in the art. For example, the LIS accesses a

wiremap as mentioned above and uses that together with a network address of the terminal to determine an associated geographic location. Alternatively, a global positioning system is used or an emergency caller specifies his or her own location.

In the event that an emergency call is made from one of the terminals 19 that terminal 19 sends a request via switch 20 to the LIS 23 for its geographical location (see box 30 of Figure 2). That geographic location information is returned and sent by the terminal 19 to the call server 21 as part of the call set-up process (see box 31 of Figure 2).

The call server then sends the geographical location information to the LGS. For example, this information is sent in the form of a subscriber location report (SLR) and comprises a call back number for the emergency caller as well as the geographical location information (see box 32 of Figure 2.) However, this is not essential, any suitable form of message can be used to send the geographical location information.

The LGS uses the geographical location information to determine the relevant selective router 15 and PSAP 14 and generates an appropriate routing key. The LGS stores the geographical location information together with the routing key in a cache or other suitable memory. The routing key is made available to the call server (see box 32 of figure 2) which then routes the emergency call to the specified selective router 15 (see box 33 of Figure 2) via a media gateway. The selective router 15 then delivers the emergency call to the appropriate PSAP together with the routing key generated by the LGS. In some cases instead of a routing key a pseudo-ANI generated by the selective router and the local ALI is sent to the PSAP instead of the routing key.

In the method described above with reference to Figures 1 and 2 the LIS is arranged to provide geographical location information to terminals which then provide it to the call server. However, in some situations the location information does not reach the LGS. For example, if there is an error in transmission and packets are dropped. Also, there are situations in which the user terminal is a wireless device that is moving. In that case it may not be

possible for the LGS to keep up to date with the rapidly changing location of the mobile terminal.

A second method for enabling the location information to reach the call server is therefore proposed and is now described with reference to Figure 3. This method is preferably used in conjunction with that of Figure 1 although that is not essential; the two methods can be used independently of one another. Using the methods independently, although not as fool-proof as using them together, is acceptable in some cases. For example, where location information is available via another means. This other means can be for example, explanation from the emergency caller him or herself or a separate global positioning system device of the emergency caller.

Figure 3 shows the same components as in Figure 1 and the same reference numerals are used as appropriate.

In this second method the LGS 22 polls or queries the LIS 23. For each port at the switch 20 to which a terminal is connected the LIS determines an associated geographical location as described above with reference to Figure 1. Thus in this second method the LGS polls the LIS rather than waiting for geographic information sent from the call server. The LGS is also able to do both these things; that is, poll the LIS for the geographic information and receive it from the call server.

Consider the situation when an emergency call is made from one of the terminals 19. This call reaches the call server 21 as known in the art and the call server 21 receives an identifier of the calling terminal as part of the call process. The call server then sends a message to the LGS requesting geographical location information for the emergency calling terminal. The message comprises a subscriber location report or any other suitable type of message. The message comprises the identifier of the calling terminal as well as details of the LIS associated with the call server 21.

The LGS itself does not have the geographical location information requested and so it queries the LIS for that information using the identifier of the calling terminal.

As in the method described with reference to Figure 1, the LGS uses the geographical location information to determine the relevant selective router 15 and PSAP 14 and generates an appropriate routing key. The method then proceeds as described above with reference to Figure 1 such that the emergency call is routed to the appropriate PSAP and the location information is also delivered to the PSAP.

Thus both the first and second methods described above involve using the LIS to determine the location from which an emergency call originates. In the first method the LIS sends this geographical information to a terminal which sends it to the call server during call set up. In the second method the LGS actively polls the LIS for the geographical location information.

The methods described thus far enable an emergency call to be routed to the appropriate PSAP. In order for the PSAP to also obtain the geographical location information of the emergency caller an interface is provided between the LGS and the emergency services network. This is now described with reference to Figure 4.

Figure 4 is a schematic diagram of another embodiment of the network of Figure 1. The same reference numerals are used as appropriate. An emergency services network 40 as known in the art of conventional switched telephone networks is connected to a packet-based communications network 41 via one or more media gateways 42. A conventional public switched telephone network 43 is also connected to the emergency services network 40 via any suitable type of interface such as an ISDN User Part (ISUP) interface, as is a conventional cellular network 44. In a preferred embodiment of the present invention an interface between the LGS 22 and the emergency services network 40 is provided using the same method as used to interface between location gateway entities in a cellular network and an emergency services network. At least part of the present invention lies in the realisation that an interface from a cellular network can be reused to integrate a packet-based network and a conventional emergency services network. Preferably the E2 interface standard defined in TR-45 J-STD-036 "Enhanced Wireless 9-1-1 Phase 2" Telecommunications Industry Association, 2000 is chosen although any other suitable interface method can be used. The aforementioned document is incorporated herein by reference.

Figure 4 shows the LGS 22 connected to the local and/or national ALI of the emergency services network 40 using an E2 emergency services protocol (ESP) as mentioned above. This ESP allows the emergency network to make a request for a caller location which is then delivered for display to a PSAP operator.

For example, the PSAP sends a query to the local ALI 17. In Figure 4 this query is referred to as ESPOSREQ (ESRK). The query contains details of the routing key and requests the associated geographical location information.

The local ALI 17 forwards the query (also known as a bid) to the national ALI 18 which in turn forwards the query to the appropriate LGS 22. The LGS has previously stored the routing key together with the geographical location information and so it is able to return the geographical location information to the national ALI. This is shown in Figure 4 as esposreq (Position). From there it is returned, via the local ALI, to the PSAP.

At the LGS, the cached routing key and location information are cleared from memory when appropriate. For example, after a pre-specified time interval or at the end of the emergency call. In the latter case, the call server 21 is arranged to send a message indicating call terminal to the LGS. The message is of any suitable form such as a subscriber location report.

More detail about particular examples of the present invention is now given.

Emergency Call Routing

For the sake of simplicity, the following discussion is based on the assumption that the Selective Router will use an ESRK provided in the ISUP call setup (IAM - Initial Address Message) to select the correct outgoing CAMA trunk for the corresponding serving PSAP. However, it is not essential to use an ESRK. Any suitable key such as an ESRD can be used instead.

Trunk Media Gateway (TMG) to Selective Router Routing

Opening up the VoIP network cloud, we can see that an emergency call needs to be delivered into the wireline voice network in order to enter the

existing emergency services network. In VoIP networks, this is done by transiting the call out of the IP network and into wireline network via a Trunk Media Gateway (TMG).

Since there are no dialed digits that can be used to effect routing of the emergency call (911 does not identify a unique destination), it is necessary for the TMG selected to have direct ISUP trunking capability to the selective router(s) that it supports routing to. To reuse the cellular mechanism for call routing, the TMG needs to provide a unique ESRK to the selective router. That is, the TMG ISUP signaling preferably supports the inclusion of this parameter in the IAM message. Further, if the TMG has outgoing trunks to more than one selective router, it needs to be instructed as to which trunk to select based on the ESRK. That is, in the absence of routing based on dialed digits, the TMG needs to be told which outgoing voice trunk and ISUP signaling destination to select based on the value of the ESRK for that call. This implies a routing table that the network will use to ensure that the TMG is appropriately directed.

Call Server to TMG Routing

Looking further back into the VoIP network cloud, we see that the VoIP call itself is under the control of a call server. This network entity provides at least the equivalent functionality of a wireline switch or a cellular mobile switching center. The call server is responsible for setting up the initial state associated with an emergency call and routing it to the correct destination.

As has been noted at each step, the dialed digits do not provide a definitive route to the destination and, as noted in the previous section, the TMG outgoing trunk needs to be selected based on the ESRK so the appropriate selective router is trunked to. Since the call is delivered to the TMG by the call server, it is the responsibility of the call server to provide this ESRK in the IP based call setup and corresponding trunk selection through the TMG.

Since the call server has the responsibility to select a TMG based on the ESRK, the existence of a routing table within the call server is implied. This table allows the call server to associate a TMG with a given ESRK value.

Location Based Emergency Call Routing

This section describes an example of how the call server determines the ESRK associated with final destination PSAP. This is addressed by the introduction of a new network entity called the Location Gateway Server (LGS). This network entity supports two key functions:

- On request from a call server, and given the identity of an emergency caller/client, it obtains the location of that client from the IP access network. For routing purposes, this location may be provided as a geodetic (latitude/longitude) location.

- Based on the location determined, and using a native spatial database capability which can identify an emergency services zone corresponding to a destination PSAP, it generates a unique and applicable ESRK value that will indicate a route to the correct serving PSAP.

A single message and response is defined between the call server and the LGS which is used by the call server to request the ESRK. These are the EmergencyCallRequest (ECR) and the ECResponse messages. The key parameters of the request and response are the client ID in the former and the ESRK in the latter.

A second message, ECTerminate, is also required to indicate the termination of the emergency call. The LGS maintains transient state information associated with emergency calls in progress. It needs to allocate an ESRK out of a pool of available numbers and it needs to be able to return the ESRK to this pool at the conclusion of the call. Thus, it is important for the call server to provide a message to the LGS indicating that the call is terminated. The ESRK associated with the call and provided in the call termination indication message provides the necessary state association for the LGS.

It is also possible for the call server to provide the initial location of the client in the message to the LGS. This is also useful in a situation where there is no LIS and clients/users specify their own location (e.g. picked from a menu).

Emergency Caller Location Delivery

The question of how an LGS determines the location of a client device is described later. Before looking into that question, the other aspect of location – the delivery of it to the PSAP operator – is examined.

As has been noted, the location of a VoIP client can be a transitory piece of information. As such, it is not adequate - as a general solution - to rely on a static data entry accessible by the emergency network and keyed against the CLID. As with cellular networks, the information associated with a subscriber should be determined, and is only valid, within the time that the call is active. Outside the period of duration of the emergency call, the emergency network stores no information and has no knowledge related to the identity or location of the subscriber.

In order to support Phase 2 E911 requirements, J-STD-036 defined the E2 interface between the ALI entities in the emergency services network and the location gateway entities (GMLCs and MPCs) in the connecting cellular networks. The emergency services protocol (ESP) supported over this interface was defined by both J-STD-036 and in the NENA publication mentioned above.

An embodiment of this invention teaches that this same E2 interface and ESP protocol specification be reused on the LGS to support the delivery of location information associated with VoIP emergency calls.

The ESRK becomes a reference to the call in progress as well as being the routing indicator used in call setup. ESP allows the emergency network to make a request for a caller location which can then be delivered for display to the PSAP operator. The LGS already has the location information for the client since it was used to deliver the call routing information. By caching this location in conjunction with the ESRK call-in-progress, state, the LGS is able to provide this location information in the esposreq sent in response to a request made over the E2 interface by the emergency network.

Mid-Call Location Updates

Since cellular subscribers can, by definition, be mobile, the ESP semantics also support the ability for the emergency network to request an updated location for the caller. Using the same call identifier (e.g. the ESRK) as was

used to request the location initially, the same ESPOSREQ message is used to request an updated location. That is, there is a parameter in this message to indicate which type of location - initial or updated - that the emergency network would like. If an updated location is required, the cellular network knows that it should utilize its resources to see if a more up to date location is available.

This same mechanism is used in an embodiment of the present invention for the VoIP network. While in initial deployments, the IP access networks may only return relatively static locations (e.g. from switch port wire mappings), future deployments will be able to exploit advanced positioning technologies that can track a mobile IP device, just as they can a mobile cellular device today. Since the semantics for requesting an updated location are already supported on the E2 interface, there will be no changes necessary to the emergency network in order for it to exploit this tracking capability.

Civic Address and Geodetic Location Support

The introduction of Phase 2 E911 support for cellular emergency callers introduced the concept, and the precedent, that the location of the caller may actually be provided to the PSAP as a geodetic location. This has necessitated changes to PSAPs such that to be Phase 2 capable they need not only the ability to display a location in this format to an operator but also that these PSAPs have the necessary procedures and policies in place to relay location information in this form to emergency response teams and be able deal with accuracy that can vary below 100 meters at the 67th percentile and approach arbitrary levels of inaccuracy for the other 1/3 of calls.

This precedent can be taken advantage of for VoIP clients where, in the absence of a civic address which can be displayed to the PSAP operator, a geodetic location - just as is used for phase 2 cellular location - is provided in an embodiment of this invention.

However, this does not mean that emergency calls from IP based voice networks need always be restricted to geodetic based location reporting. As discussed, the ESP signaling parameters as defined by NENA includes a parameter called "location description". The NENA specification defines a

number of different XML tag based fields that can be used to constitute this parameter. This opens the possibility that the LGS, in responding to an ESPOSREQ request over the E2 interface, can utilise this parameter to also provide a civic address for the caller.

In cellular systems, this parameter has a nominal use around supporting phase 1 capable PSAPs where the location description provided will generally correspond to a street address identifier for the serving base station in the cellular network. However, this use does not preclude the alternative use in IP based voice networks.

Where VoIP clients have a relatively static location - for example, where the client is a conventional telephone form factor device with a relatively fixed desktop location - then the access network, which provides location to the LGS, may opt to provide a civic address encoding in addition to the geodetic location. A discussion on general location determination and the associated signaling is given below.

A valid question is how the emergency services network can know that it is receiving a civic address for the caller rather than a nominal base station address. This can be discriminated in a number of ways. The key is that the emergency network can be aware that it is interfacing to an IP based voice network rather than a cellular network. Three potential ways to perform this discrimination are:

- The emergency network will generally select the E2 interface that it needs to send a request to on the basis of the ESRK associated with the call. ESRKs tend to be allocated to network operators in pools. This same association can allow the emergency network to infer the nature of the connecting network.

- The esposreq response contains a parameter which is the Company ID. This can be used by the emergency network to distinguish IP vs cellular carriers.

- The position data parameter in the esposreq which contains the geodetic location also contains a sub-parameter called "position source" which indicates the technology used to establish the location.

New code points can be allocated for IP network positioning technologies. This could be used by the emergency network to establish that the location is being provided by an IP voice network.

The example mechanisms discussed above identify how the existing cellular E911 phase 2 infrastructure and interfaces in the emergency network can be effectively reused with little or no modification to support the delivery of caller location from IP based voice networks.

In order to minimise the need to transform and translate the information related to location, in a preferred embodiment the specifications used for this on the E2 interface are reused within the signaling of the IP network. That is the geodetic location coding defined by NENA in the document referred to above as well as the XML tag encodings defined in "Real Time ALI Exchange Interface Agreement – Issue 6.1", AT&T and Pacific Bell, March 25, 1995 by NENA are also preferred for use between the IP network elements as they are delivered through to the LGS.

End to End – Adding Location Determination

There are numerous approaches to location determination within IP networks and any suitable approach can be used in the present invention. A number of things will affect the type of solution put in place. Amongst these are:

- The nature of the connection used by the client. That is, whether it is a domestic broadband connection, an enterprise IP switch connected client, a wireless client connecting via a campus wireless LAN, etc.
- Legacy circumstances. That is, the extent to whether the clients, access devices, and switches have native support for location delivery versus the need to overlay a solution for location determination on existing infrastructure.
- The type of location information and accuracy required for a given target environment. For example, are static civic addresses with sufficient geodetic accuracy for routing sufficient or is a more accurate geodetic location required in the absence of a civic address?

The NENA website itself has a number of submissions and proposals around different positioning technologies for IP and any one of these may be adopted in a given access network.

The Location Identification Server – LIS

An embodiment of this invention proposes that an intermediate network entity be defined which provides a uniform query interface to the LGS network element such that it need not be concerned with the nature of the positioning technology used.

The newly identified network element is the Location Identification Server (LIS). This network element sits between the LGS and the access network and invokes the applicable positioning technologies. It supports a simple request/response message that allows the LGS obtain the location of a client.

Client Identifier Options

In order to do this, the LGS needs to provide a client identifier which is meaningful to the LIS and significant within the access network that the client is attached through. Types of potential client identifier vary but some candidates are:

- Ethernet MAC address
- MSISDN - international encoding of corresponding dialable digits
- RFC 2486 Network Address Indicator - user@realm style address
- SIP URL address
- Some other network element, e.g. LIS, generated handle to the client that is independent of other addressing schemes.

The above list is by no means definitive but the definition of the query messaging between the LIS and the LGS is defined such that these and other forms of client identification can be supported over this interface. An important driver of the form of client identification supported is which identifier can be provided by the call server function in its request to the LGS. Any practical

network deployment will need to ensure that the same client identifier form can be used meaningfully by the call server, LGS, and LIS.

By way of example, in initial implementations of this architecture where the access network and client devices are largely legacy, and without native location determination capabilities, the likely candidate for many deployments may be the MAC address.

An example of an end to end solution using a LIS that employs SNMP bridge MIB polling and MAC address association is described below with reference to Figure 7.

Geodetic vs Civic Address Location – revisited

As discussed above, location may be provided as a geodetic location for the purposes of call routing plus, optionally, a civic address that can be displayed to the PSAP operator. The parameter in the response message from the LIS to the LGS that specifies the returned location preferably supports a coding that supports both of the location formats concurrently. The geodetic location is provided in order to support emergency call routing. Also as discussed above, it is preferred that the specifications used for coding location are the same as those on the E2 interface. That is the geodetic location coding as well as the XML tag encodings defined by NENA are preferably used to encode the location provided to the LGS by the LIS. This eliminates the need to translate and transform this information as it is passed from the LGS to the emergency services network.

The architecture that has been described herein - from the LIS through the LGS, call server, and PVG network entities interfacing to the emergency services network ISUP and E2 interfaces - should meet the needs of emergency calling from VoIP networks well into the future. Further, as more standardisation occurs at the IP access and native positioning support is deployed, this transition to more reliable and accurate location determination will be able to occur seamlessly without impacting the VoIP to emergency network interface. The changes will be perceived as an improvement in coverage and quality of service for VoIP emergency callers as well as ease of

deployment for VoIP operators but without impacting the operation of the emergency network generally.

In addition to the above, as the emergency network infrastructure evolves away from the current legacy of CAMA trunks and PAM interfaces, individual PSAPs will be able to interface directly to the IP network. The same functions of call routing and location delivery will still be needed and the mechanisms described can still be utilized. Instead of routing out to ISUP trunks, the call server can direct the call to a direct VoIP based ACD function. The ESP messaging referred to above is already IP based and the option becomes available for updated PSAPs to query the LGS directly instead of their requests being proxied through an ALI.

Using DHCP to improve client integration

Since the identity, location, and capabilities of the LIS will vary from access network to access network, it is preferred that in some embodiments DHCP be used to advise IP clients of the identity of the serving LIS. This permits two major optimisations:

- The client will be able to explicitly register with the LIS so that it is known to that entity for purposes of location. This will also establish a signaling relationship that can be used for advanced positioning mechanisms if supported. It also offers the opportunity for the LIS to assign a client-specific identifier which the client can provide to network services such that no other client key is required for the purposes of location requests through the LGS/LIS network.

- The call setup signaling to the call server can be modified to support the ability of the client to forward the serving LIS identity to the call server. This in turn can be communicated as part of the location request to the LGS, permitting the LGS to have explicit knowledge of the appropriate LIS to query.

These embodiments are illustrated in Figure 5.

Supporting international emergency calling

It is an interesting characteristic of VoIP networks that the distance between a client user and the call server handling the call processing may be arbitrarily great. A VoIP client can typically use the same call server regardless of the point of attachment to the network. So, the client may be in a different city, a different state, or even a different country.

It has been an implicit assumption in the discussion to date, that the call server has inbuilt knowledge of the LGS that it should inform of the incidence of an emergency call and request routing information from. While this may hold true of a nationwide carrier with points of presence across many states, it may prove difficult for some VoIP network operators to provide the same ubiquity of presence. When the question of supporting international calling is raised, then it becomes even less likely that this assumption will apply.

This constraint will likely continue for the short term. However, the use of DHCP may, in the future, also provide a mechanism for dealing with this. In this instance, the registration of a client on a local network involves not only an indication of the serving LIS identity but also an indication of the applicable emergency LGS (eLGS).

With this facility, the client can provide the eLGS identity to the call server. This introduces the possibility of a network of regional LGS platforms to serve the VoIP network. The ESRK allocation pools can be efficiently distributed between these LGS and they can retain the responsibility of maintaining the spatial boundary information for the emergency service (PSAP) zones in their regions.

The signaling associated with this scenario is also shown in Figure 5. Note that the call server was able to refer to an eLGS in the visited network rather than the one in the subscriber's home network. This allowed the appropriate ESRK for the PSAP in the visited network operator's region to be allocated by that operator. Further, the PSAP in that region only needs to have an E2 interface association with that network's LGS and not the home network LGS.

The arrow labeled in Figure 5 shows that the DHCP server provides LIS and eLGS identities to the client on initialization. Arrow 1a represents the optional step whereby the client registers with the LIS to establish a signaling

relationship for future positioning. As shown by arrow 2 the client then provides eLGS and LIS identities to call server on emergency call initiation. Then in the step shown by arrow 3 the call server provides LIS identity to eLGS in emergency call request.

Enterprise Versus Carrier VoIP Network Deployment

In the embodiments described so far it has been an assumption that the VoIP network operator has sufficient points of presence in each of the regions of interest to be able to route the emergency calls onto the local network and into the emergency services network. This is typically true of a public carrier network which operates its own PVG platforms that tandem directly into the public wireline network but it is less likely for an enterprise operating a VoIP network over its intranet.

In the case of an enterprise VoIP operator, this may not be an issue where the PABX or other PSTN gateway utilised by that enterprise is colocated with its user population. However, if the user population is widely geographically distributed via a wide area intranet and/or VPN links and they share a common PSTN gateway, then there is no native mechanism to support routing to the correct PSAP.

- For a colocated user population, the class 5 switch in the local operator network which provides the enterprise service looks after the subsequent routing of the 911 call to the correct selective router and PSAP.

- This local exchange interface does not support the use of an ESRK in the call setup signaling to indicate a preferred route and a local exchange will not tend to support the necessary trunking to remote selective routers for out-of-region callers.

- For small and medium enterprises, it would not necessarily be economical to operate an LGS nor would it be optimal to distribute ESRK pools around arbitrary numbers of enterprises.

Despite these constraints, it is still desirable to utilise the embodiments that have been described herein as the challenge of routing calls from geographically distributed callers needs to be addressed. While there are alternative proposals these tend to rely on direct dialing local access numbers for PSAPs. While this is effective in the short term, it is by definition bypassing the existing mechanisms and processes for emergency call distribution.

At least two possible approaches to supporting the enterprise environment in the long term exist.

- Through the standards process, the local operator switch interface could be modified such that the ESRK can be delivered in the call setup.

This approach has a number of limitations including the fact that the time lag in defining this signaling and having switch vendors implement and deploy it can be very large. More significantly, it doesn't address the concern that the local operator and switch is unlikely to maintain direct trunks to all required destination selective routers.

- Enterprises can seek emergency service support from public network carriers that support VoIP deployments. This means utilising the LGS and PVG resources of the public carrier but only for the purposes of emergency call routing.

In this situation, the enterprise would still provide the LIS functionality within their intranet IP access. Using the equivalent of the DHCP mechanism described above, the enterprise client can be advised of the carrier LGS applicable to emergency calls in that location and relay this to the call server at call setup. At the same time the identity of the serving LIS can also be relayed via the call server to the LGS.

This arrangement is illustrated in Figure 6.

Figure 7 shows a simplified example of a VoIP deployment where the network operator is a carrier 70 and the subscriber population are within enterprise managed networks 71, 72. That is, this shows virtual private voice network

deployment, where the call services are operated on an IP network with call serving functionality outsourced from the enterprise to the carrier.

In this example, it is assumed that each of the enterprises operates the voice network under the constraint that all voice clients need to be connected via specific IP switches supporting a standard SNMP bridge MIB 73 that permits port scanning to occur and also permits the MAC address of connected clients to be retrieved.

Further, the client implementation and protocol are conventional but include the delivery of the client MAC address as part of the native call signaling with the call server.

These constraints permit the operation of the network such that the MAC address can be used as a query key between the call server and LGS (Lv) interface and the LGS and LIS (Li) interface. The LIS implementation in this case involves the continuous SNMP polling of managed switches according to provisioned data which includes the list of managed switches, their ports, and the nominal location of the end-cabling attached to those ports - as both a geodetic location and, optionally, a civic address. On each poll cycle, the LIS stores any connected MAC address values against the port records within this wire map.

A query to the LIS from the LGS, then, simply results in the stored location information in this wire map being keyed from the provided client MAC address in the query. This location information is returned for subsequent processing by the LGS as described herein.

This example illustrates how the complexities of location determination in the access network are abstracted away from the rest of the emergency call handling. Other examples of LIS implementations would be those that could map a DSLAM port to a physical home address location for ADSL broadband internet based subscribers. Again, the details of how this particular LIS performed this function would be hidden from the rest of the VoIP network.

This embodiment provides the advantage that there is now a seamless migration path to native positioning systems that will not impact the network beyond the access interface to the LIS.

Call Back Number Considerations

One of the current limitations of the existing emergency services network is the ability to support callback number reporting to the PSAP where that callback number exceeds the number of digits used for a normal local dialable number. Examples of callback numbers that may not be supported are:

- International callback numbers such as international roaming cellular callers or, in future, international roaming VoIP callers.
- Enterprise callers to emergency services where the terminal callback number is not delivered in the call setup information.

The use of E2 as a dynamic query interface also facilitates the delivery of callback information. Since this information is delivered out of band from the call setup, it isn't subject to the same constraints as imposed by the selective router and CAMA trunk infrastructure.

The callback number is one of the parameters in the esposreq message in ESP. This allows the originating voice network which uses the E2 interface the ability to deliver an appropriate callback number, if available, for the particular call in progress. The LGS then can also be used to query the access network or be informed by the Call Server, as appropriate, of a callback number to cache in anticipation of the PSAP query.

Figure 8 is a message sequence chart showing a consolidated end to end signaling flow for several of the embodiments described herein. It includes the scenario of a mid-call location update request from the PSAP.

CLAIMS

1. A method of providing a routing key for routing an emergency call from a packet-based communications network node to an emergency services network node in a switched telephone network, said method comprising the steps of:

(i) at a node in the packet-based communications network, receiving information about the geographical location from which the emergency call originates;

(ii) generating a routing key on the basis of the received information and pre-specified information about geographical locations served by particular emergency service network nodes.

2. A method as claimed in claim 1 wherein said step (i) further comprises receiving at the node a call-back number from which the emergency call originates.

3. A method as claimed in claim 1 which further comprises storing said generated routing key together with the received information about geographical location at the node in the packet-based communications network.

4. A method as claimed in claim 3 which further comprises providing the stored information to the switched telephone network for receipt by a public safety answering point (PSAP).

5. A method as claimed in claim 4 wherein said stored information is provided via an E2 interface.

6. A packet-based communications network node for providing a routing key for routing an emergency call from the packet-based communications network to an emergency services network node in a switched telephone network, said node comprising:

(i) an input arranged to receive information about the geographical location from which the emergency call originates;

(ii) a processor arranged to generate a routing key on the basis of the received information and pre-specified information about geographical locations served by particular emergency service network nodes.

7. A packet-based communications network comprising a node as claimed in claim 6.

8. A method of routing an incoming emergency call in a packet-based communications network to an appropriate emergency services answering point in a switched telephone network, said method comprising:

(i) at a packet-based call server, receiving the emergency call;

(ii) at a location gateway server, receiving a geographical location from which the call originated and using that to generate a routing key;

(iii) at the call server, routing the emergency call using the generated routing key.

9. A method as claimed in claim 8 wherein said geographical location information is received at the location gateway server as a result of polling a location information server.

10. A method as claimed in claim 8 wherein said geographical location information is received at the location gateway server from the call server.

11. A method as claimed in claim 8 wherein said emergency call comprises a geographical location from which the call originated.

12. A method as claimed in claim 8 wherein said packet-based communications network is a voice over internet protocol network.

13. A method as claimed in claim 8 wherein said emergency call originates from a nomadic entity.

14. A method as claimed in claim 8 which further comprises, at the location gateway server, storing the generated routing key together with the determined geographical location.

15. A method as claimed in claim 14 which further comprises making the stored information accessible to an automatic location identification node in an emergency services network.

16. A computer program stored on a computer readable medium and arranged to control a location gateway server in a packet-based communications network in order to carry out the method of claim 1.

1/8

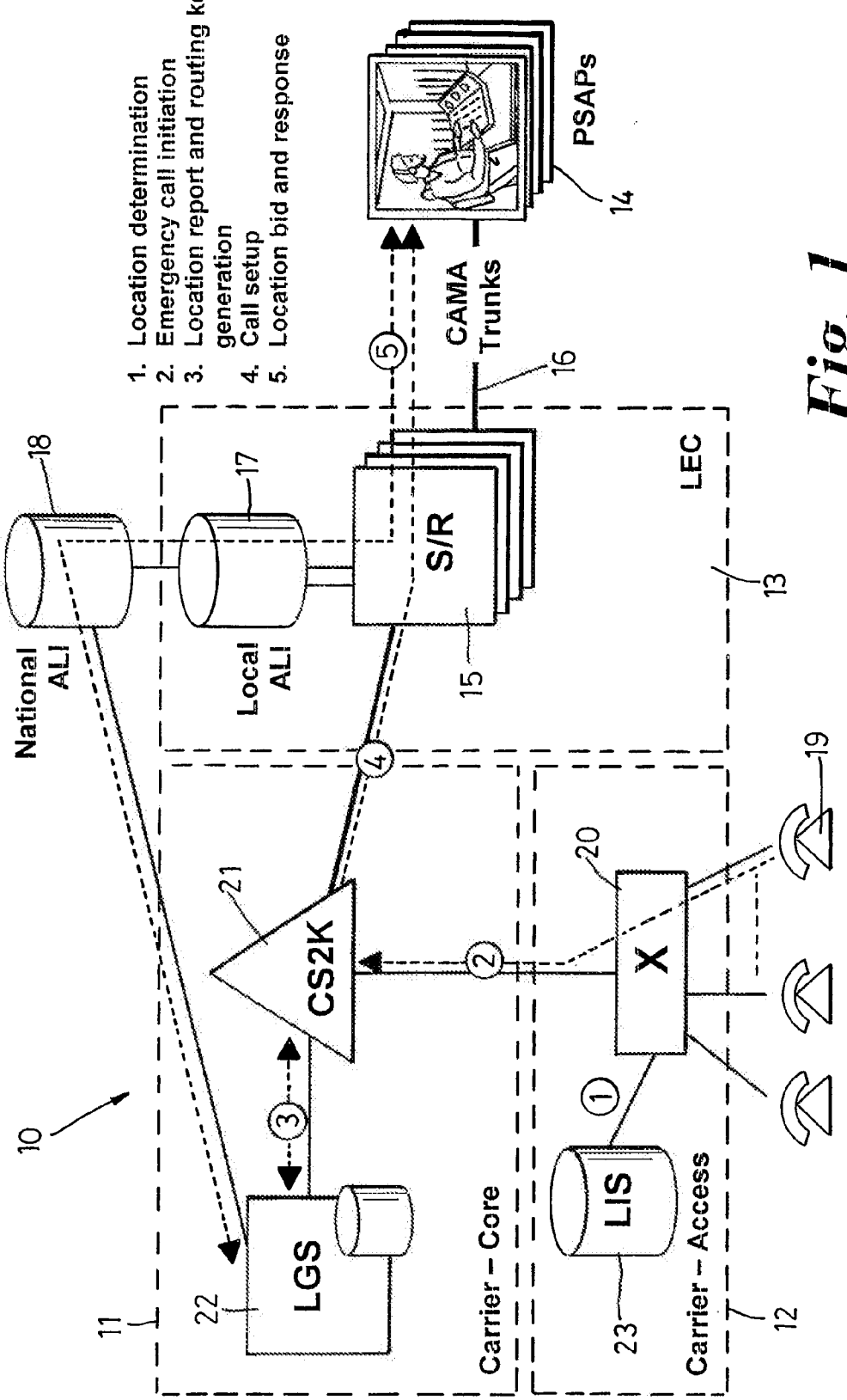


Fig. 1

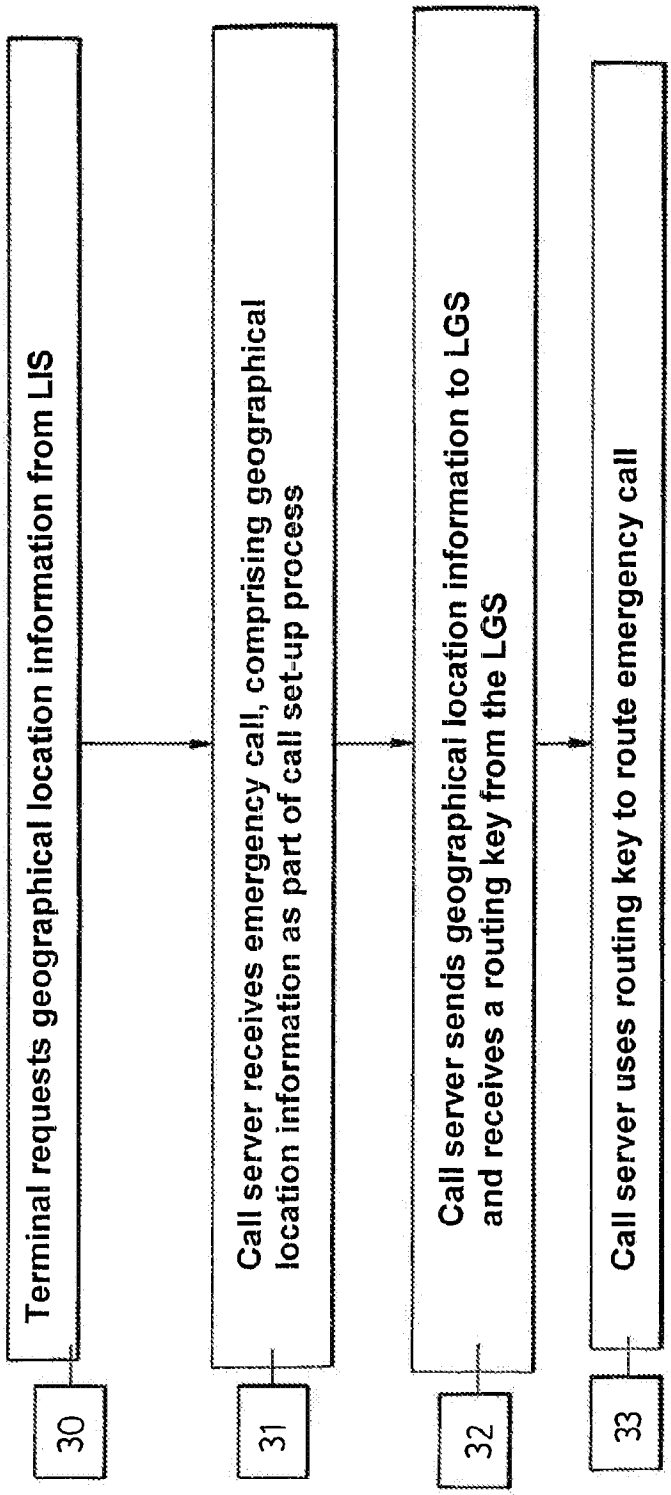


Fig. 2

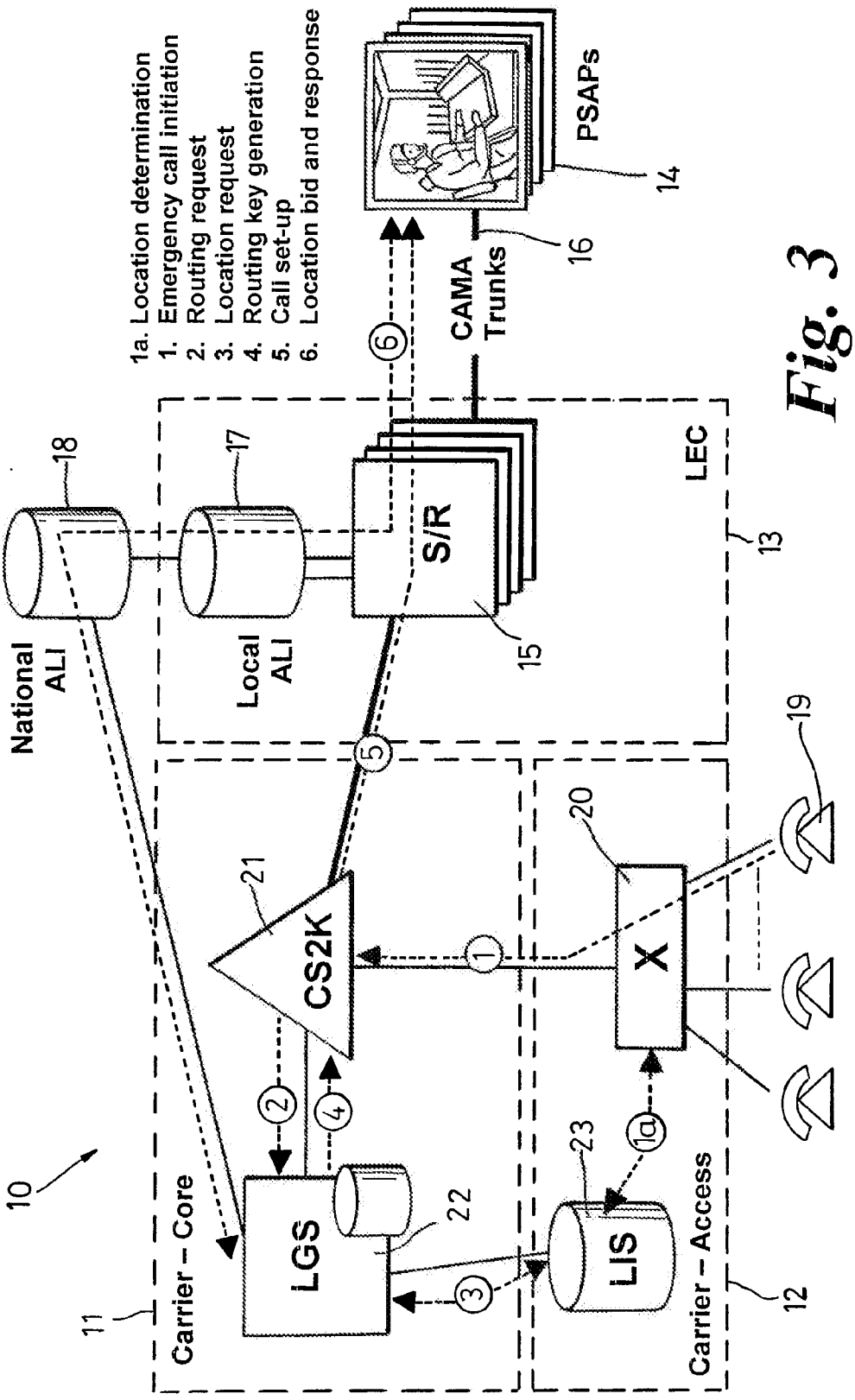


Fig. 3

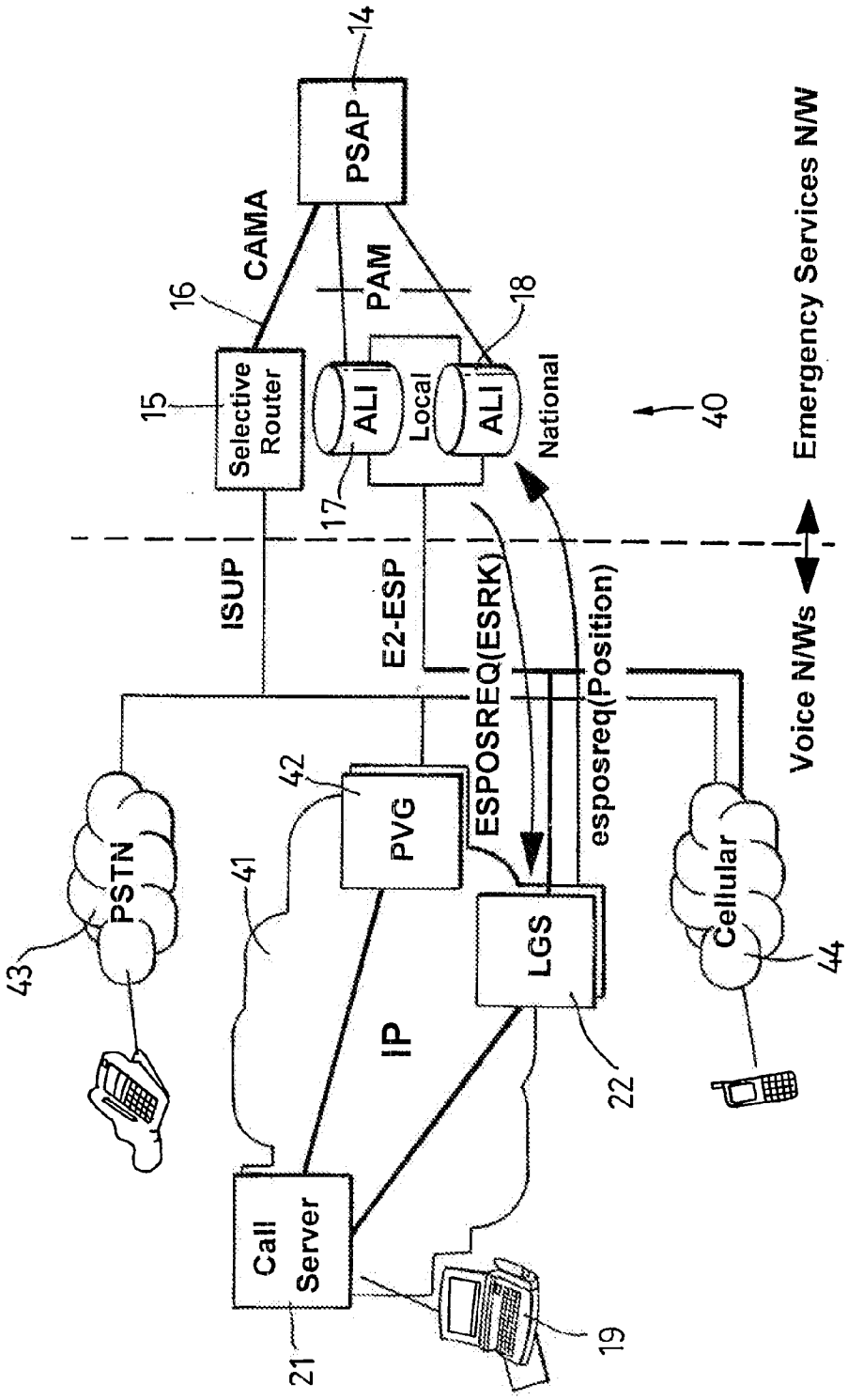


Fig. 4

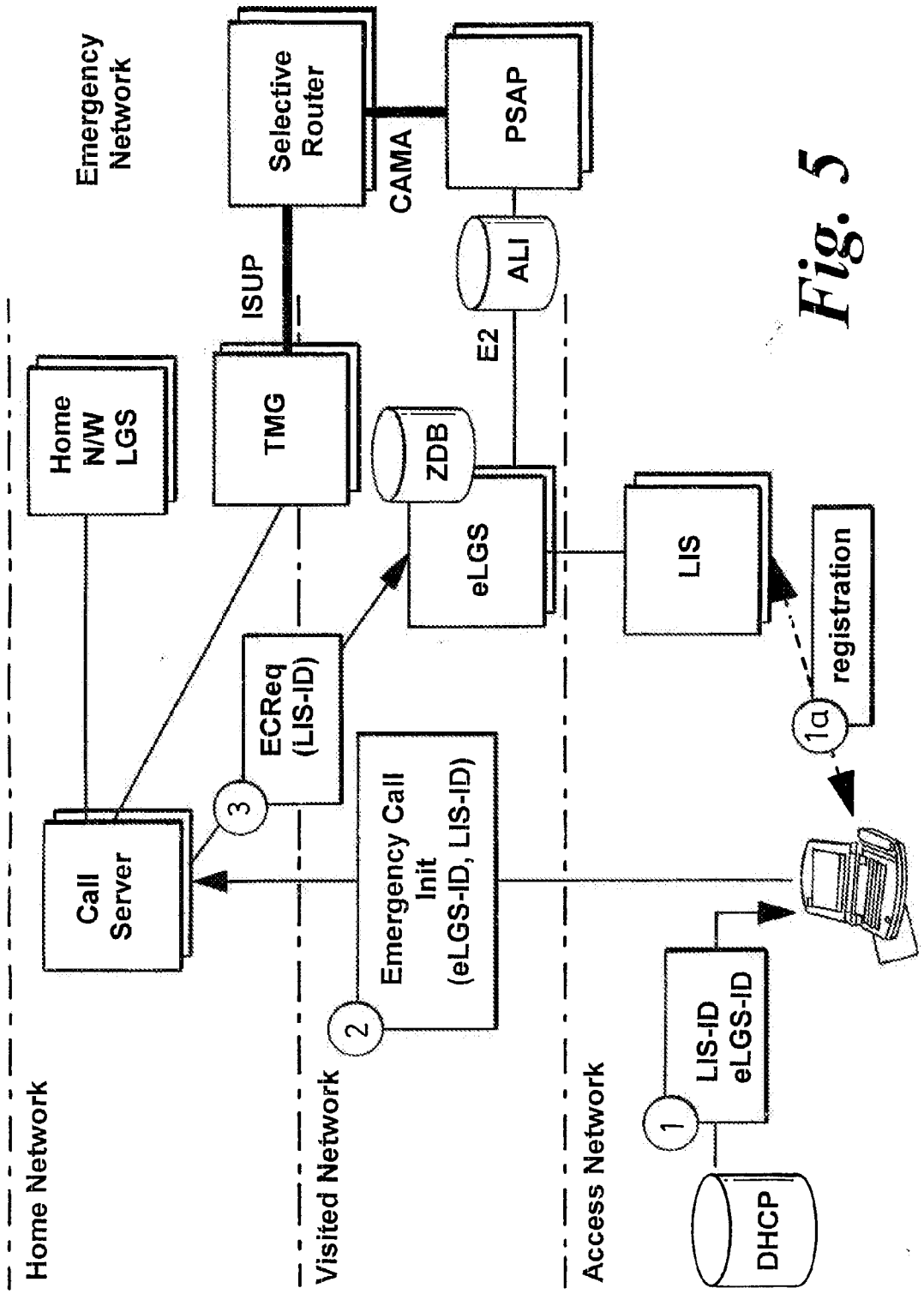


Fig. 5

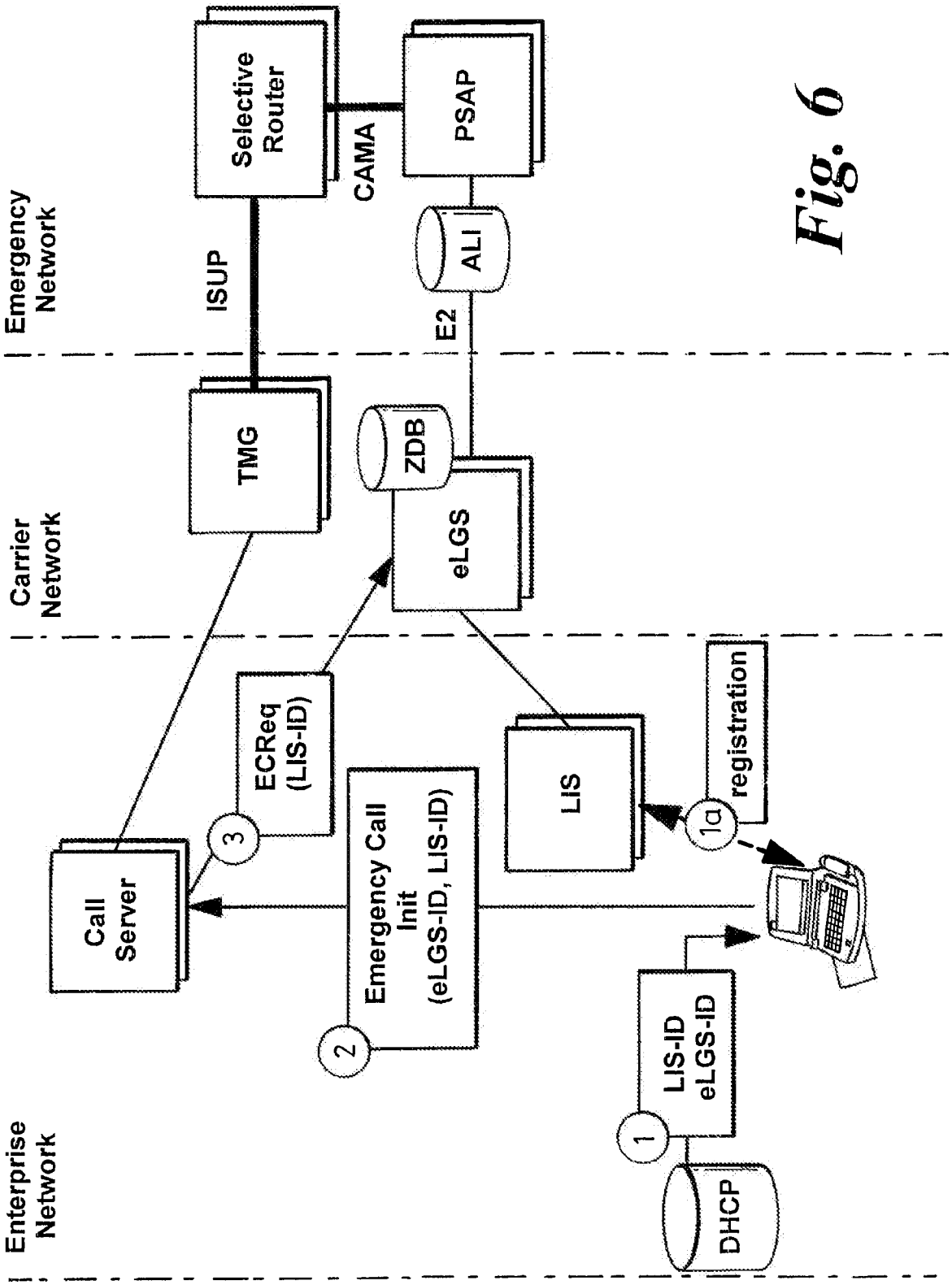


Fig. 6

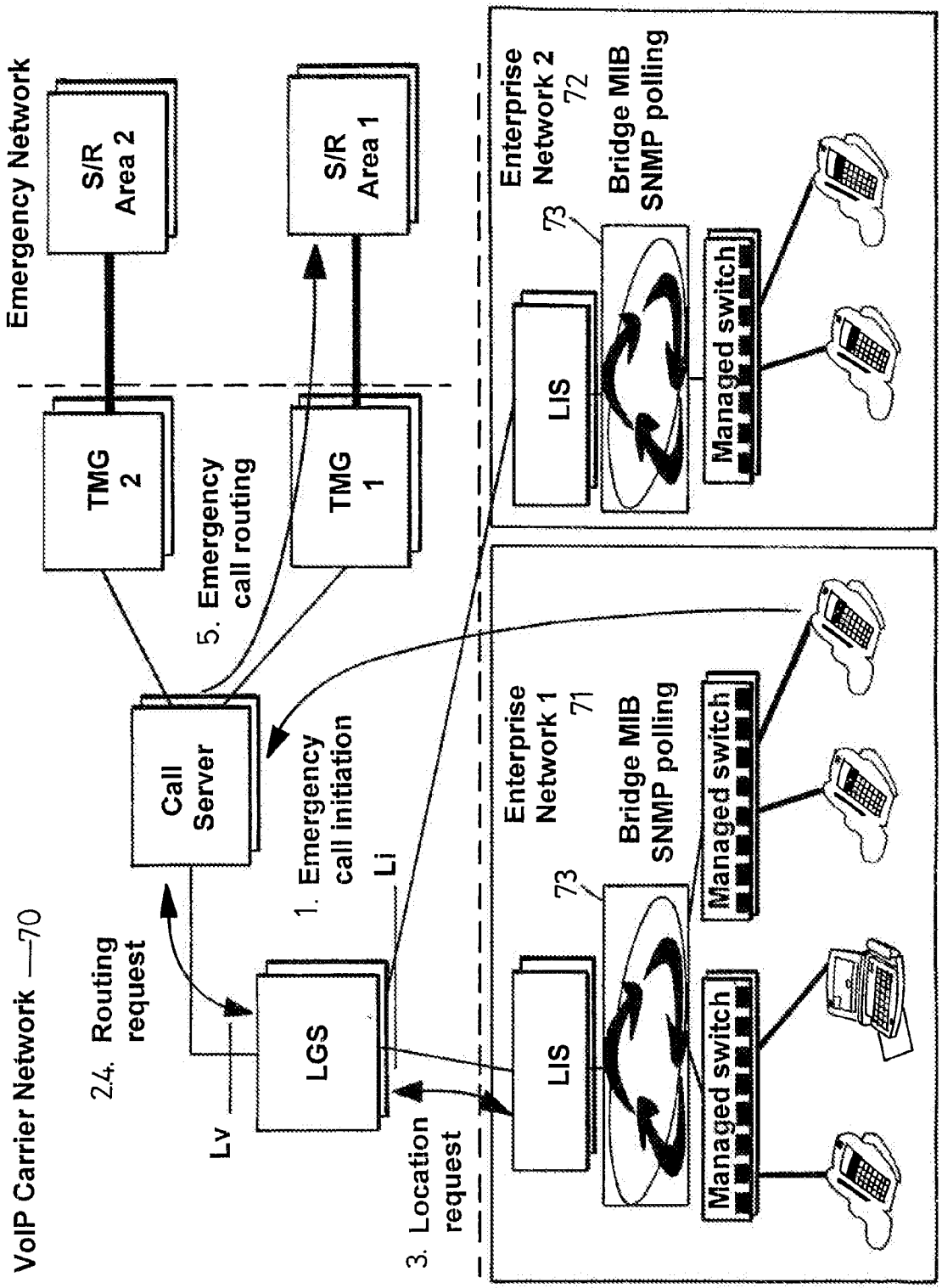


Fig. 7

8/8

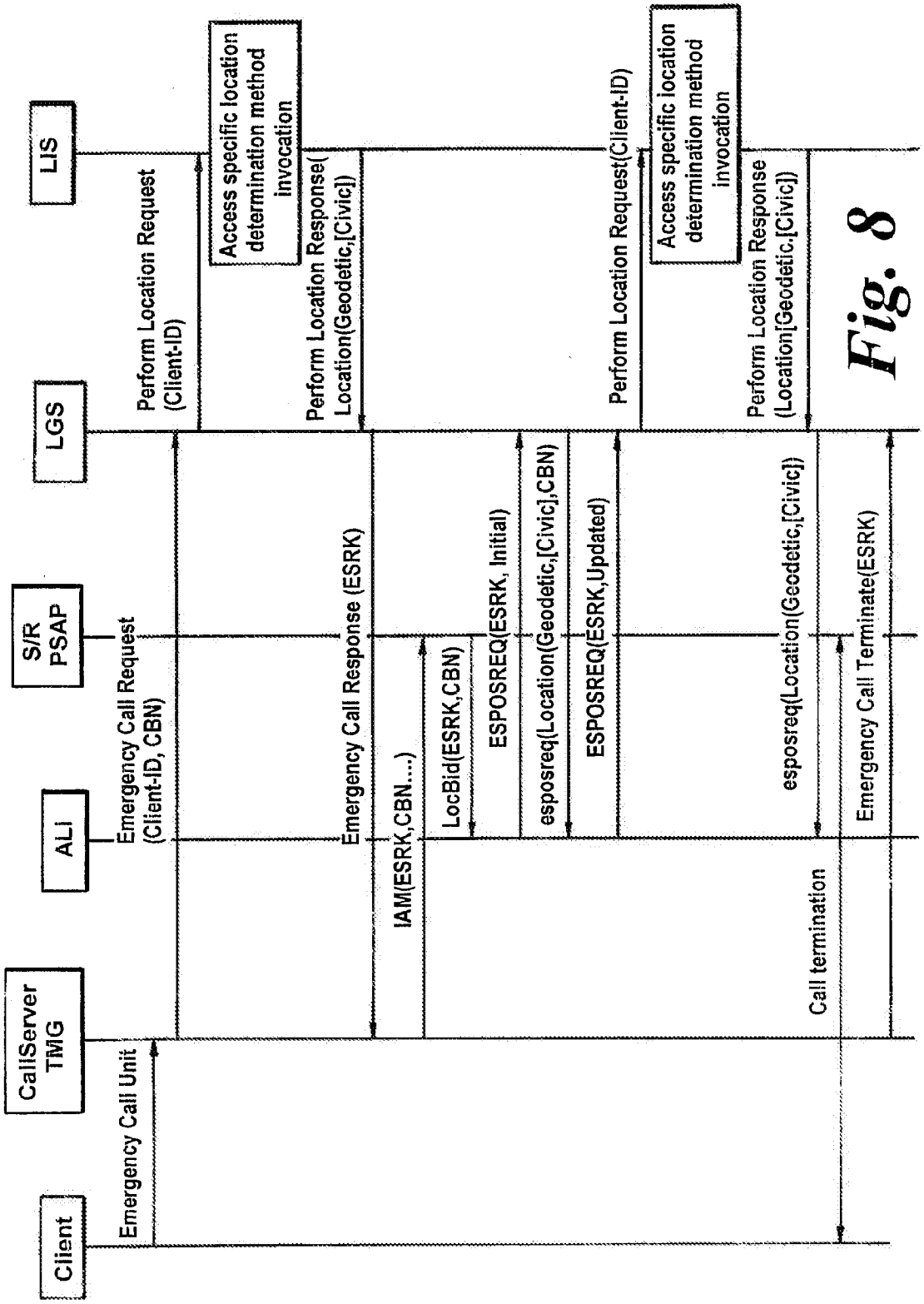


Fig. 8

INTERNATIONAL SEARCH REPORT

Ir ıl Application No
PCT/GB2005/000612

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M7/00 H04M3/42

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 587 545 B1 (ANTONUCCI JAMES T ET AL) 1 July 2003 (2003-07-01) abstract column 1, line 1 - line 18 column 2, line 52 - column 3, line 12 column 11, line 33 - line 52 column 11, line 65 - column 12, line 8 column 12, line 59 - column 13, line 11 column 13, line 25 - line 48 column 14, line 35 - line 43 column 15, line 52 - column 16, line 54	1-16
X Y	US 2003/227922 A1 (HORVATH ERNST ET AL) 11 December 2003 (2003-12-11) paragraphs '0009!, '0015! - '0020!, '0027!, '0030!, '0032!, '0034!, '0035!, '0043!, '0046!, '0048!, '0050! - '0053!	1,3-16 2

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 May 2005	24/05/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Willems, B

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/GB2005/000612

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/108175 A1 (POIKSELKA MIIKKA ET AL) 12 June 2003 (2003-06-12) paragraphs '0001!, '0002!, '0004!	2

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

'ormation on patent family members

Int ial Application No
PCT/GB2005/000612

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6587545 B1	01-07-2003	CA 2381317 A1	13-09-2001
		EP 1188302 A1	20-03-2002
		WO 0167733 A1	13-09-2001
		US 6690932 B1	10-02-2004
		US 2001028711 A1	11-10-2001
US 2003227922 A1	11-12-2003	DE 10223980 A1	08-01-2004
		CA 2429878 A1	29-11-2003
		EP 1367807 A1	03-12-2003
US 2003108175 A1	12-06-2003	AU 2002353273 A1	17-06-2003
		EP 1452049 A1	01-09-2004
		WO 03049467 A1	12-06-2003

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 June 2006 (29.06.2006)

PCT

(10) International Publication Number
WO 2006/067269 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04Q 7/38* (2006.01)
H04L 12/28 (2006.01)

(21) International Application Number:
PCT/FI2005/000540

(22) International Filing Date:
20 December 2005 (20.12.2005)

(25) Filing Langnage: English

(26) Publication Language: English

(30) Priority Data:
20041659 23 December 2004 (23.12.2004) FI

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KALLIO, Juha** [FI/FI]; Gunillantie 7 A 10, FI-00870 Helsinki (FI).

(74) Agent: **PAPULA OY**; P.O. Box 981, (Mechelininkatu 1 A), FI-00101 Helsinki (FI).

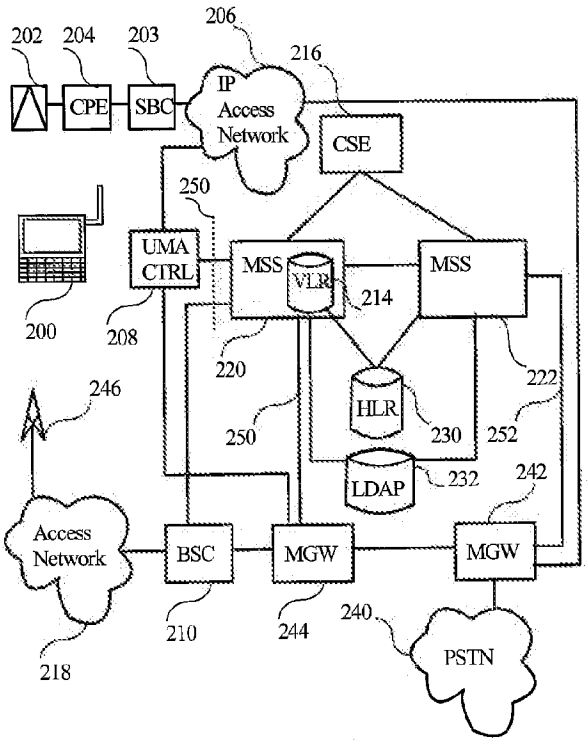
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, 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:
— *with international search report*

[Continued on next page]

(54) Title: METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM



(57) Abstract: The invention relates to a method a method for routing calls and messages in a communication system. In the method a mobile station registers to a call control node using a logical name. The logical name is mapped in a directory to an international mobile subscriber identity. The call control node performs a location update to a home location register using the international mobile subscriber identity. The mobile station is reached using a called party number. As a terminating call or message is received to a core network, a roaming number is allocated for the mobile station, and the call or message is routed to the call control entity currently serving the mobile station. The call control node translates the called party number to the logical name using the directory.

WO 2006/067269 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

TITLE OF THE INVENTION

METHOD FOR THE ROUTING OF COMMUNICATIONS TO A VOICE OVER INTERNET PROTOCOL TERMINAL IN A MOBILE COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

Field of the invention:

The invention relates to routing in mobile communication systems. Particularly, the invention relates to the routing of communications to a Voice over IP (VoIP) terminal in a mobile communication system.

Description of the Related Art:

Recently Wireless Local Area Networks (WLAN) have become important in mobile communications. The advantage of WLANs over licensed band cellular communication systems such as the Universal Mobile Telecommunication system (UMTS) and Global System of Mobile communications (GSM) lies in the facts that they use an unlicensed band and the cell sizes are much smaller. These facts make possible to build private WLANs operated by small corporate entities and individual users. The cost of wireless communication in these WLANs is significantly cheaper than in licensed band cellular systems. WLANs have mostly been used for Internet access, but the idea of providing voice communications over WLANs has recently gained momentum. In order to obtain a wide market share for voice over WLAN technologies and to provide a reliable service experience for end-users, it is necessary to be able to provide dual system terminals, which support both WLAN and licensed band based radio access. In other words, it must be possible for users to roam in both WLANs and licensed band cellular systems. Usually WLAN radio access is used in urban areas where there exists

a WLAN infrastructure, whereas licensed band cellular systems are used in areas outside the WLAN coverage.

3G Partnership Project has standardized the IP Multimedia Subsystem (IMS) in order to cater for VoIP and other IP based multimedia services. Typically, a UMTS Radio Access Network is used to access a core network, which supports the IMS. However, existing circuit switched core network infrastructures, which comprise Mobile Switching Centers (MSC), Home Location Registers (HLR), Visitor Location Centers (VLR), Camel Service Entities (CSE) and Service Control Points (SCP), provide a wide range of services. When operators wish to accommodate dual system terminals with both WLAN and licensed band radio access capabilities, it would be beneficial, if the operators had some mechanism of offering same services over both radio access technologies. Especially, the providing of backward compatible service is important. In other words, it is necessary to be able to provide familiar look-and-feel services from the licensed band cellular system also in the WLAN side. These services are referred to as the legacy services. Examples of such services include call forwarding, prepaid, premium rate and free service numbers, call waiting and call transfer. Usually, prepaid service and service numbers are provided using Intelligent Network infrastructure comprising MSCs and SCPs. In the 3GPP standardized version of Intelligent Networks the SCPs are referred to as the CSEs.

Reference is now made to Figure 1, which illustrates the problems associated with the providing of legacy services for dual system terminals in prior art. Figure 1 illustrates the fact that in practice the legacy services must be rebuilt in the IMS. In IMS the network elements and the protocols are largely different so this represents a significant effort. In Figure there is a Mobile Station (MS) 100, which is a

dual system mobile station capable of communicating both over a WLAN radio access and a licensed band radio access. The licensed band radio access may be, for example, a Time Division Multiple Access (TDMA) based GSM radio access or a Wideband Code Division Multiple Access (WCDMA) based UMTS radio access. In Figure 1 there is also a WLAN 124, which communicates with an IP Multimedia Subsystem (IMS) comprising at least a P-CSCF 102, an I-CSCF 104, an S-CSCF 106, a MGCF 120 and a MGW 122. Multimedia communications to and from MS 100 when in the area of WLAN 124 are provided via IMS. WLAN 124 is connected to Media Gateway (MGW) 122, which converts IP-based user plane traffic to circuit switched PSTN 126. WLAN 124 communicates also with Proxy Call State Control Function (P-CSCF) 102. Signaling plane traffic is routed to a P-CSCF such as P-CSCF 102. The signaling plane traffic is, for example, Session Initiation Protocol (SIP) based. SIP is defined in Internet Engineering Task Force (IETF) document RFC 3261. P-CSCF 102 is used to access Inquiring Call State Control Function (I-CSCF) 104, which determines using a Home Subscriber Server (HSS) 108 Serving Call State Control Function (S-CSCF) 106 in which a given subscriber is currently registered. The S-CSCF controls the multimedia communications originating from and terminating to MS 100. The S-CSCF communicates with Media Gateway Control Function (MGCF) 120, which converts signaling plane traffic into circuit switched signaling. For example, MGCF 120 converts the SIP signaling used between MS 100, P-CSCF 102, I-CSCF 104, S-CSCF 106 and MGCF 120 into the ISDN User Part (ISUP) signaling used in PSTN 126. MGCF 120 also controls MGW 122 using, for example, International Telecommunications Union (ITU-T) H.248 protocol. S-CSCF 106 is connected to three service platforms, namely Application Server (AS) 110, CSE 116 and Open Service Architecture (OSA) server 118. S-CSCF 106 is connected

to CSE 116 via IP Mobility (IM) Service Switching Function (SSF) 112. S-CSCF 106 is connected to OSA server 118 via Service Capability Server (SCS) 114.

In Figure 1 there is also a GSM/UMTS BSS 160, which is connected to a GSM/UMTS circuit switched core network comprising at least an MSC 150, a VLR 152, a GMSC 156, an HLR 154 and a CSE 158. GSM/UMTS BSS 160 is connected to MSC 150. MSC 150 comprises also a VLR 152. MSC 150 is connected to GMSC 156. There is also HLR 154, which stores subscriber data pertaining to the location of subscribers and their service data. GMSC 156 is also connected to PSTN 126. CSE 158 controls GMSC 156 and MSC 150 in the providing of IN services to the subscribers served by BSS 160. CSE 158 has also an interface to HLR 154, which allows the enquiring and modifying of service data in HLR 154. A plurality of standardized supplementary services is implemented directly by MSC 150, GMSC 156, VLR 152 and HLR 154. Examples of such services include call forwarding, call waiting, call transfer, call completion to busy subscriber, closed user group and call barring. In addition to these there may be a variety of vendor specific supplementary services implemented directly in these network elements. In order to cater for the aforementioned legacy supplementary services a variety of service functionalities are present in MSC 150, GMSC 156, VLR 152 and HLR 154. These service functionalities are illustrated in Figure 1 as service functionality sets 170-174. Each service functionality set may comprise a number of different service functionalities hosted in a given network element.

In order to support the same legacy services while MS 100 is in the service area of WLAN 124, the service functionality sets 170-174 must be ported to corresponding IMS network elements comprising at least P-CSCF 102, I-CSCF 104, S-CSCF 106 and HSS 108. This represents a significant task since all the develop-

ment effort put in the service functionality sets 170-174 must be repeated when equivalent service functionality sets 180-184 are implemented in IMS network elements. For example, service functionality set 170 in MSC would correspond to service functionality set 182 in S-CSCF 106 and service functionality set 171 in CSE would correspond to service functionality sets 181, 183 and 184 in AS 110, CSE 116 and OSA server 118, respectively. However, the correspondence is not direct and obvious. It is sufficient to say that the work in the porting of legacy service functionality sets from the GSM/UMTS circuit switched core network to IMS side is non-trivial since the protocols used between the IMS network elements and the MS 100 are largely different from the ones used in GSM/UMTS circuit switched core network.

One possibility in the providing of legacy services for mobile stations roaming from GSM/UMTS BSS to WLAN side is presented in publication "SIP-Enabled Gateway MSC: Linking WiFi Hot Spots with 2.5/3G Networks", Amir Atai, Ajay Sahai, Telica, March 31, 2004. The solution disclosed by Atai comprises the connecting of WLANs directly to a GMSC in the circuit switched core network, which acts also as a serving Visitor MSC (VMSC). The disadvantage of the solution disclosed by Atai is that a given subscriber is always served by a given GMSC. However, even in the case of dual system terminals, it must be possible for the operator to receive a terminating call for a given terminal in any GMSC. The treatment of terminating calls in the GMSC must be uniform across 2G/3G and WLAN terminals. The call must be routed to the correct serving VMSC using a roaming number obtained from an HLR irrespective of the type of the terminal. Further, it is beneficial to be able to configure the DNS so that a number of MSC servers are referred to using the same Fully Qualified Domain Name (FQDN), for example,

"sip.operator.com", wherein "operator" stands for the operator name and "sip" stands for a set of SIP registrars. When a dual system terminal registers to the circuit switched core network via a WLAN and provides the FQDN for the SIP service, it is possible for the DNS to return IP-addresses for different MSC servers acting as SIP registrars in a round-robin fashion. Thus, at different registration times a different IP address may be provided from the DNS to the dual system terminal. Additionally, some legacy services may require that calls pertaining to legacy services must be routed to/via a voice server or a centralized IN service switching point. Thus, it would be a benefit to be able to use legacy ISUP signaling between the circuit switched core network elements. When pure SIP signaling is used the users' ITU-T E.164 format subscriber numbers are not available.

Summary of the invention:

The invention relates to for routing calls in a communication system comprising at least a mobile station, a first call control node, a second call control node, a directory and a home location register. The method comprises: receiving a registration message from said mobile station to said first call control node, said registration message comprising a logical name referring to said mobile station; mapping said logical name to an International Mobile Subscriber Identity (IMSI) referring to said mobile station in said directory at the request of said first call control node; updating the location of said mobile station to said home location register at the request of said first call control node, said request comprising said International Mobile Subscriber Identity; receiving a call set-up request message in said second call control node, said call set-up request message comprising at least a called party number; sending an in-

quiry message from said second call control node to said home location register, said inquiry message comprising at least said called party number; allocating a roaming number from said first call control node at the request of said home location register; sending an inquiry response message from said home location register to said second call control node comprising at least said roaming number; sending a call set-up request message from said second call control node to said first call control node; and mapping said called party number to said logical name referring to said mobile station in said directory at the request of said first call control node.

The invention relates also to a system comprising at least a mobile station, a first call control node, a second call control node, a directory and a home location register. The system further comprises: a mobility entity in said first call control node configured to receive a registration message from said mobile station, said registration message comprising a logical name referring to said mobile station, to request the mapping of said logical name to an International Mobile Subscriber Identity (IMSI) referring to said mobile station from said directory, to request the updating of the location of said mobile station from said home location register by specifying said International Mobile Subscriber Identity (IMS); a call control entity in said second call control node configured to receive a call set-up request message, said call set-up request message comprising at least a called party number, to send an inquiry message from said second call control node to said home location register, said inquiry message comprising at least said called party number, to receive an inquiry response message from said home location register comprising at least a roaming number, to send a call set-up request message to said first call control node;

and a call control entity in said first call control node configured to request the mapping of said called party number to said logical name referring to said mobile station from said directory.

The invention relates also to a call control node comprising a mobility entity configured to receive a registration message from a mobile station, said registration message comprising a logical name referring to said mobile station, to request the mapping of said logical name to an International Mobile Subscriber Identity (IMSI) referring to said mobile station from a directory, to request the updating of the location of said mobile station from a home location register by specifying said International Mobile Subscriber Identity (IMSI) and a call control entity configured to receive a call set-up request message, said call set-up request message comprising at least a called party number, to send an inquiry message to said home location register, said inquiry message comprising at least said called party number, to receive an inquiry response message from said home location register comprising at least a roaming number, to send a call set-up request message to a second call control node, and to request the mapping of said called party number to said logical name referring to said mobile station from said directory.

The invention also relates to a computer program comprising code adapted to perform the following steps when executed on a data-processing system: receiving a registration message from a mobile station, said registration message comprising a logical name referring to said mobile station; requesting the mapping of said logical name to an International Mobile Subscriber Identity (IMSI) referring to said mobile station from a said directory; requesting the updating of the location of said mobile station from a home location register, said request comprising said Interna-

tional Mobile Subscriber Identity; receiving a call set-up request message, said call set-up request message comprising at least a called party number; sending an inquiry message to said home location register, said inquiry message comprising at least said called party number; receiving an inquiry response message from said home location register comprising at least a roaming number; sending a call set-up request message to another call control node; and requesting the mapping of said called party number to said logical name referring to said mobile station from said directory.

In one embodiment of the invention, a calling party number is obtained in the second call control. The calling party number is obtained, for example, for the call set-up request message received to the second call control node. The calling party number is provided to the first call control node in the call set-up message that is sent in response to receiving the roaming number from the home location register. When receiving the call set-up request message, the first call control node extracts the calling party number and determines whether the calling party number comprises a prefix, which indicates that the calling party number may be translated to a logical name. If the calling party number comprises such as prefix it is mapped to a second logical name referring to a calling party in the directory at the request of said first call control node. The directory returns the second logical name to the first call control node in response. The call set-up request messages and the calling party number analysis are performed in a call control entity in the call control node.

In one embodiment of the invention, the availability of a Wireless Local Area Network (WLAN) at the mobile station is determined in a communication entity of the mobile station. The communication entity establishes a connection from said mobile station to

an access router connected to the wireless local area network. The communication entity obtains the identity of said first call control node via said access router. The access router is, for example, a router that controls packet data service access to and from mobile stations in the area of the WLAN. The router may also perform authentication, authorization and accounting functions for mobile stations in the WLAN to which it is connected.

In one embodiment of the invention, the communication system comprises a Wireless Local Area Network (WLAN).

In one embodiment of the invention, the mobile communication system comprises at least one of a Global System of Mobile Communications (GSM) network and a Universal Mobile Telephone System (UMTS) network.

In one embodiment of the invention, the first and the second call control nodes are Mobile Service Switching center Servers (MSS). The MSSes may control at least one media gateway or media proxy, which handle user plane traffic. The user plane traffic may be received from the Public Switched Telephone Network (PSTN) or other call control nodes as a circuit switched connection, which is converted in a media gateway to a packet switched connection. In one embodiment of the invention, the first and the second call control nodes are Mobile Service Switching Centers (MSC).

In one embodiment of the invention, the mobile station comprises a Session Initiation Protocol (SIP) user agent. When in the area of a WLAN, the user agent performs location registration by sending Session Initiation Protocol (SIP) registration messages to the first call control node. The call control nodes may comprise a call control entity, which communicates with the user agent using Session Initiation Protocol

(SIP) signaling. The call control entity may communicate with other call control nodes using a circuit switched signaling such as ISDN User Part (ISUP). If a calling party and a called party belong to the same operator's network, the user plane traffic may not be converted to a circuit switched connection, but may be instead carried over packet data from the calling party mobile station to the called party mobile station. In that case, the user plane IP addresses associated with the calling and the called parties are carried in ISUP signaling messages.

In one embodiment of the invention, the call set-up request message is an ISDN User Part (ISUP) call set-up request message. In one embodiment of the invention, the call set-up request message is a Session Initiation Protocol (SIP) Invite message or generally any equivalent voice over IP call set-up request message.

In one embodiment of the invention, the directory is a Lightweight Directory Access Protocol (LDAP) directory. The directory is accessed using the LDAP protocol.

In one embodiment of the invention, the mobile station comprises a wireless local area network terminal. In one embodiment of the invention, the mobile station comprises a Subscriber Identity Module (SIM).

In one embodiment of the invention, the mobile station is a multi-radio terminal, which is supports both WLAN and licensed band radio connectivity. Licensed band radio connectivity comprises, for example, Global System of Mobile communications (GSM) radio connectivity and Universal Mobile Telecommunication System (UMTS) connectivity on the radio bands that have been allocated for operators providing 2G and 3G service.

In one embodiment of the invention, the call control entity within the call control node is a software component. In one embodiment of the invention, the mobility entity within the call control node is a software component. In one embodiment of the invention, the communication entity within the mobile station node is a software component. Each of these components may comprise at least one independently compiled or translated program module. The components may comprise a number of processes or threads executed in a processor or a virtual machine such as a Java virtual machine.

In one embodiment of the invention, the computer program is stored on a computer readable medium. The computer readable medium may be a removable memory card, magnetic disk, optical disk or magnetic tape.

In one embodiment of the invention, the term call refers also to a short message. In this embodiment the call set-up message is a short message delivery message and the call control entity is a short message delivery entity. In this case the roaming number is a routing number for delivering the short message to the first call control entity.

In one embodiment of the invention, the DNS is configured so that a number of MSC servers are referred to using the same Fully Qualified Domain Name (FQDN), for example, "sip.operator.com", wherein "operator" stands for the operator name and "sip" stands for a set of SIP registrars. When a dual system terminal registers to the circuit switched core network via a WLAN and provides the FQDN for the SIP service, the DNS may return IP-addresses for different MSC servers acting as SIP registrars in a round-robin fashion. Thus, at different registration times a different IP address may be provided from the DNS to the dual system terminal.

The benefits of the invention are related to the uniform handling of 2G/3G terminals and dual system terminals from the core network and supplementary service perspective. In the case of any dual system terminal supporting both WLAN and licensed band access, it is possible for the operator to receive a terminating call for the terminal in any GMSC. The subscriber numbering is not affected due to the fact that the terminal is a dual system terminal. The call may be routed to the correct serving VMSC using a roaming number obtained from an HLR irrespective of whether the current VMSC acts as a SIP registrar for a WLAN hot spot or whether the current VMSC is simply serving a 2G/3G area.

Further, it is possible to configure the DNS so that a number of MSC servers are referred to using the same Fully Qualified Domain Name (FQDN). When a dual system terminal registers to the circuit switched core network via a WLAN and provides the FQDN for the SIP service, the DNS may return IP-addresses for different MSC servers acting as SIP registrars in a round-robin fashion. Thus, at different registration times a different IP address may be provided from the DNS to the dual system terminal.

Further, by allowing the use of MSISDN numbers in a call set-up request messages received to a gateway MSS, it is possible to maintain the normal circuit switched core network roaming mechanisms comprising the use of HLRs, VLRs and roaming number allocation. It is not necessary to employ the different mechanisms for IP multimedia subsystem. This allows the use of legacy supplementary services from the circuit switched core network. From supplementary service point of view the treating of WLANs in a manner similar to licensed band radio service areas provides for easier service deployment and operation.

Additionally, some legacy services may require that calls pertaining to legacy services must be routed to/via a voice server or a centralized IN service switching point. Thus, it is a benefit to be able to use legacy ISUP signaling between the circuit switched core network elements.

BRIEF DESCRIPTION OF THE DRAWINGS:

The accompanying drawings, which are included to provide a further understanding of the invention and constitute a part of this specification, illustrate embodiments of the invention and together with the description help to explain the principles of the invention. In the drawings:

Fig. 1 is a block diagram illustrating the problems associated with the providing of legacy services for dual system terminals in prior art;

Fig. 2 is a block diagram illustrating a communication system according to the invention;

Fig. 3 is a message sequence chart illustrating location updating from a Session Initiation Protocol (SIP) User Agent (UA) to a Mobile Switching Center Server (MSS) in one embodiment of the invention;

Fig. 4 is a message sequence chart illustrating a mobile-to-mobile call between two User Agents (UA) that are Session Initiation Protocol (SIP) based in one embodiment of the invention;

Fig. 5 is a flow chart depicting one embodiment of a method for the routing of communications to a Session Initiation Protocol (SIP) User Agent in a communication system; and

Fig. 6 is a block diagram illustrating a Mobile Switching Center Server (MSS) in one embodiment of the invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS:

Reference will now be made in detail to the embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

Figure 2 is a block diagram illustrating a communication system according to the invention. The communication system comprises at least a Mobile Station (MS) 200, a serving MSS 220, a gateway MSS 222, a Home Location Register (HLR) 230, a Lightweight Directory Access Protocol (LDAP) directory 232, a Camel Service Entity (CSE) 216, a Base Station Controller (BSC) 210 and a first access network 218 connected to a Base Transceiver Station (BTS) 234. MS 200 is a SIP enabled user agent, which obtains SIP connectivity via MSS 220. MS 200 is a multi-radio terminal, which is supports both WLAN and licensed band radio connectivity. In one embodiment of the invention, MS 200 comprises a communication entity (not shown), which performs all communication related functions. A WLAN Base Transceiver Station (BTS) 202 provides WLAN radio connectivity, whereas a BTS 246 supports licensed band radio connectivity. Licensed band radio connectivity may be, for example, based on WCDMA radio access or TDMA radio access. Serving MSS 220 comprises a Visitor Location Register (VLR) 214, which stores subscriber data for subscribers currently registered in serving MSS 220. Gateway MSS 222 has a signaling connection to a Public Switched Telephone Network (PSTN) 240 and to serving MSS 220. Gateway MSS 222 controls a first MGW 242 and MSS 220 controls a second MGW 244. First MGW 242 is connected to PSTN 240 and provides user plane conversion to/from circuit switched E1/T1 to IP packets. Second MGW 244 is connected to PSTN 240 and provides user plane conversion to/from circuit switched BSC 210 to IP packets. UMA controller 208 may also provide a circuit switched connection to second MGW 244. Packets are routed between first MGW 242 and sec-

ond MGW 244 based on requests from MSS 222 and MSS 220, respectively. BSC 210 is connected to MSS 220 using protocol interface 250. Protocol interface 250 is, for example, GSM A/Gb-interface or UMTS Iu-interface. BSC 210 may thus also be a UMTS Radio Network controller.

In Figure 2 there is also a second access network 206, the signaling plane of which is connected to MSS 220 via an Unlicensed Mobile Access (UMA) controller 208. Second access network 206 is an IP based Access Network. UMA controller 208 interfaces into MSS 220 by looking like a standard RAN. In other words, UMA controller 208 emulates BSC 210 for MSS 220. To second access network 206 is also connected via a Session Border Controller (SBC) 203 a Customer Premise Equipment (CPE), which is, for example, an access router. WLAN Base Transceiver Station (BTS) 202 is connected to CPE 204. There may be a number of WLAN BTSes, which are connected via CPE 204 to second access network 206. SBC 203 acts as a SIP proxy and hides the address space within the operator's network, which comprises at least the second access network 206 from MS 200. User plane traffic to/from MS 200 goes via SBC 203 to first MGW 242 when there is a call between MS 200 and a subscriber connected to PSTN 240. SBC 203 may also perform standard firewall related tasks such as packet filtering. LDAP directory 232 is used to perform translation of SIP URIs to ITU-T E.164 addresses and vice versa. For example, LDAP directory translates calling party SIP URIs to calling party IMSIs on the requests of serving MSSes and provides the IMSIs in respective response messages. As MS 200 performs registration, in other words, an initial location updating procedure, in MSS 220 the LDAP directory provides the subscriber information to MSS 220, which is not normally available via SIP signaling from MS 200 to MSS 220, but which is available via GSM A-

interface signaling or UMTS Iu-interface signaling either at location updating or at call set-up request. Such information includes, for example, an IMSI corresponding to MS 200 SIP URI. The information is provided from LDAP directory 232 to MSS 220 at the request of MSS 220.

In one embodiment of the invention, the operator's network uses a single LDAP directory, for example, LDAP directory 232. As a subscriber registers via any MSS equipped with a SIP-interface, the same LDAP directory may be accessed. Thus, the LDAP directory is the same irrespective of the enquiring MSS. In one embodiment of the invention, there is more than one LDAP directory.

Figure 3 is a message sequence chart illustrating location updating from a Session Initiation Protocol (SIP) User Agent (UA) to a Mobile Switching Center Server (MSS) in one embodiment of the invention. At time t_1 MS 200 determines that WLAN access via WLAN BTS 202 is available and determines that communication to and from MS 200 should be routed via WLAN radio access. MS 200, in other words, a SIP user agent sends a DNS enquiry message to a DNS server 314 as illustrated with arrow 301. The DNS enquiry message specifies a SIP server Fully Qualified Domain Name (FQDN), which is resolved by DNS server 314 into at least one IP address. In Figure 3 there is provided a single IP address that refers to MSS 220. DNS server 314 responds with an enquiry response message, which provides the IP address to MS 200 as illustrated with arrow 302. Thereupon, MS 200 sends a SIP Register message to MSS 220 as illustrated with arrow 303. The SIP Register message carries at least the SIP URI of MS 200 and the user agent IP address to be used by MSS 220 to send user plane and signaling plane packets to MS 200. The SIP Register message may traverse an SBC (not shown), which alters the user agent IP address.

As MSS 220 receives the SIP Register message, it sends an LDAP search message to LDAP directory 232 as illustrated with arrow 304. The LDAP search message comprises at least the SIP URI referring to MS 200. In response to LDAP search message LDAP directory 232 obtains the subscriber data associated with the SIP URI. LDAP directory 232 sends an LDAP search response message to MSS 220 as illustrated with arrow 305. The LDAP search response message comprises at least the IMSI associated with MS 200. Other parameters comprised in the LDAP search response message may comprise a calling party E.164 address associated with MS 200 (MSISDN-A), a user name and authentication related parameters such as a nonce and an expected authentication response from MS 200. When receiving the LDAP search response message MSS 220 sends a SIP 401 response message to MS 200 as illustrated with arrow 306. The SIP 401 response message comprises a WWW-authenticate/digest header, which in turn comprises the realm associated with SIP service in the operator's network, the operator's domain, the nonce received from LDAP directory 232 and an algorithm to be used in authentication, which is normally Message Digest 5 (MD5). In response to receiving the SIP 401 response message, MS 200 provides a SIP Registration message to MSS 220 as illustrated with arrow 307. The SIP Registration message comprises an authorization/digest header, which comprises the user name associated with MS 200, the realm associated with SIP service in the operator's network, the operator's domain, the nonce, an URI associated with MSS 220 and a response generated by MS 200 based on parameters received in SIP 401 response message. Upon receiving the SIP Registration message comprising the authorization/digest header, MSS 220 compares the response generated by MS 200 to the expected response received from LDAP directory 232.

In response to successful authentication MSS 220 starts performing location update with HLR 230. MSS 220 updates the location of MS 200 to the VLR 214 associated with it. However, in the case of Figure 3 the VLR 214 is considered as part of MSS 220 and is not shown separately. In one embodiment of the invention, MSS 220 obtains all the MS 200 parameters necessary for location updating that are not provided in SIP Register message from LDAP directory 232. After the successful authentication, MS 200 sends a location update request message to HLR 230 as illustrated with arrow 308. The location update request message comprises at least the IMSI associated with MS 200. In response to the receiving of the location update request message HLR 230 sends at least one insert subscriber data message to MSS 220 as illustrated with arrow 309. The insert subscriber data message provides subscriber data associated with MS 200. The subscriber data is updated to the VLR 214 associated with MSS 220. MSS 220 acknowledges insert subscriber data message as illustrated with arrow 310. When all insert subscriber data messages have been acknowledged by MSS 220, HLR 230 sends a location update response message to MSS 220 as illustrated with arrow 311. Thereupon, MSS 220 sends a SIP 200 OK message to MS 200 as illustrated with arrow 312.

Figure 4 is a message sequence chart illustrating a mobile-to-mobile call between two User Agents (UA) that are Session Initiation Protocol (SIP) based in one embodiment of the invention. The user agents are the calling party mobile station, namely MS 200 and the called party mobile station, namely MS 452. The calling party is referred to as the A-party and the called party as the B-party, hence the designation of letters A and B to respective network elements and addresses associated with the respective parties. MS 200 is handled by MSS 220, which is thus

also referred to as the MSS of the calling party (MSS-A). MS 452 is handled by MSS 450, which is thus also referred to as the MSS of the called party (MSS-B). Initially, at time t_1 the user of MS 200 decides to place an outgoing call to MS 452. The calling user specifies the called party by selecting or entering SIP-URI-B, which is a SIP URI according to RFC 3261. MS 200 sends a SIP Invite message to MSS 220 in which MS 200 is currently registered as illustrated with arrow 401. Upon receiving the SIP Invite message MSS 220 sends an LDAP search request message to LDAP directory 232 as illustrated with arrow 402. The LDAP search request message comprises at least the called party SIP-URI-B. When the SIP-URI-B is obtained by LDAP directory 232, it is translated to an E.164 address, namely MSISDN-B. LDAP directory 232 sends an LDAP search response message to MSS 220, which comprises at least the MSISDN-B, as illustrated with arrow 403.

Upon receiving the LDAP search response message and the MSISDN-B MSS 220 is now capable of routing a call to MS 452 using the routing means of MSC servers without employing IMS routing means. The routing means of MSC servers are similar to the routing means of circuit switched calls in GSM/UMTS core networks. Similarly, it is possible for MSS 220 to use the service functionalities catering for the supplementary services of circuit switched calls. Further, it is possible for MSS 220 to use billing functionalities catering for circuit switched calls. It should also be noted that since the calling party E.164 number MSISDN-A is available from the LDAP directory enquiry performed during location updating, it is possible to use also MSISDN-A in the providing of supplementary services. For example, both MSISDN-A and MSISDN-B may be used instead of SIP names to refer to the calling and the called party if an enquiry is sent to CSE 216 in order to initiate Camel supplementary

services. The Camel supplementary service only needs to inspect E.164 addresses instead of SIP URIs.

MSS 220 sends a Send Routing Instructions (SRI) message to HLR 230 comprising MSISDN-B, as illustrated with arrow 404. Upon receiving the Send Routing Instructions message HLR 230 obtains the subscriber data associated with the called subscriber. HLR 230 knows the MSC server and VLR, in which the called subscriber is registered, namely MSS 450. The HLR in turn enquires MSS 450 and the VLR therein by sending a Provide Roaming Number (PRN) message as illustrated with arrow 405. The roaming number is also known as Mobile Station Roaming Number (MSRN). The VLR then provides the HLR 230 with a roaming number using message illustrated with arrow 406. The roaming number is then used to route the call towards MSS 450. The HLR packs the data associated with the called subscriber and the roaming number in its response message 407 to MSS 220, which will act as a Gateway MSC in accordance with the GSM/UMTS circuit switched core network. The MSS 220 then routes the call in a direction towards MSS 450 using the roaming number. The MSS 220 sends an ISUP Initial Address Message (IAM) forward towards MSS 450 and starts waiting for the ACM message from the direction of MSS 450, as illustrated with arrow 408. The ISUP IAM message comprises, for example, the calling party E.164 address, namely MSISDN-A, and the called party E.164 address, namely MSISDN-B. Upon receiving IAM message 408 from MSS 220, MSS 450 sends an LDAP search request message to LDAP directory 232 as illustrated with arrow 409. The LDAP search request message comprises, for example, the MSISDN-A and MSISDN-B parameters from ISUP IAM message. In response to the LDAP search request message, LDAP directory 232 maps the MSISDN-A and MSISDN-B to SIP-URI-A and SIP-URI-B. LDAP directory 232 sends an LDAP search request response message comprising SIP-URI-A and SIP-URI-B as

illustrated with arrow 410. After having received the SIP URIs from the LDAP search response message, MSS 450 sends a SIP Invite message to MS 452 as illustrated with arrow 411. The SIP Invite message comprises at least the SIP-URI-A and SIP-URI-B parameters and the IP address used to send user plane and signaling plane packets to MS 452. The IP address has been provided to MSS 450 during location update signaling. The IP address is either directly associated with MS 452 or it refers to an SBC via which SIP signaling messages are sent to MS 452. MSS 450 sends an ISUP Address Complete Message (ACM) to MSS 220 as illustrated with arrow 412. Thereupon, MSS 220 sends a SIP trying message to MS 200 as illustrated with arrow 413.

In one embodiment of the invention, SIP signaling is used between MSS 220 and MSS 450. In this case, for example, the call set-up message is a SIP Invite message. Even though SIP signaling is used between MSS 220 and MSS 450, it is still possible to use MSISDN and roaming number for the routing of calls to MS 200. This allows the maintaining of legacy supplementary services and billing mechanisms that employ E.164 numbers instead of SIP names.

In one embodiment of the invention, the user plane and the signaling plane packets associated with a given MS have different IP addresses. In one embodiment of the invention, the IP addresses refer to Packet Data Protocol Contexts (PDP) within a General Packet Radio System (GPRS) Gateway GPRS Support Node (GGSN).

Figure 5 is a flow chart depicting one embodiment of a method for the routing of communications to a Session Initiation Protocol (SIP) User Agent in a communication system.

At step 502 a first MSS waits for a location update message from an MS. If no message is received, the method continues at step 502.

At step 504 the first MSS maps the SIP URI received in the location update message from the MS to an IMSI associated with the MS.

At step 506 the first MSS sends a location updating request to an HLR. In the location update request message the IMSI associated with the MS is specified.

At step 508 a second MSS receives a call set-up request addressed to the MS. The call request provides at least an MSISDN associated with the MS.

In one embodiment of the invention the call set-up request provides only a SIP URI associated with the MS. The second MSS maps the SIP URI to the MSISDN associated with the MS.

At step 510 the second MSS enquires the HLR using the MSISDN associated with the MS and reserves a roaming number from the first MSS in order to route the call to the MS. The roaming number may be reserved from a visitor location register in association with the first MSS.

At step 512 the second MSS routes the call set-up request to the first MSS using the roaming number.

At step 514 the first MSS receives the call set-up request. In one embodiment of the invention, the first MSS maps the MSISDN associated with the MS to the SIP URI associated with the MS.

At step 516 the first MSS checks if the calling party number in the call set-up request may be mapped to a SIP URI associated with the calling party. The check may be performed, for example, by analyzing the calling party number and determining whether the number comprises a prefix, which indicates that the calling party number may be mapped to a SIP URI.

Figure 6 is a block diagram illustrating a Mobile Switching Center Server (MSS) in one embodiment of the invention. In Figure 6 there is a Mobile

Switching Center Server (MSS) 600. MSS 600 comprises a Call Control (CC) entity 602 and a mobility management entity 610. The call control entity communicates with a Session Initiation Protocol (SIP) entity 604, which in turn communicates, for example, with a mobile station such as mobile station 200 in Figure 2. The call control entity 602 communicates also with a Mobile Application Part (MAP) entity, which is used to access the home location register. Call control entity 602 may also communicate with an ISUP entity in order to establish, maintain and release calls. Mobility management entity 610 communicates with the home location register via mobile application part entity 606. Mobility management entity 610 is used in the updating of mobile station location in the home location register. Registration requests are received to the mobility management entity 610 from mobile stations via the session initiation protocol entity 604. Mobility management entity 610 and call control entity 602 communicate with a directory using a Lightweight Directory Access Protocol (LDAP) entity 612. In one embodiment of the invention, the mobility management entity 610 comprises also a visitor location register.

It is obvious to a person skilled in the art that with the advancement of technology, the basic idea of the invention may be implemented in various ways. The invention and its embodiments are thus not limited to the examples described above; instead they may vary within the scope of the claims.

CLAIMS:

1. A method for routing calls in a communication system comprising at least a mobile station, a first call control node, a second call control node, a directory and a home location register, the method comprising:

receiving a registration message from a mobile station to a first call control node, said registration message comprising a logical name referring to said mobile station;

mapping said logical name to an International Mobile Subscriber Identity referring to said mobile station in a directory at the request of said first call control node;

updating a location of said mobile station to a home location register at a request of said first call control node, said request of said first call control node comprising said International Mobile Subscriber Identity;

receiving a call set-up request message in a second call control node, said call set-up request message comprising at least a called party number;

sending an inquiry message from said second call control node to said home location register, said inquiry message comprising at least said called party number;

allocating a roaming number from said first call control node at a request of said home location register;

sending an inquiry response message from said home location register to said second call control node comprising at least said roaming number;

sending the call set-up request message from said second call control node to said first call control node; and

mapping said called party number to said logical name referring to said mobile station in said direc-

tory at a second request of said first call control node.

2. The method according to claim 1, the method further comprising:

obtaining a calling party number in said second call control node;

determining in said first call control node whether said calling party number comprises a prefix indicating that said calling party number may be translated to a second logical name; and

mapping said calling party number to the second logical name referring to a calling party in said directory at a third request of said first call control node.

3. The method according to claim 1, the method further comprising:

determining an availability of a Wireless Local Area Network at said mobile station;

establishing a connection from said mobile station to an access router connected to said wireless local area network; and

obtaining an identity of said first call control node via said access router.

4. The method according to claim 1, wherein said communication system comprises a Wireless Local Area Network.

5. The method according to claim 1, wherein said mobile communication system comprises at least one of a Global System of Mobile Communications network and a Universal Mobile Telephone System network.

6. The method according to claim 5, wherein said first and said second call control nodes are Mobile Service Switching center Servers.

7. The method according to claim 1, wherein said mobile station comprises a Session Initiation Protocol user agent.

8. The method according to claim 7, wherein said registration message is a Session Initiation Protocol registration message.

9. The method according to claim 1, wherein said call set-up request message is an ISDN User Part call set-up request message.

10. The method according to claim 1, wherein said directory is a Lightweight Directory Access Protocol directory.

11. A system comprising at least a mobile station, a first call control node, a second call control node, a directory and a home location register, the system further comprising:

a mobility entity in said first call control node configured to receive a registration message from said mobile station, said registration message comprising a logical name referring to said mobile station, to request a mapping of said logical name to an International Mobile Subscriber Identity referring to said mobile station from said directory, and to request updating of a location of said mobile station from said home location register by specifying said International Mobile Subscriber Identity;

a call control entity in said second call control node configured to receive a call set-up request message, said call set-up request message comprising at least a called party number, to send an inquiry message from said second call control node to said home location register, said inquiry message comprising at least said called party number, to receive an inquiry response message from said home location register comprising at least a roaming number, and to send a call set-up request message to said first call control node; and

a call control entity in said first call control node configured to request a mapping of said called

party number to said logical name referring to said mobile station from said directory.

12. The system according to claim 11, wherein the call control entity in said first call control node is configured to determine whether a calling party number comprises a prefix indicating that said calling party number may be translated to a second logical name, and to request the mapping of said calling party number to the second logical name referring to a calling party from said directory.

13. The system according to claim 11, the system further comprising:

a communication entity in said mobile station configured to determine the availability of a Wireless Local Area Network, to establish a connection from said mobile station to an access router connected to said wireless local area network, and to obtain an identity of said first call control node via said access router.

14. The system according to claim 11, wherein said system comprises a Wireless Local Area Network.

15. The system according to claim 11, wherein said system comprises at least one of a Global System of Mobile Communications network and a Universal Mobile Telephone System network.

16. The system according to claim 15, wherein said first call control node and said second call control node are Mobile Service Switching center Servers.

17. The system according to claim 11, wherein said mobile station comprises a Session Initiation Protocol user agent.

18. The system according to claim 17, wherein said registration message is a Session Initiation Protocol registration message.

19. The system according to claim 11, wherein said call set-up request message is an ISDN User Part call set-up request message.

20. The system according to claim 11, wherein said directory is a Lightweight Directory Access Protocol directory.

21. A call control node comprising:

a mobility entity configured to receive a registration message from a mobile station, said registration message comprising a logical name referring to said mobile station, to request a mapping of said logical name to an International Mobile Subscriber Identity referring to said mobile station from a directory, and to request updating of a location of said mobile station from a home location register by specifying said International Mobile Subscriber Identity; and

a call control entity configured to receive a call set-up request message, said call set-up request message comprising at least a called party number, to send an inquiry message to said home location register, said inquiry message comprising at least said called party number, to receive an inquiry response message from said home location register comprising at least a roaming number, to send a call set-up request message to a second call control node, and to request a mapping of said called party number to said logical name referring to said mobile station from said directory.

22. A computer program embodied within a computer readable medium, the computer program being configured to perform the steps of:

receiving a registration message from a mobile station, said registration message comprising a logical name referring to said mobile station;

requesting a mapping of said logical name to an International Mobile Subscriber Identity referring to said mobile station from a directory;

requesting an update of a location of said mobile station from a home location register, said request

comprising said International Mobile Subscriber Identity;

receiving a call set-up request message, said call set-up request message comprising at least a called party number;

sending an inquiry message to said home location register, said inquiry message comprising at least said called party number;

receiving an inquiry response message from said home location register comprising at least a roaming number;

sending a call set-up request message to another call control node; and

requesting a mapping of said called party number to said logical name referring to said mobile station from said directory.

23. The computer program according to claim 22, wherein said computer readable medium is a removable memory card.

24. The computer program according to claim 22, wherein said computer readable medium is a magnetic or an optical disk.

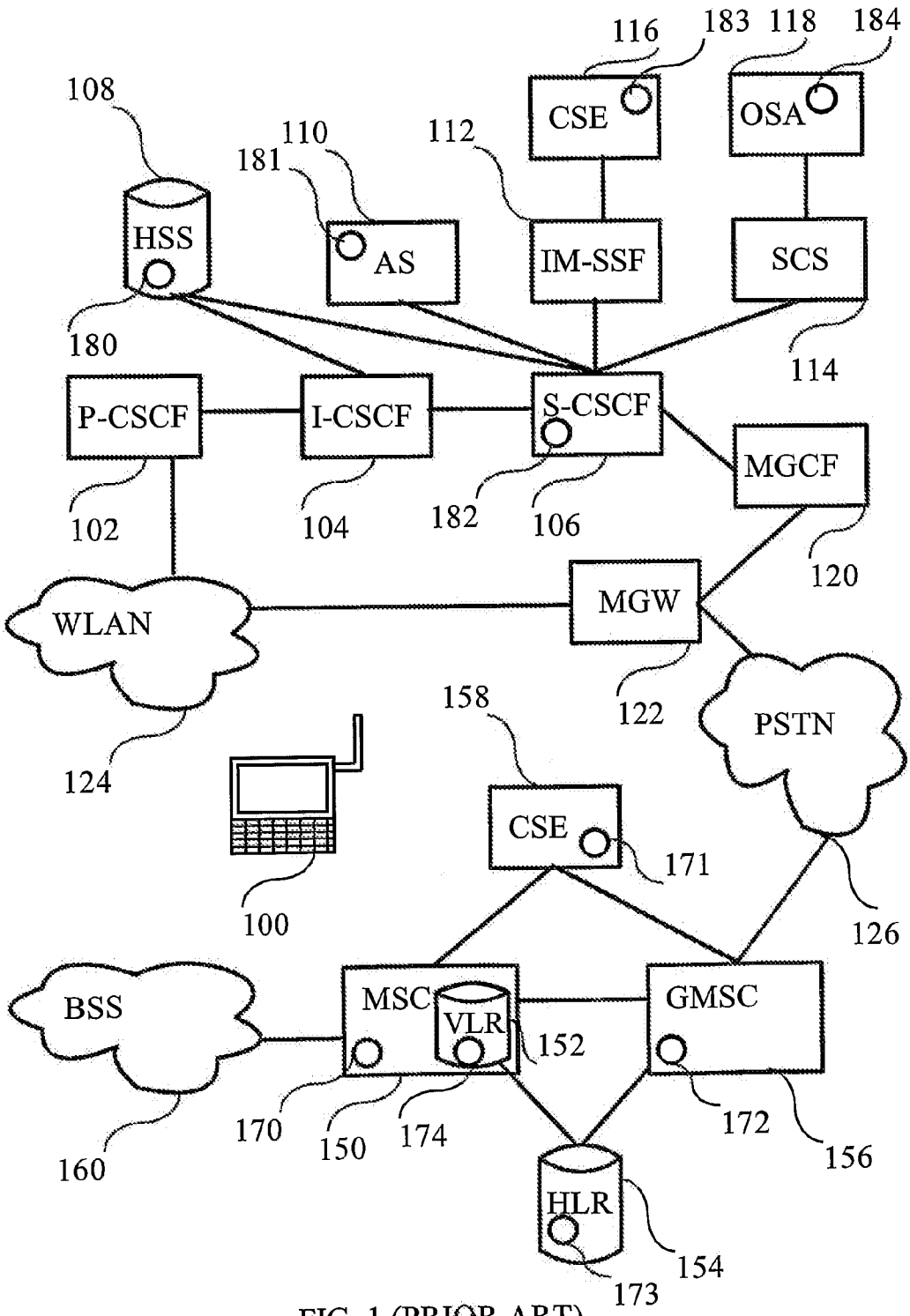


FIG. 1 (PRIOR ART)

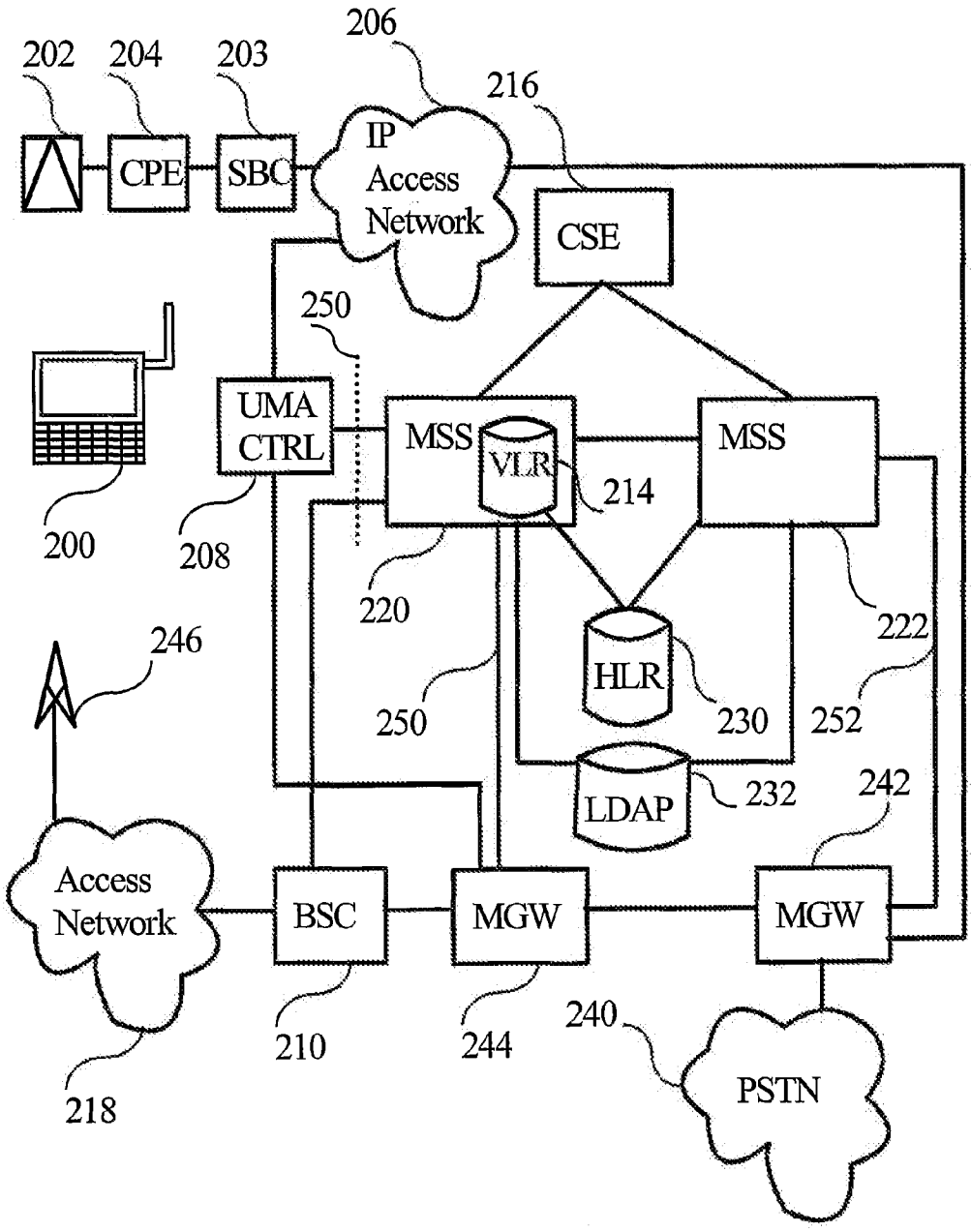

202
204
203
206
216
CPE
SBC
IP
Access
Network
CSE
250
UMA
CTRL
MSS
VLR
214
MSS
200
208
220
222
246
HLR
250
230
252
LDAP
232
242
Access
Network
BSC
MGW
MGW
210
244
240
PSTN
218

FIG. 2

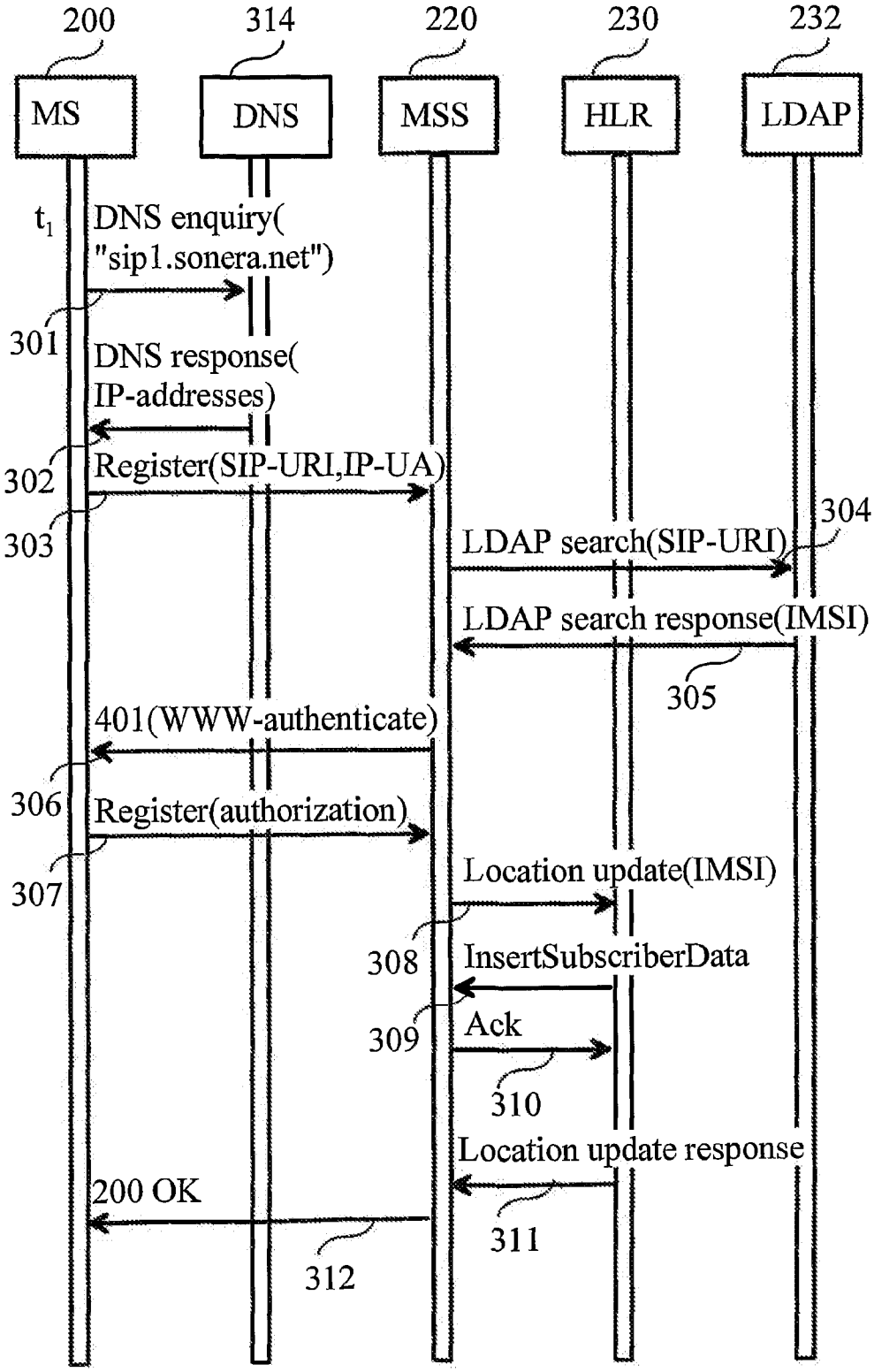

200
314
220
230
232
MS
DNS
MSS
HLR
LDAP
t1
DNS enquiry("sip1.sonera.net")
301
DNS response(IP-addresses)
302
Register(SIP-URI,IP-UA)
303
304
LDAP search(SIP-URI)
LDAP search response(IMSI)
305
401(WWW-authenticate)
306
Register(authorization)
307
Location update(IMSI)
308
InsertSubscriberData
309
Ack
310
Location update response
311
200 OK
312

FIG. 3

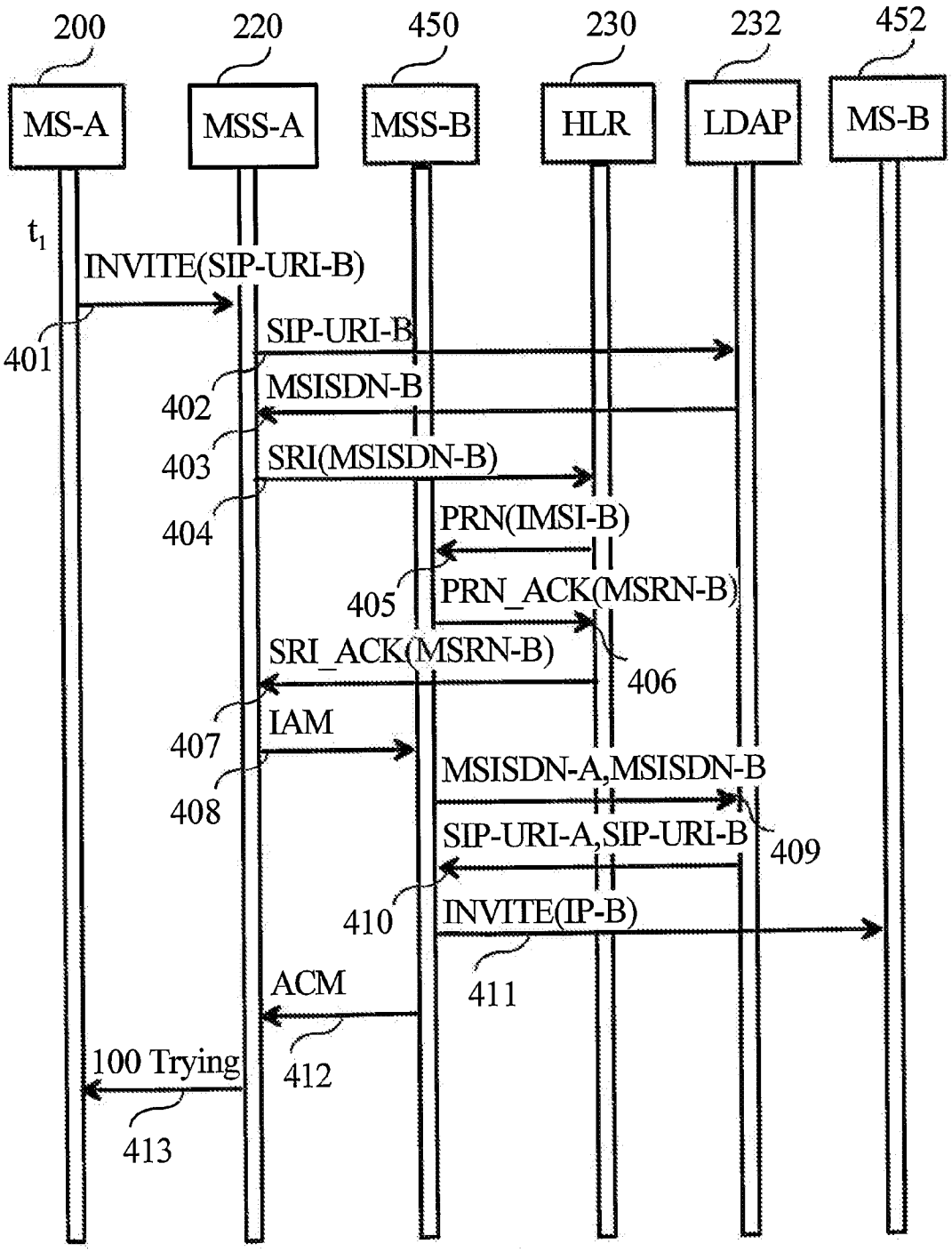

200
220
450
230
232
452
MS-A
MSS-A
MSS-B
HLR
LDAP
MS-B
t1
INVITE(SIP-URI-B)
401
SIP-URI-B
402
MSISDN-B
403
SRI(MSISDN-B)
404
PRN(IMSI-B)
405
PRN_ACK(MSRN-B)
406
SRI_ACK(MSRN-B)
407
IAM
408
MSISDN-A,MSISDN-B
409
SIP-URI-A,SIP-URI-B
410
INVITE(IP-B)
411
ACM
412
100 Trying
413

FIG. 4

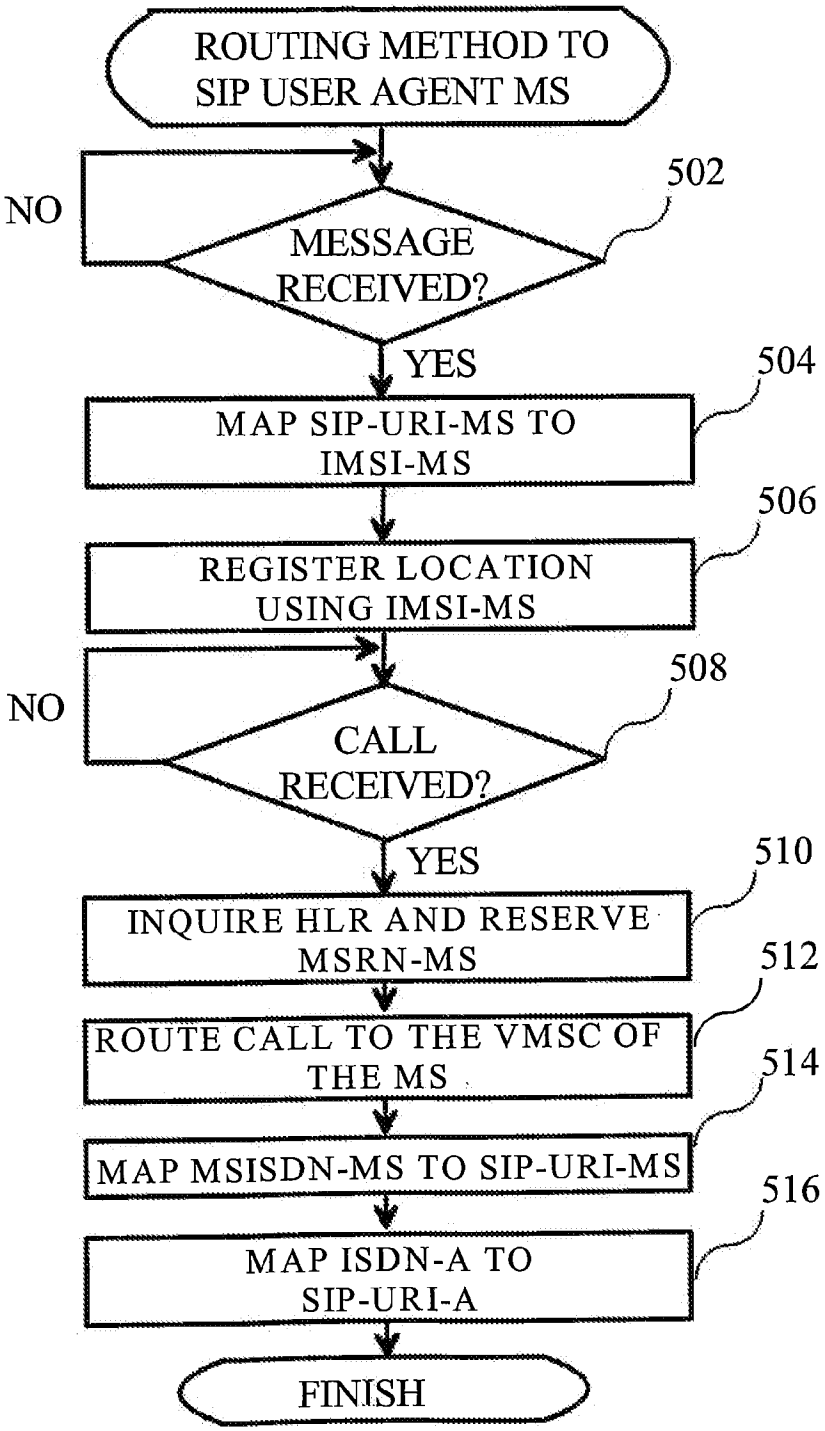

ROUTING METHOD TO SIP USER AGENT MS
NO
MESSAGE RECEIVED?
502
YES
MAP SIP-URI-MS TO IMSI-MS
504
REGISTER LOCATION USING IMSI-MS
506
NO
CALL RECEIVED?
508
YES
INQUIRE HLR AND RESERVE MSRN-MS
510
ROUTE CALL TO THE VMSC OF THE MS
512
MAP MSISDN-MS TO SIP-URI-MS
514
MAP ISDN-A TO SIP-URI-A
516
FINISH

FIG. 5

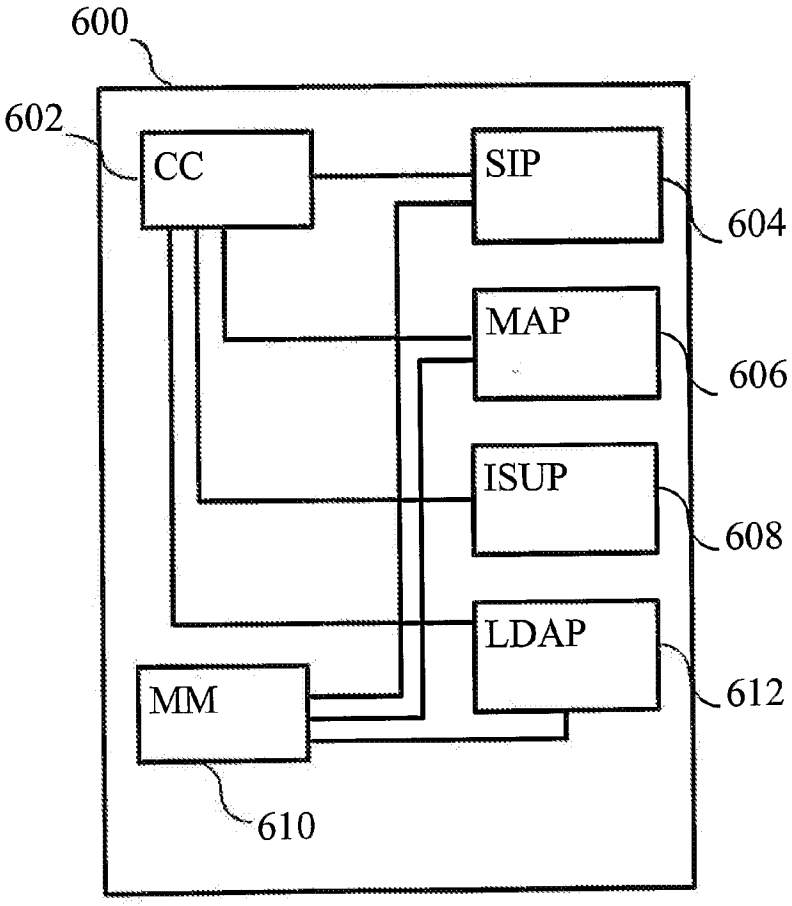


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2005/000540

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004017564 A1 (TOGEWA HOLDING AG), 26 February 2004 (26.02.2004), claims 1-3, abstract --	1-24
A	WO 0122766 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 29 March 2001 (29.03.2001), claim 1, abstract --	1-24
A	US 20020119775 A1 (MUKHERJEE, A), 29 August 2002 (29.08.2002), claims 1,6,7, abstract --	1-24

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 May 2006	19 -05- 2006
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Lisbeth Andersson /LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2005)

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0079814 A1 (NOKIA NETWORKS OY), 28 December 2000 (28.12.2000), page 5, line 19 - page 8, line 3, abstract -- --------	1-24

International patent classification (IPC)
H04L 12/56 (2006.01)
H04L 12/28 (2006.01)
H04Q 7/38 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument(service in Swedish).

Use the application number as username.
The password is **RWNXKSOQFK.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

WO	2004017564	A1	26/02/2004	AU	2002313435	A	03/03/2004
				AU	2002328760	A	03/03/2004
				BR	0215840	A	21/06/2005
				BR	0215841	A	21/06/2005
				CA	2495343	A	26/02/2004
				CA	2495539	A	26/02/2004
				CH	694677	A	31/05/2005
				CN	1650577	A	03/08/2005
				EP	1529374	A	11/05/2005
				EP	1529375	A	11/05/2005
				JP	2005539418	T	22/12/2005
				JP	2005539419	T	22/12/2005
				NO	20051348	A	15/03/2005
				NO	20051368	D	00/00/0000
				RU	2005104241	A	10/08/2005
				US	20050177733	A	11/08/2005
				US	20060004643	A	05/01/2006
				WO	2004017565	A	26/02/2004
WO	0122766	A1	29/03/2001	AU	7565000	A	24/04/2001
				CA	2385478	A	29/03/2001
				EP	1214858	A	19/06/2002
US	20020119775	A1	29/08/2002	US	6944451	B	13/09/2005
WO	0079814	A1	28/12/2000	AU	5022500	A	09/01/2001

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2006 (06.07.2006)

PCT

(10) International Publication Number
WO 2006/072099 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2005/047679

(22) International Filing Date:
29 December 2005 (29.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/027,915 30 December 2004 (30.12.2004) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LEBIZAY, Gerald** [BE/US]; 11-B Prospect Street, Madison, NJ 07940 (US).

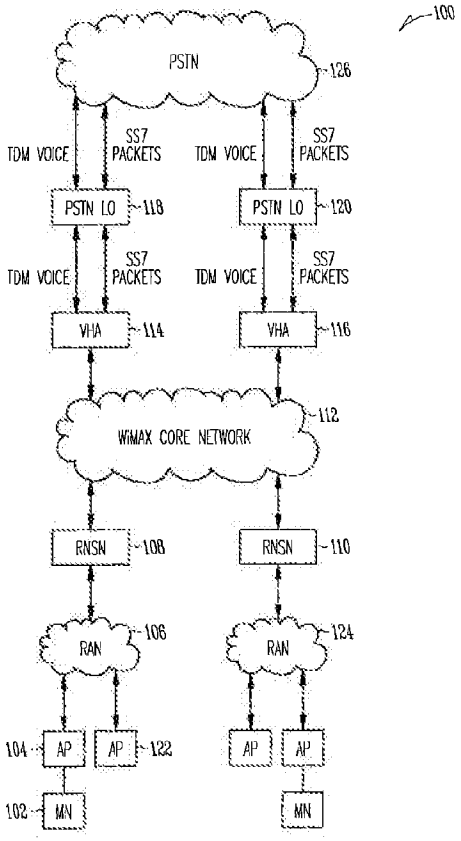
(74) Agents: **STEFFEY, Charles, E.** et al.; Schwegman, Lundberg, Woessner & Kluth, P.A., P.O. Box 2938, Minneapolis, MN 55402 (US).

(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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, NL, PL, PT,

[Continued on next page]

(54) Title: DISTRIBUTED VOICE NETWORK



(57) Abstract: A method and apparatus (114, 116) that receives an IP packet and encapsulates the packet with an IP header. Further, time-domain multiplexed voice data is received and converted into VoIP packets. Still further, Signaling System (7) (SS7) compliant signals are decoded. The decoded (SS7) signals are received and encapsulated prior to transmission to a telephony device (102).

WO 2006/072099 A1

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

DISTRIBUTED VOICE NETWORK

Technical Field

Embodiments of the invention relate to voice-over-IP technology implemented on a mobile wireless broadband network.

Background

Voice-over-IP (VoIP) technology permits parties to communicate orally over a packet-switched IP network. VoIP technology has grown in popularity, and depending upon certain factors, can offer sound quality that is comparable to that of the public switched telephone network (PSTN).

Also growing in popularity are wireless mobile networks. Wireless mobile networks permit a device to link to a network without requiring a physical conductive line to carry data between the device and the network. Further, such networks permit mobility by allowing a device to change access points in a manner transparent to network elements or nodes outside of the wireless mobile network domain.

Despite the growing popularity of VoIP technology and wireless mobile networks, there are no mobile client devices for present VoIP services over the Internet. One factor that hinders the advancement such mobile devices relates to finding a simple scheme by which a mobile device may be permitted to roam a significant geographic area (and therefore potentially wander between domains), while appearing keep a single IP address. The user datagram protocol (UDP) indexes connections by use of a quadruplet that contains the IP addresses and port number of both connection endpoints. Changing any one of these four numbers causes the connection to be disrupted and lost. Therefore, it is important that the device appear to keep the same IP address while roaming geographically. The difficulty in addressing this issue grows as the geographic area through which a device is permitted to roam grows.

From the foregoing, it is evident that there exists a need for a scheme by which a wireless IP telephony device can be permitted to roam a geographically significant area, such as a metropolitan area. It is desirable that such a scheme be relatively simple to implement as an overlay to an existing wireless network. It is further desirable that such a scheme be easily interconnected to the PSTN.

Brief Description of the Drawings

Figure 1 depicts a network environment in which an embodiment of a voice home agent is deployed.

Figure 2 depicts a protocol stack making up a voice home agent, according to an embodiment of the invention.

Figure 3 depicts a tunneling scheme employed by the mobile IP layer of the protocol stack depicted in Figure 2.

Figure 4 depicts a method of initiating a VoIP phone call, according to an embodiment of the invention.

Figure 5 depicts a method of executing a VoIP phone call, according to an embodiment of the invention.

Figure 6 depicts a hardware environment in which a voice home agent may be embodied, according to an embodiment of the invention.

Detailed Description

Figure 1 depicts a network environment 100 in which one or more mobile nodes 102 may be permitted to roam over a geographically significant area, such as across a metropolitan area. The mobile nodes 102 communicate via digital transmission (typically in the 2-to-6 GHz licensed bands, with typical channel bandwidths ranging from 1.5 to 20 MHz) to an access point 104. An access point (also referred to herein as a base station), such as the one identified by reference numeral 104, receives transmissions from the mobile node, and communicates the transmissions to network elements within an associated regional access network 106. According to an embodiment, the regional access network 106 is a wired network (i.e., a physical line interconnects the various elements making up the regional access network) that is a generic packet based access network, such as an Ethernet network, an IP/MPLS network, or an ATM network. The transmission between the access points 104 and the mobile nodes 102 is compliant with Institute of Electrical and Electronics Engineers (IEEE) 802.16 standard signals, IEEE std. 802.16-2001, published 2001 and later versions (hereinafter IEEE 802.16 standard or IEEE 802.16e standard). A regional access network 106 interconnecting access points (such as 104) compliant with IEEE 802.16e standards is referred to as a WiMAX network.

At the periphery of the WiMAX regional access network 106 is a radio network services node 108. The radio network services node 108 provides routing and control between other WiMAX regional area networks, such as the WiMAX network identified by reference numeral 124. Each regional access network 106 and 124 includes a radio network services node (108, 110) that couples the regional access network 106 or 124 to a WiMAX core network 112, which interconnects all of the regional access networks 106 and 124. Although the WiMAX core network 112 is depicted in Figure 1 as interconnecting two WiMAX networks 106 and 124, the WiMAX core network 112 may, in principle, interconnect any number of regional access networks.

The WiMAX core network 112 may be an ordinary IP network, composed of commonplace IP network elements, such as optical networking elements permitting high speed data transfer. As such, the WiMAX core network 112 may interconnect directly with the Internet (not depicted in Figure 1).

At the periphery of the WiMAX core network 112 are one or more voice home agents 114 and 116. There exists a voice home agent 114 or 116 associated with each WiMAX regional access network 106 and 124. The structure of, and methods enacted by, a voice home agent 114 or 116 are discussed in detail below. Briefly, a voice home agent is a network element that permits VoIP integration between a WiMAX core network (such as core network 112) and the public switched telephone network (PSTN) 126. Additionally, a voice home agent provides functionality that permits a mobile node (such as mobile node 102) to roam from one WiMAX regional access network (such as network 106) to another (such as 124).

Although Figure 1 depicts a single voice home agent 114 or 116 associated with each regional access network 106 or 124, more than one voice home agent may be associated with a given regional access network. Thus, although reference numerals 114 and 116 are presented herein as referring to a single voice home agent, each reference numeral 114 and 116 may be understood as referring to a group of voice home agents servicing their respective WiMAX regional access networks 106 and 124.

Each voice home agent 114 and 116 interfaces the WiMAX core network 112 to a local office 118 or 120 of the public switched telephone network 126. The public switched telephone network 126 uses an out-of-band signaling scheme known as Signaling System 7 (SS7), defined by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). An out-of-band signaling scheme

employs a different physical path for call control than is used to carry the content of the call itself (e.g., the voice data). Therefore, as shown in Figure 1, a voice home agent serves as two separate interfaces: an interface for voice data, which is delivered as time domain multiplexed digital voice data, and an interface for SS7 control signals, which are delivered as SS7 packets.

A mobile node, such as the one identified by reference numeral 102, may be embodied as a telephone handset (in like fashion as a cellular telephone), may be embodied as a personal digital assistant, or may be embodied as another mobile computing device. Upon power-up, a mobile node makes an initial transmission to the nearest available access point. At the time of transmission, the access point assigns the mobile node a management channel, which identifies the mobile node to the access point. The access point and mobile node may communicate with another over a distance ranging from one to five or ten miles. Given the size of such an area, other mobile nodes may be located therein. Therefore, an access point may communicate with hundreds of mobile nodes. The use of management channels permits an access node to distinguish one access point from another.

Each access point in a WiMAX regional access network has an IP address that identifies it. However, this IP address is functional only within the regional access network (also referred to as a domain) in which the access point is situated. Thus, an access point may directly send data to another access point within the regional access network in which it is situated. To direct data to an access point in another domain, the radio network services node servicing the particular domain in which the access point is situated must be used as an intermediary.

As mentioned above, during power-up of the mobile node, an initial transmission is made to the base station for the sake of establishing a management channel and authenticating the user. Thereafter, the mobile node makes an initial communication with the voice home agent servicing the domain in which the mobile node is situated. This communication marks the beginning of a registration process, by which the mobile node informs the voice home agent of which domain the mobile node is in. In response, the voice home agent assigns the mobile node an IP address, known as a mobile IP (MIP) address. The voice home agent also records a care-of address for the mobile node. The MIP address for the mobile node does not change, even should the mobile node wander to a geographic region in which it communicates with another access point or with another

WiMAX regional access network altogether. The care-of address, on the other hand, identifies the domain with which the mobile node is communicating, and therefore changes when the mobile node roams from one regional access network to another.

A voice home agent may assign a mobile node more than one IP addresses. For example, a mobile node may have one IP address assigned to it for the carrying of voice data, and another IP address assigned to it for the carrying of signaling data. For the sake of simplicity, the disclosure proceeds from the assumption that each mobile node has a single IP address assigned to it during registration.

At the time of registration, the voice home agent updates a database that it maintains. The database may contain information concerning the features supported by the mobile node (call waiting, voicemail, etc.). The database is updated to associate a telephone number by which the mobile node is identified, the MIP address assigned to the mobile node, and the domain in which the mobile node is located (i.e., the care-of address of the mobile node).

A WiMAX regional access network 106 or 124 employs a technique known as tunneling. By virtue of this technique, movement of a mobile node within a geographic area served by a given WiMAX domain 106 or 124 is transparent to network elements or nodes outside of the domain. Thus, for example, a network node outside of WiMAX domain 106 cannot tell whether mobile node 102 is communicating with access point 104 or access point 122. A network element outside of the domain 106 need only know that the mobile node 102 is located in domain 106 to communicate with the mobile node 102. Therefore, whenever a mobile node (such as mobile node 102) moves from one domain to another, the mobile node re-registers with the voice home agent it previously registered with. In response, the voice home agent updates its database to associate a new care-of address (i.e., network address of the domain with which the mobile node communicates) with the mobile node.

The preceding discussion focused on a network environment in which a voice home agent 114 or 116 operates. The following discussion briefly presents protocol layers making up a voice home agent 114 or 116.

Figure 2 depicts a protocol stack 200 executed by the voice home agent 114 or 116. As can be seen from Figure 2, the protocol stack 200 includes a Mobile IP (MIP) layer 202 that provides functionality complying with an industry-accepted MIP standard, such as the standard described in "IP Mobility Support," C. Perkins, ed., IETF RFC 2002,

Oct. 1996. The functionality provide by the MIP layer 202 is made available to the upper layers 204-210 of the stack 200.

The MIP layer provides the tunneling functionality mentioned above. Figure 3 depicts the MIP layer 202 receiving a packet 300 having an IP header 302. The IP header 302 contains the MIP address assigned to a particular mobile node in its 32-bit destination IP address field, and it therefore termed IP $\text{Header}_{\text{MIP}}$. In response to receiving such a packet 300, the MIP layer 202 appends the packet 300 to a second IP header 304. The second IP header uses the care-of address of the particular mobile node identified by the MIP address, and is therefore termed IP $\text{Header}_{\text{CareOf}}$. Thus, the WiMAX core network 112 observes the second IP header 304 and routes the packet 300 according to the second IP header 304, meaning that the packet 300 is routed to the appropriate domain 106 or 124. Prior to reception by the mobile node, the second IP header 304 is stripped away.

The effect of the tunneling technique described with reference to Figure 3 is that each mobile node receives IP packets containing the MIP address assigned to it during the registration process. Accordingly, each mobile node may roam—even roam between domains—while retaining the IP address assigned to it during the registration process.

Many layers of tunneling may be used in the network environment 100 depicted in Figure 1. For example, each WiMAX regional access network 106 and 124 may employ tunneling, so that elements laying outside the domain need only address IP packets to the proper domain in order for the packet to reach the desired mobile node.

Returning to Figure 2, it can be seen that the protocol stack 200 also includes a VoIP layer 204, which provides voice over IP functionality that may be compliant with an industry-accepted VoIP standard, such as Realtime Transport Protocol (RTP), which is defined by IETF RFC 1889 and/or Realtime Streaming Protocol (RTSP), which is defined by IETF RFC 2326. Briefly, the VoIP layer 204 receives VoIP packets and transforms those packets into time domain multiplexed digital voice data for the public switched telephone network (PSTN) 118 and 120, and *vice versa*. As discussed below, in the context of a discussion between a user of a mobile node and a user of the PSTN, the VoIP layer 204 converts time domain multiplexed digital data into VoIP packets. The VoIP packets contain the MIP address assigned to the particular mobile node. The VoIP packets are passed to the MIP layer 202, which appends the VoIP packets to an IP header containing the care-of address of the particular mobile node.

The protocol stack 200 also includes a session initiation protocol layer 206, which provides SIP functionality that may be compliant with an industry-accepted standard, such as IETF RFC 3261. Briefly, the SIP layer 206 provides application-layer control functionality for creating, modifying, and terminating communication sessions with one or more participants. For example, the SIP layer 206 contains the functionality to signal a mobile node that another party wishes to communicate with it.

The protocol stack 200 also includes a layer 210 that interfaces with the PSTN. The layer 210 includes a media gateway (MGW) that converts time-domain multiplexed voice data into IP packets. It also includes an SS7 interface that receives SS7 signals, decodes the signals, and passes the extracted information to the voice home agent control plane 208.

The voice home agent control plane 208 coordinates the actions of the other layers. It mediates communication between the major gateway and the VoIP layer 204, and also mediate communication between the SS7 interface and the SIP layer 206. For example, the voice home agent control plane 208 may receive a signal from the SS7 interface 210 indicating that a connection to a particular telephone number is desired. In response, the control plane 208 invokes the SIP plane 206 to send an SIP invite message to the mobile node corresponding to the telephone number. Similarly, the control plane 208 receives voice data in a particular time slot and forwards the data to the VoIP layer for conversion into VoIP packets, and for communication to particular mobile node (in this way, a voice path is maintained).

The preceding discussion briefly presented protocol layers 202-210 making up a voice home agent 114 or 116. A discussion relating to the operation of the voice home agent 114 or 116 with respect to call initiation and call execution follows. This discussion describes the operation of the voice home agent as a whole (as opposed to on a layer-by-layer basis), and provides an high-level integrated view of the operation of the voice home agent.

Figure 4 depicts the operation of a voice home 114 or 116 agent in initiating a telephone call to a mobile node. The process may be initiated by a user of the PSTN or by a user of a mobile node served by the voice home agent 114 or 116. If the process is initiated by a user of the PSTN, then the voice home agent 114 or 116 receives an SS7 signal indicating that a telephone call is desired with a mobile node identified by a particular telephone number, as shown in operation 400. The telephone number is

extracted from the SS7 signal (operation 400). The SS7 signal is converted into an invite message (operation 400), which is an SIP message indicating that a communication session is desired. Thus, at the completion of operation 400, the voice home agent 114 or 116 has constructed an invite message addressed to a particular telephone number.

On the other hand, the process may have been initiated by a mobile node served by the voice home agent 114 or 116. When a mobile node initiates the phone call, the mobile node sends an SIP invite message addressed to a chosen telephone number to the voice home agent 114 or 116. This SIP invite message is received by the voice home agent, as shown in operation 402.

Whether the SIP invite message is received (as is the case when a mobile node initiates the phone call) or is created by the voice home agent (as is the case when a user of the PSTN initiates the phone call), operation flow next proceeds to operation 404. In operation 404, the voice home agent queries a database to identify a MIP address and care-of address associated with the telephone number embedded in the invite message.

If the telephone number identified in operation 404 corresponds to the domain served by the voice home agent 114 or 116, then the voice home agent 114 or 116 sends the SIP invite message to the mobile node using the tunneling technique described with reference to Figure 3 (operation 406).

If the telephone number identified in operation 404 corresponds to a domain not served by the voice home agent 114 or 116, then the voice home agent 114 or 116 sends the SIP invite message to the voice home agent 114 or 116 serving the domain corresponding to the invited mobile (operation 408).

If the telephone number indicates that the telephone number refers to a telephony device served by the PSTN, the invite message is converted to an SS7 signal to originate the phone call on the PSTN (operation 410).

After the invite message has been sent (by way of an SIP invite message or by way of an SS7 signal), the voice home agent 114 or 116 awaits a response to the invite message, as shown in operation 412. If the user of the invited telephony device wishes to answer the phone call, a response indicating such a desire is received by the voice home agent 114 or 116 (operation 412). If the response originates from a mobile node, the response may reach the voice home agent 114 or 116 in the form of an SIP acknowledge (ack) message. On the other hand, if the response originates from a PSTN telephony

device, the response may come to the voice home agent 114 or 116 in the form of an SS7 signal that may be converted into an SIP ack message.

After the response is received, it is forwarded to the initiator (operation 414). If the initiator of the phone call is a mobile node, the forwarding operation involves sending the response to the mobile node, using MIP layer 202 to employ the tunneling technique described with reference to Figure 3. On the other hand, if the initiator of the phone call is a telephony device on the PSTN, then the response is converted into an SS7 signal, and is directed to the PSTN through the SS7 interface 210.

Finally, assuming the response received in operation 412 indicates that the user of the invited mobile node wishes to engage in a communication session (i.e., wishes to answer the call), a voice path between the inviting and invited devices is established (operation 416). Establishing the voice path may involve associating a particular time slot in the time-domain multiplexed voice data from the PSTN local office 118 or 120 with a particular MIP address (and vice versa). Additionally, it may involve associating an MIP address of a mobile node with a care-of address or an address of a voice home agent 114 or 116 servicing a particular mobile node.

After a VoIP session has been established (as shown in Figure 4), the parties may speak to one another. While the parties speak, the voice home agent 114 or 116 receives either VoIP packets or time-domain multiplexed voice data from the PSTN, as shown in operation 500 of Figure 5. If the voice home agent receives time-domain multiplexed voice data from the PSTN, such data is converted to VoIP packets, as discussed above.

Next, as shown in operation 502, the VoIP packets or voice data are sent along the voice pathway established in operation 416 of Figure 4. In the case of sending VoIP packets to a mobile node, this may mean sending received VoIP packets to a voice home agent 114 or 116 servicing the mobile node, or may mean directly sending received VoIP packets to a mobile node, using the tunneling technique described with reference to Figure 3. In the case of sending voice data to telephony device on the PSTN, operation 502 includes converting VoIP data to time-domain multiplexed digital voice data, and inserting such voice data into an appropriate time slot, so that the PSTN switching equipment routes the data to the appropriate location.

The preceding discussion related to the operation of the voice home agent during initiation and execution of a phone call. The following discussion presents, from a

system-level point of view, initiation and execution of a phone call in the context of the network environment 100 depicted in Figure 1.

In the context of a telephone call between a PSTN telephony device (initiator of call) and a mobile node (responder to call), the flow proceeds as follows. Initially, the voice home agent 114 or 116 receives an SS7 signal indicating that a communication session is desired with a mobile device corresponding to a given telephone number. The voice home agent extracts the telephone number, and creates an SIP invite message addressed to an MIP address of the invited mobile node. (If the invited mobile node is not available, the call may be re-routed to a voice mail service.)

By virtue of the tunneling capability of the voice home agent and the various WiMAX domains, the SIP invite message reaches the invited mobile node, addressed to the mobile node's MIP address. Within the SIP invite message, caller-ID information is embedded. Therefore, a message identifying the inviting telephony device may be displayed at the invited mobile node. Meanwhile, the voice home agent 114 or 116 sends an SS7 signal resulting in a ring-back tone to the inviting telephony device.

If the user of the mobile node accepts the call, then an SIP acknowledgement message is sent to the voice home agent 114 or 116. The voice home agent 114 or 116 translates the SIP acknowledgement message into an SS7 signal, and establishes a voice path. At this time, the users of the PSTN telephony device and the mobile node begin speaking.

In the context of a telephone call between two mobile nodes (in different domains), the flow proceeds as follows. Initially, the voice home agent receives an SIP invite message from the inviting mobile node. The SIP invite message is addressed to a telephone number corresponding with the desired mobile node. In response, the voice home agent forwards the SIP invite message to the voice home agent servicing the domain in which the invited mobile node is located. The latter voice home agent sends the response to the MIP address of the invited mobile node.

By virtue of the tunneling capability of the voice home agent and the various WiMAX domains, the SIP invite message reaches the invited mobile node, addressed to the mobile node's MIP address. Within the SIP invite message, caller-ID information is embedded. Therefore, a message identifying the inviting telephony device may be displayed at the invited mobile node. Further, the IP address of the inviting mobile node is contained in the SIP invite message.

If the user of the invited mobile node accepts the call, then an SIP acknowledgement message is sent to the voice home agent 114 or 116 servicing the domain in which the invited mobile node is located. In response, the voice home agent 114 or 116 forwards the SIP acknowledgement message to the voice home agent 114 or 116 servicing the domain in which the inviting mobile node is located. The latter voice home agent 114 or 116 forwards the SIP acknowledgement message to the inviting mobile node's MIP address. The SIP acknowledgement message contains the IP address of the invited node.

Voice communication may now occur in one of two manners. First, the mobile nodes may communicate with one another without the mediation of voice home agents. This is possible because, by virtue of the SIP invite and acknowledgement message, each mobile node is aware of the other's IP address. However, the connection between the two mobile nodes will be lost, should either of the mobile nodes roam to a different domain.

Secondly, the voice path may extend between both voice home agents. This scheme allows for either of the mobile nodes to roam from domain to domain.

Figure 6 depicts a hardware environment in which the voice home agent 114 or 116 may be embodied. The environment includes four blades 600, 602, 604, and 606. Each blade contains its own computing environment, including a processor, a memory, and an input/output module (control hub and I/O bus, for example) providing access to a network interface or to storage. Each blade 600-606 may communicate via a local area network, such as via an Ethernet hub. The blades 600-606 may be embodied as thin boards that may be mounted within a rack.

Each blade may be dedicated to executing various facets of the previously described control plane functions or data plane functions. For example, blade 602 may execute the functions relating to the MIP layer 202. This blade 602 also executes the routing functionality required when a VoIP packet is received, and needs to be routed to another voice home agent, or to a mobile node, as described above. The blade 602 includes a network interface to permit the software/firmware executed thereon to communicate with the WiMAX core network 112.

Blade 604 may execute the VoIP functionality described above with reference to the VoIP layer 204 discussed in Figure 2. The blade 604 includes a time domain multiplexing interface to permit the software/firmware executed thereon to interact with time domain multiplexed digital voice data from the PSTN.

Blade 606 may decode SS7 signals and send the extracted content to the SS7 application layer functionality residing on blade 600. The blade 606 includes an SS7 interface to permit the software/firmware executed thereon to interact with the SS7 packets from the PSTN local office.

Blade 600 may execute the voice home agent control plane functionality described above. For this purpose, the blade include a storage device (to maintain the database necessary to enact such functionality). The blade 600 also executes the SIP functionality and application layer functionality of the SS7 subsystem. In one embodiment, the blade 600 executes a billing routine. The billing routine may track, on a user-by-user or account-by-account basis, the amount of time a given user is connected to the network, the amount of traffic consumed by the user, the type of service consumed (local call, long distance call, etc.) by the user, or the bandwidth consumed by the user. The tracked information may be stored in a database, and periodic bills may be generated therefrom.

Embodiments of the invention may be implemented in one or a combination of hardware, firmware, and software. Embodiments of the invention may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by at least one processor to perform the operations described herein. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium may include read-only memory (ROM), random-access memory (RAM), magnetic disc storage media, optical storage media, flash-memory devices, electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), and others.

The Abstract is provided to comply with 37 C.F.R. Section 1.72(b) requiring an abstract that will allow the reader to ascertain the nature and gist of the technical disclosure. It is submitted with the understanding that it will not be used to limit or interpret the scope or meaning of the claims.

In the foregoing detailed description, various features are occasionally grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments of the subject matter require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby

incorporated into the detailed description, with each claim standing on its own as a separate preferred embodiment.

Claims

The claimed invention is:

1. A device comprising:

encapsulation circuitry to receive an IP packet and prepend the packet with an IP header;

voice-over-IP (VoIP) circuitry to receive time-domain multiplexed voice data and convert said data into VoIP packets;

signaling circuitry to decode Signaling System 7 (SS7) compliant signals; and

control circuitry to

receive decoded SS7 signals from the signaling circuitry and pass the decoded SS7 signals to the encapsulation circuitry for transmission to a telephony device; and

receive VoIP packets from the VoIP circuitry and pass the VoIP packets to the encapsulation circuitry for transmission to the telephony device.

2. The device of claim 1, wherein the encapsulation circuitry, VoIP circuitry, signaling circuitry, and control circuitry are embodied as a microprocessor in data communication with a memory device.

3. The device of claim 1, wherein:

the encapsulation circuitry is embodied as a first blade, the VoIP circuitry is embodied as a second blade, the signaling circuitry is embodied as a third blade, and the control circuitry is embodied as a fourth blade; and

the first, second, third, and fourth blades are in data communication with one another.

4. The device of claim 3, wherein the first, second, third, and fourth blades communicate via an local area network.

5. The device of claim 3, wherein the fourth blade is further configured to maintain a database relating telephone numbers, mobile IP (MIP) addresses, and care-of addresses of mobile telephony devices.

6. The device of claim 3, wherein the first blade includes an interface to an IP network.

7. The device of claim 3, wherein the second blade includes an interface to a network carrying time-domain multiplexed voice data.

8. The device of claim 3, wherein the third blade includes an interface to an SS7 network.

9. A method of conducting a voice-over-IP telephony session, comprising:

receiving a request, from a first telephony device, to invite a second telephony device identified by a particular telephone number to participate in a voice-over-IP telephony session;

relating the telephone number to an IP address associated with the telephone number;

sending an invitation to the IP address;

receiving a response to the invitation; and

modifying and forwarding the response to the first telephony device, such that the modified response contains a first IP header including a first IP address of the first telephony device and a second IP header including a second IP address of the first telephony device, wherein the first IP address indicates a point of connection of the first telephony device to a network, and wherein the second IP address is generated as a result of registration of the first telephony device with a voice home agent.

10. The method of claim 9, wherein relating the telephone number to an IP address comprises accessing a database to determine an IP address of a voice home agent serving the second telephony device.

11. The method of claim 9, wherein the invitation is compliant with a session initiation protocol (SIP).

12. The method of claim 9, further comprising:

receiving an IP packet containing data representing a voice; and

forwarding the IP packet to the first device using a third IP header including a third IP address, and a fourth IP header including a fourth IP address;

wherein the third IP address indicates a point of connection of the first telephony device to a network, and wherein the fourth IP address is generated as a result of registration of the first telephony device with a voice home agent.

13. The method of claim 9, further comprising:

receiving an IP packet containing data representing a voice; and

sending the IP packet to a voice home agent serving the second device.

14. The method of claim 9, further comprising:

determining that the first telephony device changed its point of connection to the network; and

redefining the first IP address to identify the changed point of connection.

15. The method of claim 9, wherein the first IP address identifies a radio network services node coupled to an 802.16e-compliant network that includes an access point to which the first telephony device communicates.

16. A machine-accessible medium that provides instructions, which when accessed, cause the machine to perform operations comprising:

receiving a request, from a first telephony device, to invite a second telephony device identified by a particular telephone number to participate in a voice-over-IP telephony session;

relating the telephone number to an IP address associated with the telephone number;

sending an invitation to the IP address;

receiving a response to the invitation; and

modifying and forwarding the response to the first telephony device, such that the modified response contains a first IP header including a first IP address of the first telephony device and a second IP header including a second IP address of the first telephony device, wherein the first IP address indicates a point of connection of the first telephony device to a network, and wherein the second IP address is generated as a result of registration of the first telephony device with a voice home agent.

17. The medium of claim 16, wherein relating the telephone number to an IP address comprises accessing a database to determine an IP address of a voice home agent serving the second device.

18. The medium of claim 16, wherein the invitation is compliant with session initiation protocol (SIP).

19. The medium of claim 16, wherein the operations further comprise:

receiving an IP packet containing data representing a voice; and

forwarding the IP packet to the first device using a third IP header including a third IP address, and a fourth IP header including a fourth IP address;

wherein the third IP address indicates a point of connection of the first telephony device to a network, and wherein the fourth IP address is generated as a result of registration of the first telephony device with a voice home agent.

20. The medium of claim 16, wherein the operations further comprise:

receiving an IP packet containing data representing a voice; and

sending the IP packet to a voice home agent serving the second device.

21. The medium of claim 16, wherein the operations further comprise:

determining that the first telephony device changed its point of connection to the network; and

redefining the first IP address to identify the changed point of connection.

22. The medium of claim 16, wherein the first IP address identifies a radio network services node coupled to an 802.16e-compliant network that includes an access point to which the first telephony device communicates.

23. A system comprising:

encapsulation circuitry to receive an IP packet and prepend the packet with an IP header;

voice-over-IP (VoIP) circuitry to receive time-domain multiplexed voice data and convert said data into VoIP packets;

billing circuitry that is configured to measure duration and type of use of said system, and to relate such measurements to a user account;

signaling circuitry to decode Signaling System 7 (SS7) compliant signals; and

control circuitry to

receive decoded SS7 signals from the signaling circuitry and pass the decoded SS7 signals to the encapsulation circuitry for transmission to a telephony device; and

receive VoIP packets from the VoIP circuitry and pass the VoIP packets to the encapsulation circuitry for transmission to the telephony device.

24. The system of claim 23, wherein the encapsulation circuitry, VoIP circuitry, signaling circuitry, billing circuitry, and control circuitry are embodied as a microprocessor in data communication with a memory device.

25. The system of claim 23, wherein:

the encapsulation circuitry is embodied as a first blade, the VoIP circuitry is embodied as a second blade, the signaling circuitry is embodied as a third blade, and the control circuitry and billing circuitry are embodied together as a fourth blade; and

the first, second, third, and fourth blades are in data communication with one another.

26. The system of claim 25, wherein the first, second, third, and fourth blades communicate via an local area network.

27. The system of claim 25, wherein the fourth blade is further configured to maintain a database relating telephone numbers, mobile IP (MIP) addresses, and care-of addresses of mobile telephony devices.

28. The system of claim 25, wherein the first blade includes an interface to an IP network.

29. The system of claim 25, wherein the second blade includes an interface to a network carrying time-domain multiplexed voice data.

30. The system of claim 25, wherein the third blade includes an interface to an SS7 network.

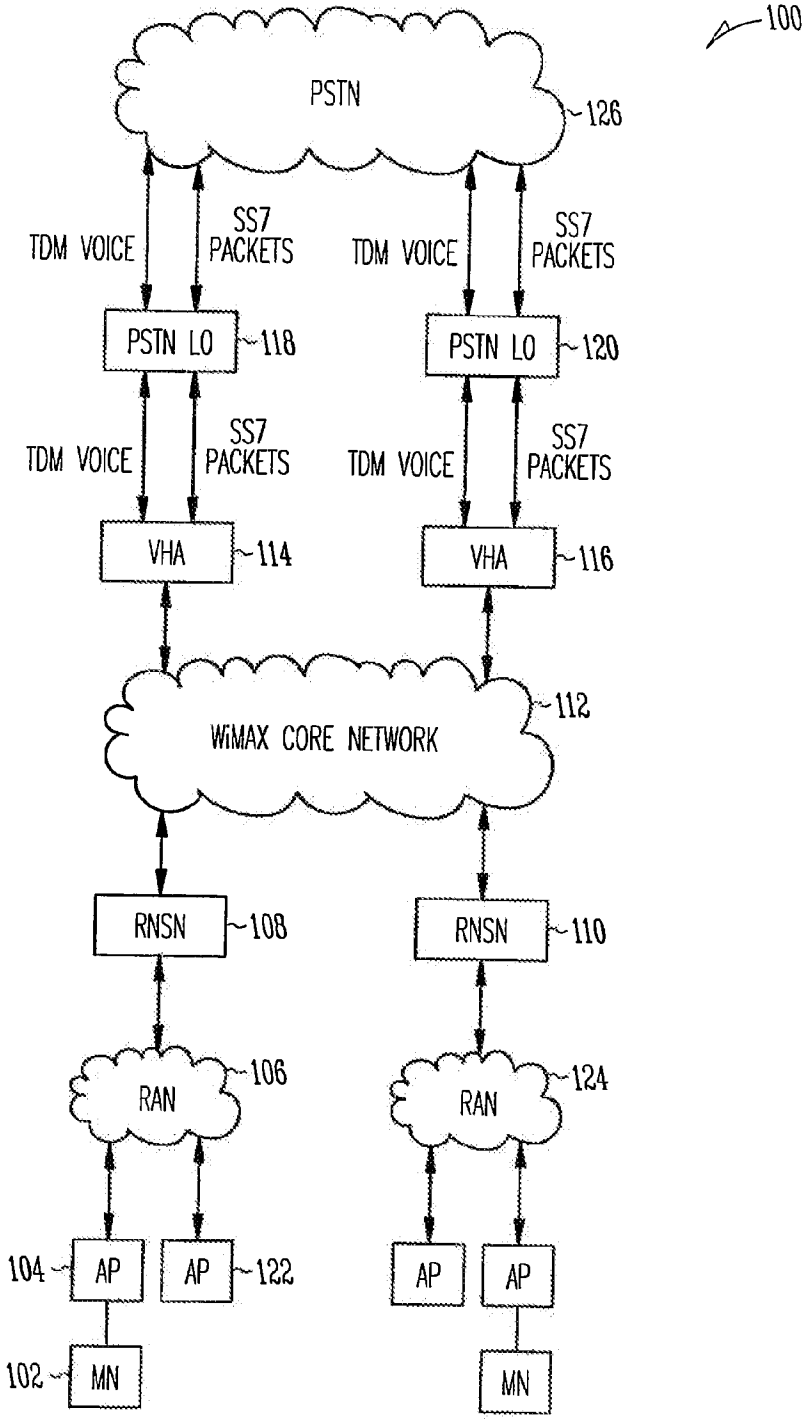

100
PSTN
126
TDM VOICE
SS7 PACKETS
TDM VOICE
SS7 PACKETS
PSTN LO
118
PSTN LO
120
TDM VOICE
SS7 PACKETS
TDM VOICE
SS7 PACKETS
VHA
114
VHA
116
WiMAX CORE NETWORK
112
RNSN
108
RNSN
110
RAN
106
RAN
124
104
AP
AP
122
AP
AP
102
MN
MN

Fig. 1

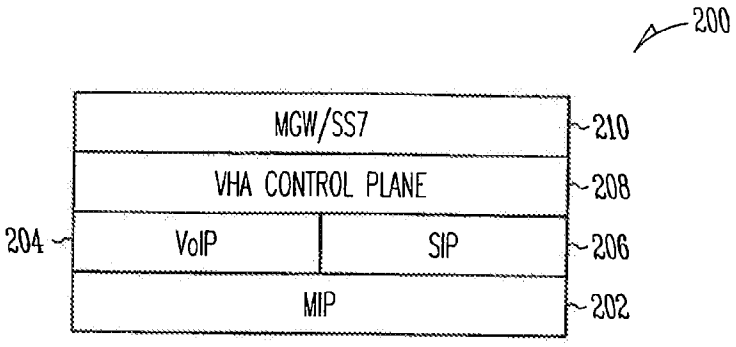

200
MGW/SS7
210
VHA CONTROL PLANE
208
204
VoIP
SIP
206
MIP
202

Fig.2

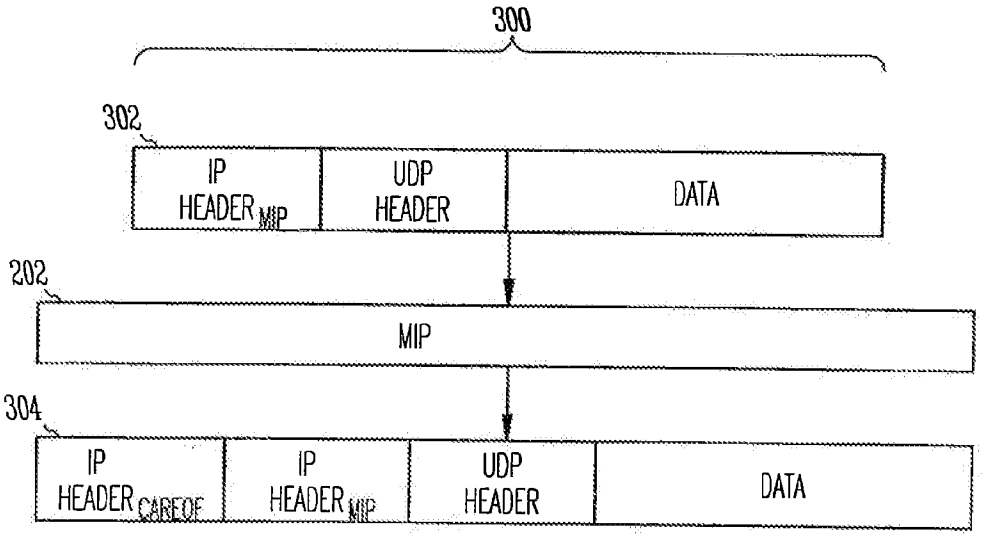

300
302
IP HEADER MIP
UDP HEADER
DATA
202
MIP
304
IP HEADER CAREOF
IP HEADER MIP
UDP HEADER
DATA

Fig.3

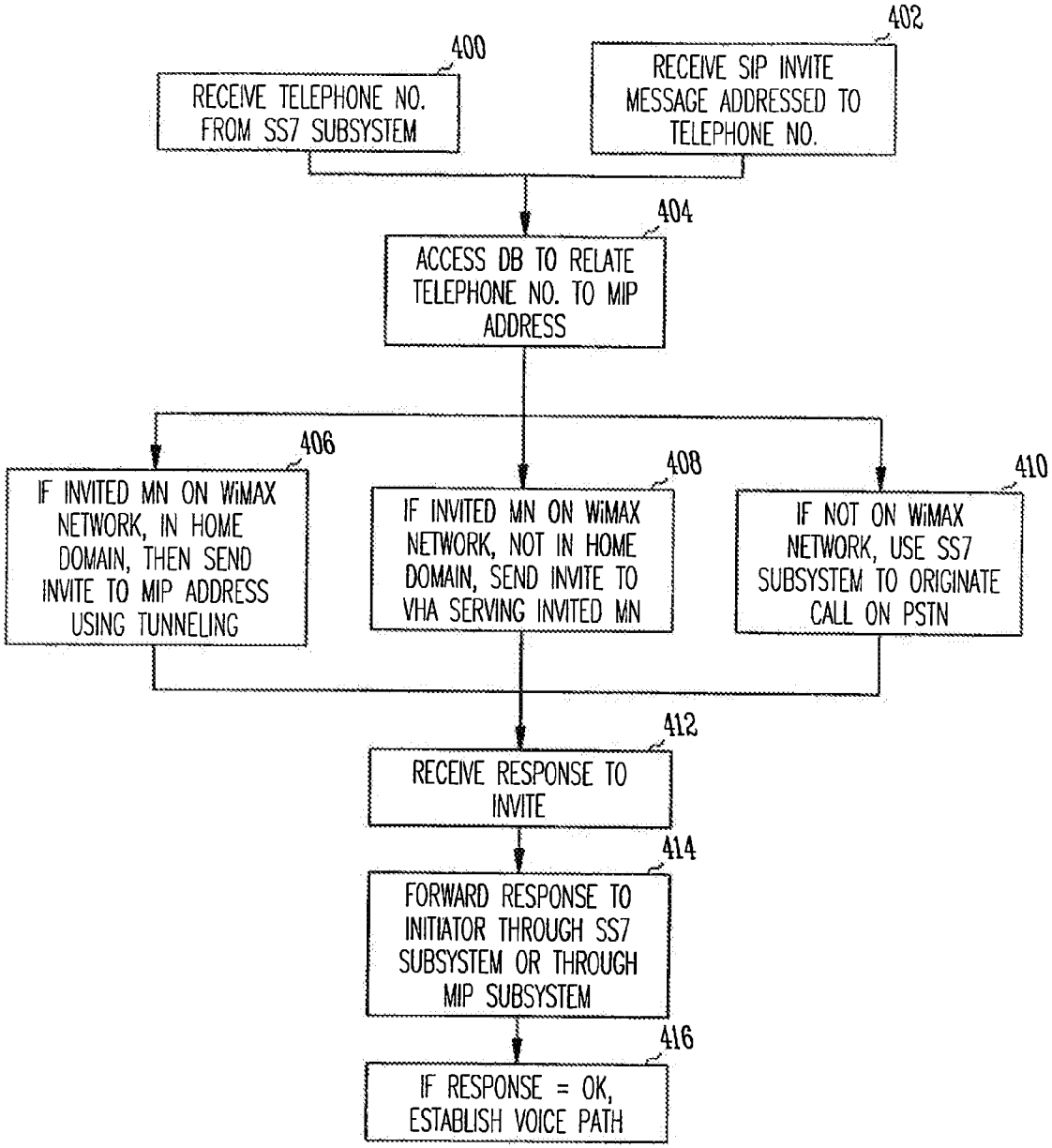

400
RECEIVE TELEPHONE NO. FROM SS7 SUBSYSTEM
402
RECEIVE SIP INVITE MESSAGE ADDRESSED TO TELEPHONE NO.
404
ACCESS DB TO RELATE TELEPHONE NO. TO MIP ADDRESS
406
IF INVITED MN ON WiMAX NETWORK, IN HOME DOMAIN, THEN SEND INVITE TO MIP ADDRESS USING TUNNELING
408
IF INVITED MN ON WiMAX NETWORK, NOT IN HOME DOMAIN, SEND INVITE TO VHA SERVING INVITED MN
410
IF NOT ON WiMAX NETWORK, USE SS7 SUBSYSTEM TO ORIGINATE CALL ON PSTN
412
RECEIVE RESPONSE TO INVITE
414
FORWARD RESPONSE TO INITIATOR THROUGH SS7 SUBSYSTEM OR THROUGH MIP SUBSYSTEM
416
IF RESPONSE = OK, ESTABLISH VOICE PATH

Fig. 4

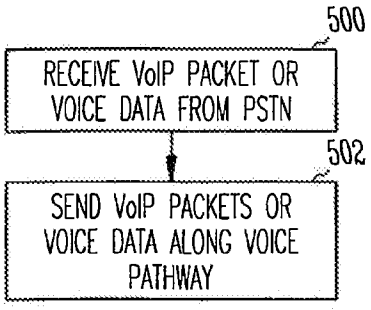

500
RECEIVE VoIP PACKET OR VOICE DATA FROM PSTN
502
SEND VoIP PACKETS OR VOICE DATA ALONG VOICE PATHWAY

Fig. 5

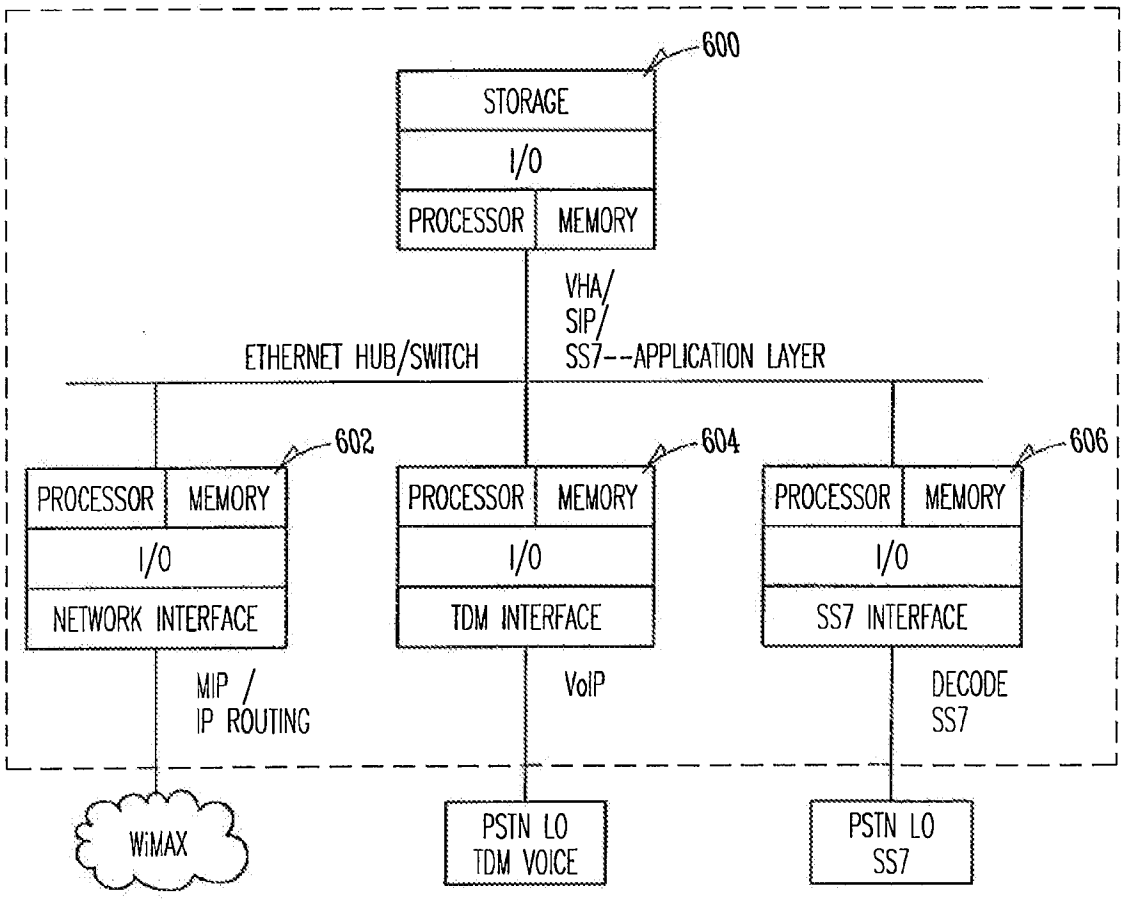

600
STORAGE
I/O
PROCESSOR
MEMORY
VHA/
SIP/
SS7--APPLICATION LAYER
ETHERNET HUB/SWITCH
602
PROCESSOR
MEMORY
I/O
NETWORK INTERFACE
604
PROCESSOR
MEMORY
I/O
TDM INTERFACE
606
PROCESSOR
MEMORY
I/O
SS7 INTERFACE
MIP /
IP ROUTING
VoIP
DECODE
SS7
WiMAX
PSTN LO
TDM VOICE
PSTN LO
SS7

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2005/047679

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/79825 A (NOKIA NETWORKS OY; NOKIA INC.) 28 December 2000 (2000-12-28) page 1 - page 5 page 8 - page 25 -----	1-30
X	NEWMAN P.: "IN SEARCH OF THE ALL-IP MOBILE NETWORK" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER,NEW YORK, NY, US, vol. 42, no. 12, December 2004 (2004-12), pages S03-S08, XP001211443 ISSN: 0163-6804 page S03 - page S05 -----	1-30
	-/--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 April 2006	04/05/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jurca, A

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DUTTA A. ET AL.: "Realizing mobile wireless Internet telephony and streaming multimedia testbed" COMPUTER COMMUNICATIONS, ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL, vol. 27, no. 8, May 2004 (2004-05), pages 725-738, XP004501203 ISSN: 0140-3664 page 726 - page 733	1-30
X	MORAND L ET AL: "Global mobility approach with mobile IP in all IP networks" ICC 2002. 2002 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS. CONFERENCE PROCEEDINGS. NEW YORK, NY, APRIL 28 - MAY 2, 2002, IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, NEW YORK, NY : IEEE, US, vol. VOL. 1 OF 5, 28 April 2002 (2002-04-28), pages 2075-2079, XP010589851 ISBN: 0-7803-7400-2 page 2075 - page 2077	1-30
A	WO 01/67789 A (TELEFONAKTIEBOLAGET LM ERICSSON) 13 September 2001 (2001-09-13) page 16 - page 20 figure 8	1-30

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2005/047679

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-8 and 23-30

Claims 1-8 and 23-30 are directed to a tunneling VoIP / PSTN gateway. This is done by decoding SS7 signals, converting TDM voice into VoIP and further encapsulating everything into IP.

---

2. claims: 9-22

Claims 9-22 are directed to the conducting of a VoIP session using tunneling. This is done by receiving a request, from a first telephony device, to invite a second telephony device identified by a particular telephone number relating a telephone number to an IP address; sending an invitation to the IP address; receiving a response to the invitation; modifying and forwarding the response, such that the modified response contains a first IP header including a first IP address of the first telephony device and a second IP header including a second IP address of the first telephony device, wherein the first IP address indicates a point of connection of the first telephony device to a network, and wherein the second IP address is generated as a result of registration of the first telephony device with a voice home agent.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2005/047679

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0079825 A	28-12-2000	AU 5096400 A	09-01-2001
WO 0167789 A	13-09-2001	AU 4832801 A	17-09-2001

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/078175 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/NZ2006/000001

(22) International Filing Date: 17 January 2006 (17.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
537800 20 January 2005 (20.01.2005) NZ

(71) Applicant and
(72) Inventor: **BAKER, Colin, Lawrence Melvin** [NZ/NZ]; 5/27 Birdwood Crescent, Parnell, Auckland, 1001 (NZ).

(74) Agent: **CARTWRIGHT, Peter**; 29 Waterloo Road, Lower Hutt, 3009, (NZ).

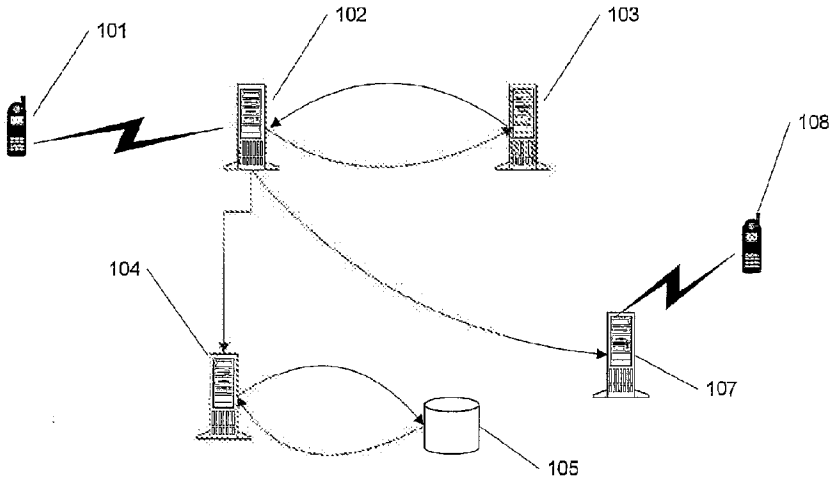
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

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

(54) Title: TELEPHONE NUMBER ALLOCATION



(57) **Abstract:** To provide a globally useful telephone number a character string which may be similar to an email address may be provided to a mobile phone server or an internet server for translation to the actual phone number and establishment of a call to that number.

WO 2006/078175 A2

TELEPHONE NUMBER ALLOCATION

Technical Field

The invention generally relates to the allocation of telephone numbers and to telephone number portability.

More particularly the invention relates to the allocation of telephone numbers so that a telephone subscriber has a phone number usable globally.

Background Art

It is known that a telephone number which is usable globally is highly desirable.

While there are numbering schemes which allow calling a phone in any country there is no method of allocating a telephone number to a person or a mobile telephone which will allow the telephone to be rung from any location in the world. Similarly, in most countries, it is not possible to transfer among phone providers and retain the same telephone number.

The closest approach requires the use of a telephone linked directly to a satellite, as for instance the Iridium® multiple satellite system which can provide communications from anywhere in the world by linking to one of a constellation of orbiting satellites.

A second method relies on the use of a cell phone which is inter-operable with the majority of cell phone systems available, and which can be entered into the database of a telephone service provider in a country concerned prior to the phone being brought into the country by a person. Some organisation beforehand is required.

It is possible to have the cell phone system in a country recognize the entry of a previously unrecognised phone as it connects to a local cell, recognise the cell phone origin, and interrogate the country of origin for the details it requires to work with the phone, but such systems require co-operation between providers in different countries and the infrastructure in many countries currently prevents this.

Other systems have proposed to treat a phone as a network card is treated in the Internet, that is, the phone has a unique network ID which can be detected from anywhere in the world, and the signal for the phone transmitted to the phone either via

the internet or via routing against a route extracted from the internet. Again considerable co-operation between providers is required for such a system to gain wide coverage.

There are already systems in existence which define the format of a global telephone number, such as standard E.164, and draft standards which define ways in which this number can be presented as an internet translatable URI (Universal Resource Identifier – see RFC3986). For instance a global number may translate under ENUM (E.164 to Uniform Resource Identifiers Dynamic Delegation Discovery System Application) as the domain name "tel: 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa" or under the Internet Society RFC2086 as "tel: +380069236144" or "tel: 36144;phone-context=watt.co.nz". None of these methods produces a name which is particularly memorable.

The general public has become used to seeing URI's presented without the initial scheme identifier (such as "http:"), and the use of the identifiers which are peculiar to telephony, such as "tel:", "sip:" is virtually unknown.

Mobile telephones now have alphanumeric keyboards, and displays to view entered data. While entry of numbers is comparatively quick entry of names is slower, but technology is allowing faster entry as time passes. Certainly it is easier to remember a name than to remember a string of numbers. Hence it is desirable to enter a name rather than a telephone number, however telephone exchanges do not accept names.

Other systems of relating such alphanumeric strings to telephone numbers in a network environment are known, such as US patent application publication US 2003/0074461, but these solutions require passing identifiers for the type of query presented, which implies some type of user knowledge of what to do. This is generally not available.

The present invention provides a solution to this and other problems which offers advantages over the prior art or which will at least provide the public with a useful choice.

Summary Of The Invention

In one exemplification the invention consists in a method of looking up a phone address as a URI comprising allocating a URI as the phone address, the URI being

located within an existing authority domain, on interrogation of the domain recognising that the URI does not relate to a valid page, subsequently comparing the URI with a list of phone number aliases, and returning the phone number to which the alias relates to the interrogating process.

Preferably the URI is a URL and the phone number alias is formatted as a userinfo subcomponent in an authority domain name.

Preferably the URL includes a delimiter replacing the standard userinfo delimiter.

Preferably the URI is a URL and the phone number alias is formatted as a subcomponent of the authority domain name with an identifiable first subcomponent.

Preferably the first subcomponent is "gpn".

In an alternative embodiment the invention relates to a method of providing an alias to a telephone number comprising specifying a phone number alias as a validly formatted hypertext transfer protocol (HTTP) address, detecting on query at the server corresponding to the address that the address does not relate to a valid HTTP page, confirming that the address relates to a phone number alias, and returning to the querying process the phone number and location relating to the alias.

Preferably the location identifies the phone code for a country.

Preferably the phone number and location are returned in standard international phone number format.

In a yet further embodiment the invention consists in apparatus for translating a telephone number being syntactically a valid domain name, the apparatus having:

a recogniser at the server representing the domain name which detects the syntactically valid domain name as a non-existent domain name reference and attempts to match the syntactically valid domain name against an entry in a list of phone number aliases

wherein on detecting a match the recogniser returns the phone number of which the syntactically valid domain name is the alias.

A further embodiment of the invention relates to an apparatus for translating a telephone number alias presented as a userinfo prefix, an authority domain name suffix and a valid URI separator between the two, the apparatus having:

a domain name recogniser

a recogniser for the separator which recognises it as denoting the prefix as being a phone number alias

a phone number alias lookup which returns the phone number equivalent to the userinfo prefix.

Preferably the apparatus is incorporated in a web server.

These and other features of as well as advantages which characterise the present invention will be apparent upon reading of the following detailed description and review of the associated drawings.

Brief Description of the Drawings

FIG. 1 is a first block diagram of a first implementation of the invention

FIG 2 is a block diagram of the detection of a phone address in a web server.

FIG 3 shows the process as it takes place at the calling phone.

Description of the Invention

It is proposed to use as a phone number a name similar to that of an email. The separating "@" used in an email may be replaced by a different character which is similarly reserved in a URI. Such a character could be one of the existing characters already reserved for use in the URI, such as a "." or "$". This has the advantage that a telephone user may have a phone number and an email name which are almost identical. Thus an email might be mailto:joel.bloggs@trisotto.com.au while the phone name could be http://joel.bloggs.trisotto.com.au or http://joel.bloggs$trisotto.com.au. The telephone authority name may have a distinctive leader to enable easy identification of the fact that this is a telephone name, for instance a leader such as "gpn" will give a phone name of http://gpn.joel.bloggs.trisotto.com.au indicating to the server at trissotto.com.au that this is a global phone number. As yet another alternative the use of phone names may be restricted to a single authority domain which specialises in translating phone names to phone numbers and directing a call to the actual phone called. In such a system a phone name might be http://joel.bloggs.trisotto.com.au@gpn.com, this being a standard format for a userinfo subcomponent (see RFC 3986) and an authority domain

name. As a variation, a complete domain could be named as .gpn and dedicated to the redirection of calls to phones so that joel.bloggs@trissotto.com.au.gpn would be a viable domain name.

Each of these possible methods of naming requires a different method of handling the phone call which issues to these addresses.

It is assumed that a phone will always have an allocated number, which may be global or local, but may be called by use of the alias as used above.

It is assumed that a phone can always call outwards, since it has only to identify a cellphone server or exchange which it can interrogate. Calling in to a phone using an alias is the problem which the current invention solves.

Figure 1 shows a call from one phone (101) to another (108) using an alias, as for instance joel.bloggs.trisotto.com.au. Phone (101) is connected to cellphone server (102), although a POTS exchange server may be substituted where the calling telephone is not a cellphone, provided that the exchange is equipped to handle the input of alphanumeric codes (as for instance in text dialling). The cellphone server is connected to a digital network having internet and telephone gateway access. The cellphone server (102) receives a request for a call from phone (101), the called phone being identified only by an authority domain name string. No scheme identifier is used, but the server/exchange (102) to which the calling phone is connected is set to assume that the call is an http scheme call since a) there is no scheme shown, and b) the called name is neither numeric nor meets the requirements for an IP address. The server therefore hands off the call to a DNS (Domain Name Server) (103) which will attempt to find the domain name (trisotto.com.au). Assuming it succeeds in this it passes back the IP address to the server which initially interrogated it. The cellphone server then interrogates the address corresponding to http://joel.bloggs.trisotto.com.au which is on host server (104).

The host server responds by recognising that the page requested is actually a phone number request and providing the current location of the called phone. As shown at FIG 2 it gets this by receiving the phone alias as a URL at (201) and returning a web page if this is a valid web page address at (203). If the page is not a valid page the error routine compares the address by string comparison against a list of phone number aliases held in the server at (204) in a known manner and if this is a recorded

phone number alias at returns it at (206). If it is not a valid phone address the standard error page is returned. The returned number may be either the local number and country identifier or it may be a number in one of the standard global formats such as ENUM.

The format of the returned message may be any valid format which is recognised by the calling server as a phone number, for instance it may merely be the HTTP response with a pre-defined header carrying the phone number, or it may be a full HTTP SOAP message including the phone number, or it may be an HTML page including the phone number in a known format. The cellphone server retrieves the phone number from the returned data and connects the caller to it in a known manner.

Optionally the host server places a query via a centralised Number Portability Database (NPDB) (105) using Query on Release (QoR) as outlined in Internet Society paper RFC3482 to receive the current location of the called phone. The lookup of the location may involve queries to the donor network (ie the network which originally created the phone number) and from there a call to the network last recognised as having contact with the phone. Having received this information it is passed back to the originating server/exchange (102) with the actual phone number in a QoR. The originating server/exchange then completes the call to the identified telephone gateway server (107) and so to phone (108). Clearly the server (104) hosting the domain name must be using software which is capable of calling the NPDB database and of performing a QoR, however this will have been downloaded by the server as part of a the phone number handling package which provided the alias mechanism.

Drawing FIG 3 shows an alternative method in which the phone, with a WAP display, may enter a phone name as one of several others in a list at (301). At (302) a phone name is selected from the list and the corresponding http address queried at (303). The querying phone receives a response at (304) which will be either an error message (305) (where the phone name does not exist) or a valid phone number encapsulated in a web page at (306) or another format recognised by the receiving phone as containing a phone number. Where a valid phone number is received the phone may autodial the number to connect to the called name as at (308) otherwise the returned page is displayed. It should be noted that the correspondence between the name and number is held and maintained centrally, as opposed to the usual

cellphone where the name and number correspondence must be maintained locally by each user.

Where an address such as http://joel.bloggs$trisotto.com.au is used the process is required to be slightly different. Such a URI requires that the DNS contacted be set up to recognise this as an address to be referred to domain trisotto.com.au, ie that the portion of the address before the "$" be disregarded and treated as the DNS would normally treat a userinfo subcomponent. At the domain server the same process as above takes place, with the difference that the server need not recognize that the "page" is actually a request for a phone number. Instead the phone user name "joel.bloggs" is simply referred to a lookup table of phone numbers and the same request to an NPDB database and handoff by QoR is then performed.

The described methods place the main burden of determining the actual telephone number on the server for the domain name to which the telephone belongs, since this is where the domain name to phone number relationship is actually held. The phone number normally output from the domain name server is, where possible, a global telephone number, however the output may be the telephone number in local form, the NPDB database being relied upon to translate to a global number.

It is possible for an alternative system to operate in which each telephone does actually have a permanent IP address. Because of the transient nature of cellphones the address translation from name to IP address as held in the DNS servers is not likely to be validly located in a local server, and instead the request is routed to the relevant root domain name server (104). Here a lookup is performed to the IP address of the telephone and this is returned to server (102) and a search instigated for that address as present on a telephone gateway. Once found the audio signal packets may be transferred.

While the description relates to the use of the invention in simple hypertext transfer protocol the return of a phone number will work equally well as a web service, with the added advantage that the process is hidden as far as the user is concerned. Thus, in practice, a user will select or enter a phone name to call, the phone, connected to the internet, will call the web service to identify the actual phone number, and this will then be dialled automatically on receipt of the return from the web service.

The phone alias is preferably formed from an existing email or other address of the phone user so that it is easily remembered by the user. In most instances the transliteration of the users email address will provide a unique phone alias which is also valid as a web address.

It is to be understood that even though numerous characteristics and advantages of the various embodiments of the present invention have been set forth in the foregoing description, together with details of the structure and functioning of various embodiments of the invention, this disclosure is illustrative only, and changes may be made in detail so long as the functioning of the invention is not adversely affected. For example the particular elements of the telephone number lookup may vary dependent on the particular application for which it is used without variation in the spirit and scope of the present invention.

In addition, although the preferred embodiments described herein are directed to cellphones for use in a worldwide calling system, it will be appreciated by those skilled in the art that the teachings of the present invention can be applied to other systems such as local internal exchanges, without departing from the scope and spirit of the present invention.

Technical Applicability

The application relates to a method and apparatus for allowing a telephone number to be expressed as a character string and to be accepted by the technical infrastructure throughout the world. As such it has technical applicability

CLAIMS

1. A method of looking up a phone address as a URI comprising allocating a URI as the phone address, the URI being located within an existing authority domain, on interrogation of the domain recognising that the URI does not relate to a valid page, subsequently comparing the URI with a list of phone number aliases, and returning the phone number to which the alias relates to the interrogating process.

2. A method as claimed in claim 1 wherein the URI is a URL and the phone number alias is formatted as a userinfo subcomponent in an authority domain name.

3. A method as claimed in claim 2 wherein the URL includes a delimiter replacing the standard userinfo delimiter.

4. A method as claimed in claim 1 wherein the URI is a URL and the phone number alias is formatted as a subcomponent of the authority domain name with an identifiable first subcomponent.

5. A method as claimed in claim 4 wherein the first subcomponent is "gpn".

6. A method of providing an alias to a telephone number comprising specifying a phone number alias as a validly formatted hypertext transfer protocol (HTTP) address, detecting on query at the server corresponding to the address that the address does not relate to a valid HTTP page, confirming that the address relates to a phone number alias, and returning to the querying process the phone number and location relating to the alias.

7. A method as claimed in claim 6 wherein the location identifies the phone code for a country.

8. A method as claimed in claim 6 wherein the phone number and location are returned in standard international phone number format.

9. An apparatus for translating a telephone number being syntactically a valid domain name, the apparatus having:

a recogniser at the server representing the domain name which detects the syntactically valid domain name as a non-existent domain name reference

and attempts to match the syntactically valid domain name against an entry in a list of phone number aliases

wherein on detecting a match the recogniser returns the phone number of which the syntactically valid domain name is the alias.

10. An apparatus for translating a telephone number alias presented as a userinfo prefix, an authority domain name suffix and a valid URI separator between the two, the apparatus having:

a domain name recogniser

a recogniser for the separator which recognises it as denoting the prefix as being a phone number alias

a phone number alias lookup which returns the phone number equivalent to the userinfo prefix.

11. An apparatus as claimed in claim 10 wherein the apparatus is incorporated in a web server.

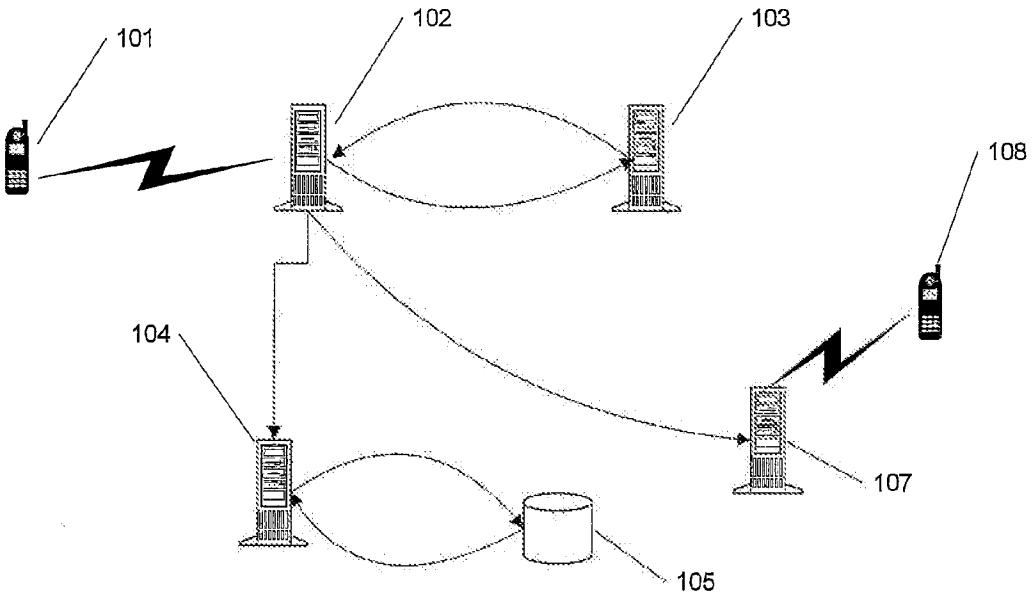

101
102
103
108
104
107
105

FIG. 1

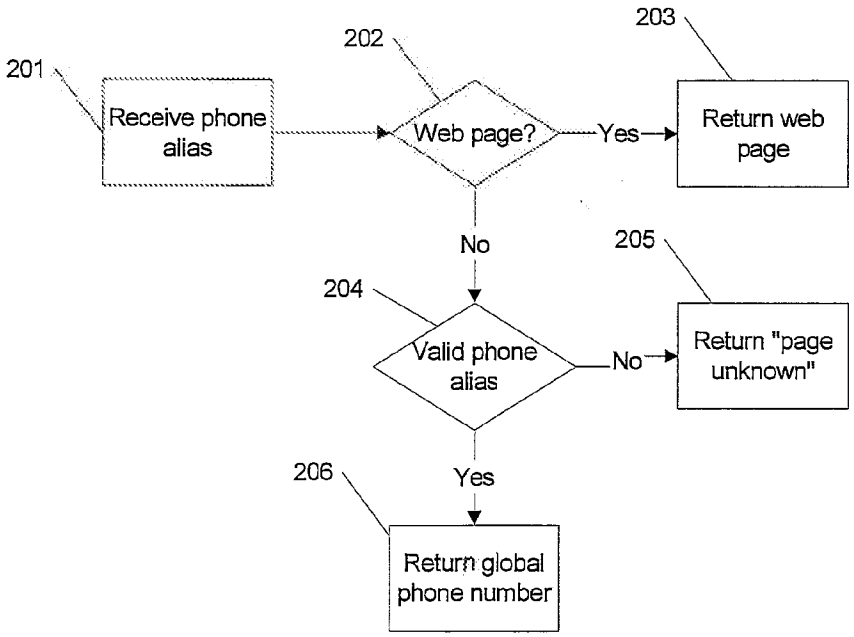

201
Receive phone alias
202
Web page?
Yes
203
Return web page
No
204
Valid phone alias
No
205
Return "page unknown"
Yes
206
Return global phone number

FIG. 2

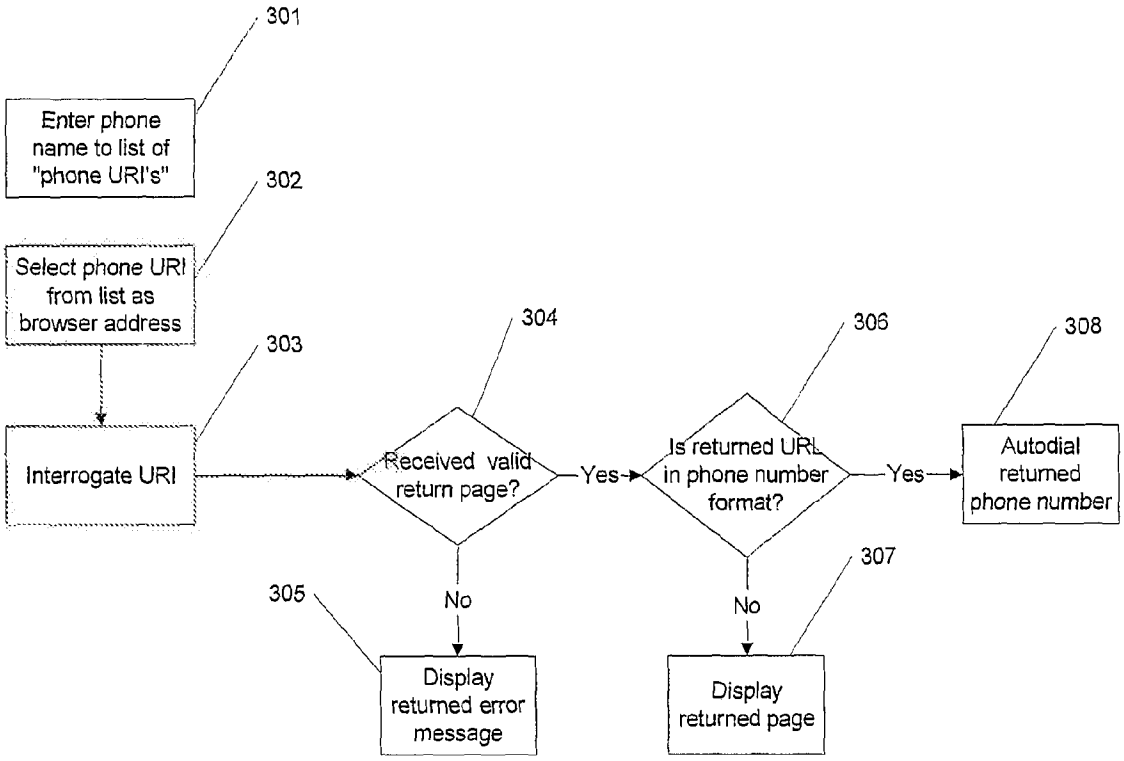

301
Enter phone name to list of "phone URI's"
302
Select phone URI from list as browser address
303
Interrogate URI
304
Received valid return page?
Yes
306
Is returned URL in phone number format?
Yes
308
Autodial returned phone number
No
305
Display returned error message
No
307
Display returned page

FIG. 3

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/078175 A3

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/NZ2006/000001

(22) International Filing Date: 17 January 2006 (17.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
537800 20 January 2005 (20.01.2005) NZ

(71) Applicant and
(72) Inventor: **BAKER, Colin, Lawrence Melvin** [NZ/NZ]; 5/27 Birdwood Crescent, Parnell, Auckland, 1001 (NZ).

(74) Agent: **CARTWRIGHT, Peter**; 29 Waterloo Road, Lower Hutt, 3009, (NZ).

(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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

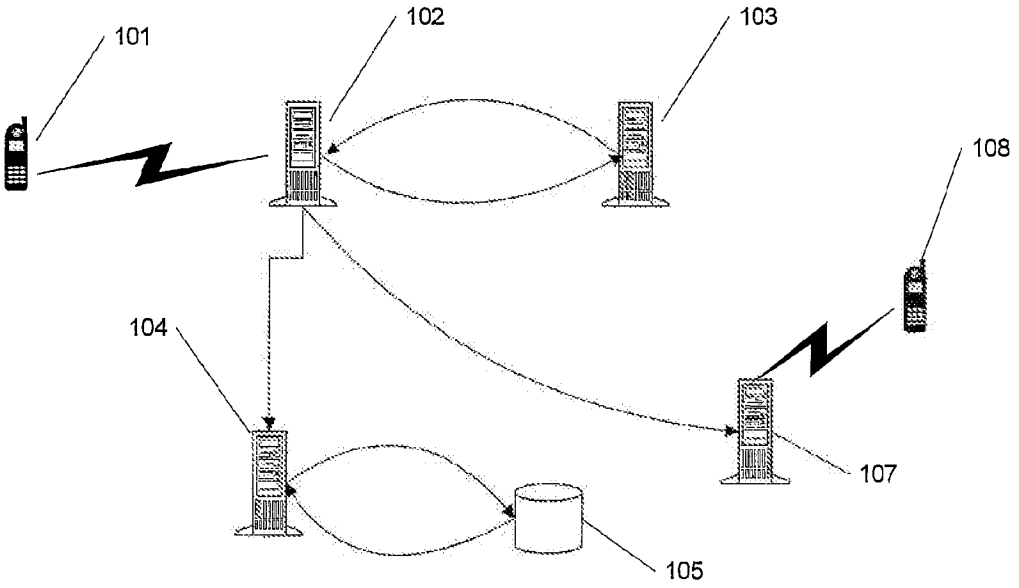
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, 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:
— *with international search report*

(88) Date of publication of the international search report:
8 September 2006

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

(54) Title: TELEPHONE NUMBER ALLOCATION



(57) Abstract: To provide a globally useful telephone number a character string which may be similar to an email address may be provided to a mobile phone server or an internet server for translation to the actual phone number and establishment of a call to that number.

WO 2006/078175 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ2006/000001

A. CLASSIFICATION OF SUBJECT MATTER

G06F 17/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8 G06F 17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Patents and applications for inventions since 1975
Korean Utility models and applictions for Utility models since 1975
Japanese Utility models and application for Utility models since 1975

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

eKIPASS "URI, PHONE, ALIAS, URL"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	KR 2001-106543 A (JANG, JUN SEOK; ET AL) 7 DECEMBER 2001 SEE THE WHOLE DOCUMENT	1-4, 6, 9-11 5, 7, 8
Y	JP 11-328076 A (ATEX KK) 30 NOVEMBER 1999 SEE THE WHOLE DOCUMENT	1-11
Y	KR 2001-76731 A (JANG, JUN SEOK; ET AL) 16 AUGUST 2001 SEE THE WHOLE DOCUMENT	1-11
A	US 6012067 A (SHYAM SUNDAR SARKAR) 4 JANUARY 2000 SEE THE WHOLE DOCUMENT	1-11
A	JP10-78928 A (D & I SYST KK) 24 MARCH 1998 SEE THE WHOLE DOCUMENT	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 JUNE 2006 (16.06.2006)	**20 JUNE 2006 (20.06.2006)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	LEE, Jung Suk Telephone No. 82-42-481-5789

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/NZ2006/000001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2001-106543 A	07/12/2001	WO 0155915 A1	02/08/2001
JP 11-328076 A	30/11/1999	NONE	
KR 2001-76731 A	16/08/2001	WO 0155915 A1	02/08/2001
US 6012067 A	04/01/2000	NONE	
JP 10-78928 A	24/03/1998	US 7058726	06/06/2006

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2007 (19.04.2007)

PCT

(10) International Publication Number
WO 2007/044454 A2

(51) International Patent Classification:
H04M 11/04 (2006.01)

(21) International Application Number:
PCT/US2006/038946

(22) International Filing Date: 4 October 2006 (04.10.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/723,961 6 October 2005 (06.10.2005) US
11/503,912 15 August 2006 (15.08.2006) US

(71) Applicant *(for all designated States except US)*: **TELECOMMUNICATION SYSTEMS, INC.** [US/US]; 275 WEST STREET, Suite 400, Annapolis, MD 21401 (US).

(72) Inventors: **CROY, Jon**; 3019 24th Avenue W, Seattle, WA 98199 (US). **HINES, John, Gordon**; 120 10th Street, Kirkland, WA 98033 (US). **JOHNSON, Darrin**; 16447 169th Street SE, Monroe, WA 98272 (US).

(74) Agent: **BOLLMAN, William, H.**; Manelli Denison & Selter PLLC, 2000 M Street, NW, 7th Floor, Washington, DC 20036 (US).

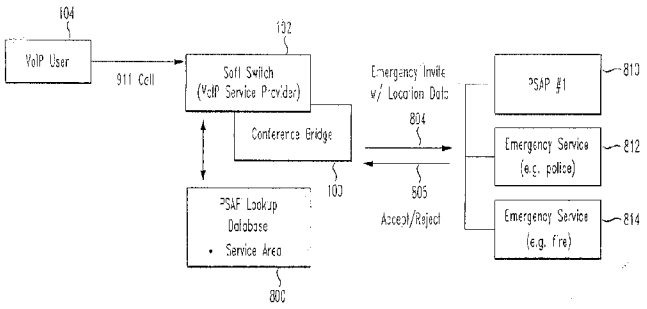
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, 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, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

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

(54) Title: VOICE OVER INTERNET PROTOCOL (VOIP) LOCATION BASED 911 CONFERENCING



(57) Abstract: Voice Over Internet Protocol (VoIP) emergency calls to an Emergency Response Center (ERC) are handled through a VoIP conference bridge on a VoIP service provider's soft switch. The soft switch works with a VoIP positioning center (VPC) to obtain location information, which is compared against a PSAP database to find an initial best-appropriate PSAP for the location of the emergency caller. The PSAP is issued an Invite message to join the conference, establishing an emergency call. Third parties such as police, ambulance may be issued Invite messages to join the conference. Cold transfers are avoided by Inviting participants to join a single emergency conference rather than passing an emergency call from party to party (e.g., from PSAP to police to ambulance, etc.) The PSAP, other emergency responders, and even the initial VoIP emergency caller may leave and rejoin the VoIP conference without dropping the conference between the others.

WO 2007/044454 A2

VOICE OVER INTERNET PROTOCOL (VoIP) LOCATION BASED 911 CONFERENCING

This application is related to and claims priority from a co-pending U.S. Provisional Application No. 60/723,960, entitled "Voice Over Internet Protocol (VoIP) Location Based Conferencing", filed on October 6, 2005; U.S. Provisional Application No. 60/733,789, entitled "Voice Over Internet Protocol (VoIP) Multi-User Conferencing", filed on November 7, 2005; and U.S. Provisional Application No. 60/723,961, entitled "Voice Over Internet Protocol (VoIP) Location Based 911 Conferencing", filed on October 6, 2005; the entirety of all three of which are expressly incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to Voice Over Internet (VoIP) protocols and architectures. More particularly, it relates to location based services for the provision of 911 emergency services using VoIP protocols and architectures.

2. Background of the Related Art

911 is a phone number widely recognized in North America as an emergency phone number that is used by emergency dispatch personnel, among other things, to determine a location of a caller. Enhanced 911 (E911) is defined by the transmission of callback number and location information. E911 may be implemented for landline and/or wireless devices.

A Public Safety Answering Point (PSAP) is a dispatch office that receives 9-1-1 calls from the public. A PSAP may be a local, fire or police department, an ambulance service or a regional office covering all services. A 9-1-1 ("911") service becomes E-9-1-1 ("E911") when automatic number identification and automatic location information from a communications device (e.g. wireless phone, VoIP Phone, etc.) is provided to the 911 operator.

Voice-Over-Internet Protocol (VoIP) is a technology that emulates a phone call, but instead of using a circuit based system such as the telephone network, utilizes packetized data transmission techniques most notably implemented in the Internet. 911 calls made using VoIP technology must reach the correct PSAP, but there currently is no uniform interface to the various PSAPs for call delivery because the technology for connecting calls varies. For instance, not all PSAPs are Internet Protocol (IP) capable. Some PSAPs are accessed via ordinary public switched telephone network (PSTN) telephone lines. Some PSAPs are accessed through selective routing such as direct trunks. Still other PSAPs are accessed using IP connections. There is no uniformity among the thousands of different PSAPs.

Moreover, some Public Safety Access Points (PSAPs) are not enhanced, and thus do not receive the callback or location information at all from any phone, landline or wireless.

The use of VoIP technology is growing quickly. As people adopt voice-over-IP (VoIP) technology for routine communications, the inventors herein recognize that there is a growing need to access E911 services including provision of location information from a VoIP device.

The existing E911 infrastructure is built upon copper wire line voice technology and is not fully compatible with VoIP. Given VoIP technology, there are at least three VoIP scenarios:

1. A VoIP UA that is physically connected to a static data cable at a "home" address. For instance, an Analog Telephone Adapter (ATA) that is connected to the "home" data cable and uses traditional telephone devices.
2. A VoIP UA that is physically connected to a data cable at a location different than its "home" address. For instance, a laptop computer device utilized away from home as a VoIP software telephone would be a VoIP 'visitor' device as described by this scenario.
3. A VoIP UA that is wireleless, physically disconnected from any data cable. In this situation, the VoIP UA connects to the VoIP service provider via

either a wide-are wireless technology (e.g., cellular, PCS, WiMAX) or via a local-area wireless technology (e.g., Wireless Fidelity (WiFi), UWB, etc.) using a laptop computer or handheld device.

VoIP phone calls are routed to a VoIP voice gateway, from which they are passed on to their destination. A VoIP voice gateway or soft switch is a programmable network switch that can process the signaling for all types of packet protocols. Also known as a 'media gateway controller,' 'call agent,' or 'call server, such devices are used by carriers that support converged communications services by integrating SS7 telephone signaling with packet networks. Softswitches can support, e.g., IP, DSL, ATM and frame relay.

The challenges evident with respect to determining the location of a calling VoIP telephone is perhaps most evident with respect to its use to make an emergency call (e.g., a 911 call). Nevertheless, VoIP telephone technology is quickly replacing conventional switched telephone technology. However, because VoIP is Internet Protocol (IP) based, call related information such as CallerID type services may not be available or accurate. A location of a given VoIP device may be provisioned to be at a given geographic location, or queried from a home location register (HLR) in a mobile system.

In addition, some Public Safety Access Points (PSAPs) are not enhanced, and thus do not receive the callback or location information at all from any phone; landline, cellular or VoIP.

Moreover, there is complexity in public access to Public Safety Answering Points due to lack of a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI) for all PSAPs. (SIP is the IP-based protocol defined in IETF RFCs 3261 and 2543.) SIP is one of two dominant protocols used by the VoIP industry. URI is the addressing technology for identifying resources on the Internet or a private intranet. URIs were originally defined as two types: Uniform Resource Locators (URLs) which are addresses with network location, and Uniform Resource Names (URNs) which are persistent names that are address independent. Today, a URI is defined by its purpose rather than the URL vs. URN classification.) Some PSAPs are accessed only by conventional telephone

line, others only by direct telephone trunk lines. Not all PSAPs are accessible via the Internet.

Fig. 5 shows basic conventional VoIP elements required to interconnect a VoIP emergency E911 caller to a relevant public safety access point (PSAP).

In particular, as shown in Fig. 5, VoIP telephone devices **102a, 102b, 102c** (collectively referred to as **102**) are connected to respective VoIP Service Provider (VSP) soft switches **104a, 104b, 104c** (collectively referred to as **104**) using an Internet Protocol (IP) connection, most commonly over the Internet. The VoIP service provider's soft switch **104** in turn communicates with a respective VoIP Positioning Center (VPC) **106a, 106b, 106c** (collectively referred to as **106**) using an appropriate IP connection. Each VSP requires use of their own VPC, as depicted in Fig. 5.

Fig. 6 shows in more detail conventional VoIP elements required by a VPC to interconnect a VoIP emergency E911 caller to a relevant public safety access point (PSAP).

In particular, as shown in Fig. 6, each VPC **106** comprises its own respective route determination module **404**, call delivery module **406**, and provisioning list **408**.

A respective location information server (LIS) **108** services each of the VPCs **106**. The LIS **108** is responsible for storing and providing access to the subscriber location information needed for E9-1-1 call processing (as defined by the NENA VoIP Location Working Group).

A conventional VoIP Positioning Center (VPC) **106** is a system that attempts to determine the appropriate or correct PSAP **114** that a VoIP emergency E911 call should be routed to based on the VoIP subscriber's position. The conventional VPC **106** also returns associated routing instructions to the VoIP network. The conventional VPC **106** additionally provides the caller's location and the callback number to the relevant PSAP through the automatic location identifier (ALI) (The ALI is a database that accepts a PSAP query, and using that relates a specific telephone number to a street address. In the case of

an Emergency Services Query Key (ESQK), the ALI database steers the query to the appropriate VPC and steers the response back to the PSAP. An ALI is typically owned by a LEC or a PSAP.)

Further as shown in Fig. 6, each VSP route the emergency 9-1-1 call, without location object added, to their VPC **106.** The VPC must determine the correct PSAP **114** (collectively represented by PSAP **114a**, **114b** and **114c**) and route to it using the appropriate technology.

In a first scenario, the VPC **106** passes the 9-1-1 call to the PSAP **114a** using an INVITE telephone number message, via a media gateway **110** that translates between the IP protocol of the INVITE message and a telephone line interface, and interfaces with the public switched telephone network (PSTN) **112.**

In a second scenario, the VPC **106** passes the 9-1-1 call to the PSAP **114b** using an INVITE S/R message, via an ESGW **120** and selective router **122.** In this scenario, the selective router **122** is connected to the relevant PSAP **114b** via direct trunks.

In a third scenario, the VPC **106** passes the 9-1-1 call to the PSAP **114c** using an INVITE PSAP message, via IP, to the PSAP **114c.**

In the second and third scenario, the ALI **126** must be inter-connected with each VPC **106** (a,b,c). Furthermore, each VPC is burdened with supporting all the various ALI protocols: ve2, e2, PAM, legacy NENA, etc.

Thus, as can be appreciated, an Emergency call (e.g., 911, E911) may require the involvement of one or more Response Centers (RCs), e.g., Public Safety Access Point (PSAP) in addition to the RC that initially receives the emergency call. This is because there is a possibility that the emergency call is received by a PSAP other than that which is assigned to the geographic region that the caller is currently located in.

Accordingly, the PSAP that initially answers the call may need to transfer the emergency call to the correct PSAP. During transfer of the emergency VoIP call, the original RC may or may not remain on the line, but for safety purposes will not likely want to disconnect or cold transfer the emergency

call. This is because errors may occur in the transfer, resulting in valuable time lost. One cause of a faulty transfer of the E911 call would be that the VoIP user has not updated the location stored by the VPC, or quite simply that bad routing has occurred. Another cause would be that the nature of the emergency requires multiple parties to be involved (e.g., fire/police, police/FBI, ambulance/CDC, etc.).

Conventional solutions are based on tools that can be used to find the phone numbers of other emergency response centers. The ERC receiving the call initially will perform a look-up for the correct response center, and may dial the identified correct response center, agency, etc., and transfer the call via direct dial/public switched telephone network (PSTN.

One exemplary conventional solution is called an Intelligent Emergency Network (IEN), available from Intrado Inc. of Longmont, Colorado. However, such conventional solutions typically require the emergency response center to know the direct dial lines of every PSAP, ESP, ERC, etc. nationally. Moreover, those lines may not always be staffed. Other potential problems would be caused if no automatic location identification (ALI) information is accessible or available.

There is a need for an architecture and methodology that both simplifies the complexity of a VoIP call transfers with respect to an emergency response center such as a public safety access point (PSAP).

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, a method of connecting an emergency caller with an emergency response center comprises establishing an emergency call conference. The emergency caller is added to the established emergency call conference, and the emergency response center is added to the emergency call conference. The emergency call is established after the emergency caller and the emergency response center are both added to the emergency call conference.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows an exemplary architecture of a VoIP emergency call conference bridge application operating in a VoIP soft switch of a VoIP provider to provide VoIP emergency call conferencing, in accordance with the principles of the present invention.

Fig. 2 shows an exemplary message flow diagram of VoIP location based 911 conferencing, in accordance with the principles of the present invention.

Fig. 3 shows an exemplary architecture of a VoIP conference bridge application operating in a VoIP soft switch of a VoIP provider to provide VoIP emergency call conferencing, in accordance with the principles of the present invention.

Fig. 4 shows an exemplary message flow diagram for establishing a VoIP location based conference, in accordance with the principles of the present invention.

Fig. 5 shows basic conventional VoIP elements required to interconnect a VoIP emergency E911 caller to a relevant public safety access point (PSAP).

Fig. 6 shows in more detail conventional VoIP elements required to interconnect a VoIP emergency E911 caller to a relevant public safety access point (PSAP).

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The present invention handles emergency calls through the use of a conference bridge on a VoIP service provider's soft switch. The soft switch works with a VoIP positioning center (VPC) to obtain location information, which may be gathered or confirmed by the initial recipient of the call, to ensure that appropriate participants to the emergency conference call are Invited to join the call. With the present invention in place, any number of emergency calls can be made, including any number of ERCs, PSAPs, ERPs, etc., (limited only by the number of conference bridges that can be established in provisioned equipment,

e.g., in the VoIP service provider's soft switch). Cold transfers can be avoided by Inviting participants to join a single emergency conference rather than passing an original call from party to party (e.g., from PSAP to police to ambulance, etc.) Moreover, the emergency call can survive as long as a participant remains in the emergency conference call, even after the original emergency caller hangs up.

Fig. 1 shows an exemplary architecture of a VoIP emergency call conference bridge application operating in a VoIP soft switch of a VoIP provider to provide VoIP emergency call conferencing, in accordance with the principles of the present invention.

In particular, as shown in Fig. 1, a user of a VoIP communications device **104** makes an emergency call (e.g., a 911 call). The VoIP service provider of the VoIP communications device **104** receives the 911 call, and assigns it to an available VoIP emergency conference call bridge **100**. The soft switch **102** obtains location information relating to the VoIP communications device **104**, either directly from the VoIP communications device **104** itself (e.g., if it includes a GPS device) or from a VoIP positioning center (VPC). The VoIP soft switch **102** compares the location information in a PSAP lookup database **800** to determine an initial PSAP for the service area responsible for the location of the VoIP communications device **104**. The PSAP lookup database provides an appropriate URL or other address information of the initial PSAP to the VoIP soft switch **102**, which in turn addresses an Invite message **804** (preferably including location information relating to the location of the VoIP communications device **104**). The PSAP **810**, in response, sends either an Accept message or a Reject message to the soft switch **102** in response to the Invite message **804**. Additional emergency services departments (e.g., police **812**, fire **814**, etc.) may be subsequently sent an Invite message to join the same VoIP emergency conference call.

Thus, the VoIP communication device **104** dials the appropriate emergency number (e.g., 911), and in response the VoIP service provider's soft switch **102** otherwise responsible for routing the user's calls instead establishes a

VoIP conference bridge **100** and places the incoming emergency call into the VoIP conference bridge **100**.

Although the initial emergency VoIP communication device **104** is a VoIP device, the soft switch **102** may additionally include interfaces to the Public Switched Telephone Network (PSTN) to permit non-VoIP emergency service provider's to join into the VoIP conference bridge.

Alternatively, instead of automatically placing the initial VoIP emergency caller **104** into the established VoIP conference bridge **100**, the VoIP soft switch **102** may instead Invite the initial VoIP emergency caller **104** to join the conference call via the VoIP conference bridge **100**. In response, the initial VoIP emergency caller **104** presumably accepts the Invite message and joins the VoIP conference bridge **100**.

At this point, the soft switch **102** may confirm location with the initial VoIP emergency caller **104** (if location information was provided with the initial call from the VoIP communication device **104**), or determines location from the subscriber's VPC, and captures the Location Object (LO).

The initial VoIP emergency caller **104** sends the LO and a 911 Invite message with an RC type (e.g., Fire Department, Homeland Security, etc.) to the soft switch **102** managing the VoIP conference bridge **100**.

The soft switch **102** sends the LO and Invite information to the VPC, which identifies the proper additional conference participant(s) (e.g., a PSAP, RC, first responder, other interested party, etc.) and corresponding contact information, and invites the proper participants to join the call.

The invited participant(s) can also invite other entities to join the VoIP emergency conference. While it is presumed that all participants in the VoIP emergency conference call may participate in the call, it is possible to include 'listen only' participants. For instance, a voice and/or data recording line may be invited to the VoIP emergency conference call to record any data and/or voice conversation.

Fig. 2 shows an exemplary message flow diagram of VoIP location based 911 conferencing, in accordance with the principles of the present invention.

In particular, as shown in Fig. 2, an emergency call **712** (e.g., 911) is placed from VoIP communications device **104.**

In response, the VoIP soft switch establishing the VoIP emergency conference call bridge transmits an emergency VoIP conference call Invite message (with or without a location object) **714** (or other location request) to the VoIP Positioning Center (VPC) **701**. Based on the location of the initiating VoIP emergency caller **104**, the VPC pass at least one Invite message using Internet Protocol (e.g., over the Internet) to interested third parties such as an initially contacted RC-1/PSAP **702**, PSAP-2 **703**, PSAP-n **704**, etc. The first emergency center contacted (RC-1/PSAP **702**) responds by verifying the location object and passing the same, along with the Invite RC Type, to the soft switch **718**.

As the emergency call progresses, other emergency responders may be brought into the VoIP emergency conference call. For instance, the soft switch that manages the VoIP conference call bridge **100** initiates an Invite message with location object to the VPC **701**, which in turn transmits an Invite message **722** to a subsequent emergency response center (e.g., PSAP-2 **703**). That subsequent emergency response center **703** responds by verifying/modifying the location object, and the Invite RC Type, as shown in message **724**.

The VoIP soft switch **102** may continue to invite additional emergency responders (or other parties) by passing an Invite message with location object through the VPC **701**, which passes an Invite with location object to the relevant other emergency responders **704.**

As an example to explain advantages of the present invention, the scenario is given where an emergency 9-1-1 call is routed to a PSAP based on a presumed or default location of the VoIP caller, but in fact it turns out that the PSAP that receives the VoIP call is not the correct entity to handle emergency calls from the particular location that the VoIP caller is currently at. Such errors

may occur, e.g., due to the user not updating the SLDB, bad routing, etc. In this scenario, the initial VoIP communications device dials 9-1-1, a conference line is initiated by the soft switch, an initially determined PSAP receives an Invite message to join the VoIP emergency conference bridge. The PSAP confirms/determines the user's location, and in the given scenario would determine that another PSAP is needed instead of or in addition to the PSAP on the line. In particular, the initial PSAP captures the Location Object (LO) and either rejects the Invite to join the VoIP emergency conference call (and is then removed from the conference bridge) or continues to participate in the VoIP emergency conference call (and so then stays on the conference bridge). Either way, a 911 emergency call Invite message is sent with the LO to the soft switch managing the VoIP emergency conference bridge. The VoIP soft switch sends the LO to the VPC, which then identifies the proper PSAP based on the LO and initiates an Invite message addressed over IP to the proper PSAP to join into the VoIP emergency conference call through the soft switch.

The VoIP conference bridge then joins the proper PSAP to the VoIP emergency conference call with the initial VoIP emergency caller (and with the initially contacted PSAP, if the initially contacted PSAP continues to participate in the call). In this manner, the initial VoIP emergency caller is kept on the line throughout the process, with preferably no additional manual action or key entry required from the initial emergency caller.

At the conclusion of the VoIP emergency call, the VoIP conference bridge is closed.

In cases where the initial routing of the VoIP emergency call was correct, the VoIP conference bridge would still be used, and the initial two parties would participate in the VoIP emergency conference call (e.g., the initial VoIP emergency caller and the initially Invited RC or PSAP). If no other parties are invited, additional queries to the VoIP Positioning Center (VPC) would not be necessary. If additional parties are invited, the soft switch would use location information and RC Type information from the initial RC or PSAP to determine the identity of other relevant RCs and/or PSAPs.

In general principle, Fig. 3 shows an exemplary architecture of a VoIP conference bridge application operating in a VoIP soft switch of a VoIP provider to provide VoIP call conferencing, in accordance with the principles of the present invention.

In particular, as shown in Fig. 3, a VoIP communications device **104** is serviced by their service provider's soft switch **102.** A positioning center **106** provides location data upon request from the soft switch **102**. Other VoIP users **110, 112, 114** etc. are potential members of any given conference.

Conference bridges **100** are implemented on the VoIP soft switch **102** located, e.g., at the VoIP service provider's VoIP network.

While the VoIP soft switch **102** is preferably capable of being provisioned with as many VoIP conference bridges **100** as are required in any particular application, only one conference bridge **100** is shown in Fig. 3 for simplicity of explanation.

Also, while the conference bridge **100** is shown implemented in the soft switch **102**, it can be embodied within another suitable network element having an Internet Protocol (IP) type connection (e.g., TCP/IP) with the initial user **104** as well as with the potential conferees **110, 112, 114**.

In accordance with the principles of the present invention, location information relating to the initial VoIP user **104** is passed to the VoIP conference bridge **100**, either from the user's VoIP communication device **104** or from their respective location server **106**. The location information is then compared by the VoIP soft switch **102** to find an initial desired PSAP.

The VoIP soft switch **102** makes use of the location information and other existing data or user input (e.g., existing preferences on file on the Soft Switch **102**, user entry through the keypad of the communications device **104**, or voice response). Based on the location and user input, the VoIP conference bridge **100** identifies the desired PSAP to be asked or Invited to join the conference currently established by the initial VoIP user **104** on the conference bridge **100**, and outputs an Invite or request message **204** to join that conference **100** to the specific URL(s), phone number(s) and/or other identifying address

information relating to VoIP communications equipment **110**, **112**, **114** of the relevant PSAP.

The soft switch **102** may also maintain the attributes and rules from other VoIP communication devices **110**, **112**, **114** etc. for receiving conference bridge calls, as well as the fixed location (e.g., a place of business) or the ability to query for a current location (e.g., for mobile communication devices such as mobile phones) for each device. Based on this information, with or without other user input (e.g., to select or prioritize among a list of available third parties), the soft switch **102** invites one or more other communication devices **110**, **112**, **114**, etc. to join the conference bridge. This creates a voice link between the first user **104** and the other third parties **110**, **112**, **114** without requiring the first user **104** to know the contact information or name of the third parties **110**, **112**, **114**.

Fig. 4 shows an exemplary message flow diagram for establishing a VoIP location based conference, in accordance with the principles of the present invention.

In particular, as shown in Fig. 4, the initial VoIP user **104** sends a request for conference bridge call to the soft switch **102**. Preferably the initial VoIP user **104** includes location information with the conference request call **201**. However, as depicted in Fig. 3, location information can be obtained from an appropriate positioning server **106** if not available from the initial VoIP user **104**.

Subsequent to the incoming conference call **201**, a suitable PSAP (and/or other emergency services, including a recorder line) is determined and invited with respective invite messages **204**, **206**.

In operation, the user's VoIP communication device **104** dials a pre-determined phone number (or URL) of the emergency service (e.g., 911) to initiate a VoIP emergency conference bridge **100** on the relevant VoIP soft switch **102**.

Fig. 3 shows use of a VoIP positioning center (VPC) **106**. The VoIP soft switch **102** may receive the user's location information either from each of the VoIP communication devices **104**, **110**, **112**, **114** etc., or from the VPC **106**.

The VoIP soft switch **102** preferably uses both the location information of the initiating VoIP user **104**, together with any profile criteria set for a given conference bridge **100**, to determine a suitable PSAP or other emergency services entity to be sent INVITE messages inviting them to join the established VoIP emergency conference bridge **100**.

The VoIP soft switch **102** invites one or more other VoIP communication devices **110**, **112**, **114**, (relating to emergency services) to join the VoIP emergency conference bridge **100**. This creates a voice link between the initiating VoIP user **104** that initially called into the VoIP emergency conference bridge **100**, and the other potential, third party conferees **110**, **112**, **114**, etc., without requiring the initiating VoIP user **104** to know the name or even the contact information of the other potential, third party emergency conferees **110**, **112**, **114**, etc.

Upon receipt of an invite to a VoIP conference bridge **204**, **206**, the potential other VoIP users **110**, **112**, **114**, etc. (PSAPs) are preferably notified similar to an incoming telephone call, e.g. with a ring signal, though it may be customized to be distinguished from the sound of an otherwise ordinary incoming phone call. For instance, a given unique phone tone may be activated upon receipt of an invite **204**, **206** to a conference bridge **100**.

In accordance with the principles of the present invention, the VoIP communication device(s) **110**, **112**, **114** receiving invitations to join a VoIP emergency call conference **100** may be provided with a filter that automatically rejects any/all invite requests not meeting their own specific criteria (e.g., the first invited participant to accept the Invite message) maintained on their VoIP devices **110**, **112**, **114** themselves, though such filtering may alternatively be performed at a network level, e.g., at the VoIP soft switch **102** or other centralized location.

Benefits of the invention include that there is no effective limit to the number of participants in the VoIP emergency conference call, there are no cold transfers of a call as VoIP invitees enter or leave the conference bridge **100**, and

there is the ability to continue the conference call even after the initial VoIP user **104** making the emergency call disconnects.

The present invention has particular applicability with any/all VoIP users, VoIP service providers, and Public Safety Access Points (PSAPs).

The invited VoIP users **110**, **112**, **114** may include a filter allowing through only acceptable Invite messages based on criteria established by or on the receiving VoIP communication devices **110**, **112**, **114**.

The present invention allows VoIP users to efficiently and quickly find and invite their most appropriate responder to their emergency, with minimal user interaction. This is particularly helpful for mobile VoIP users (e.g., while driving, walking, etc.) Moreover, there is no effective limit to the number of participants in the conference call (within network hardware limits of the conference bridge itself). There is also no risk of cold transfers of a VoIP telephone call as participants aren't handled in point-to-point connections that are transferred but rather join or exit an established conference at will. Furthermore, emergency personnel from various departments and locations in the conference call can continue in the conference even after the initial emergency caller disconnects.

Potential markets for the present invention include VoIP service providers who may implement the inventive VoIP emergency conference calling as a value added services for users. VoIP location based conferencing in accordance with the principles of the present invention has particular applicability with any/all VoIP users, VoIP service providers, and Public Safety Access Points (PSAPs).

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to make various modifications to the described embodiments of the invention without departing from the true spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method of connecting an emergency caller with an emergency response center, comprising:

establishing an emergency call conference;

adding said emergency caller to said established emergency call conference; and

adding said emergency response center to said emergency call conference;

wherein said emergency call is established after said emergency caller and said emergency response center are both added to said emergency call conference.

2. The method of connecting an emergency caller with an emergency response center according to claim 1, further comprising:

adding a third party to said emergency call conference;

3. The method of connecting an emergency caller with an emergency response center according to claim 1, wherein:

at least three parties are present in said emergency call conference at least at a beginning of said emergency call.

4. The method of connecting an emergency caller with an emergency response center according to claim 1, wherein said emergency response center comprises:

a public safety access point (PSAP).

5. The method of connecting an emergency caller with an emergency response center according to claim 2, wherein said third party comprises:

a police dispatcher.

6. The method of connecting an emergency caller with an emergency response center according to claim 2, wherein said third party comprises:

a fire department.

7. The method of connecting an emergency caller with an emergency response center according to claim 2, wherein said third party comprises:

an ambulance company.

8. The method of connecting an emergency caller with an emergency response center according to claim 1, wherein:

said emergency caller is added to said emergency call conference after said emergency response center is added to said emergency call conference.

9. The method of connecting an emergency caller with an emergency response center according to claim 1, wherein:

said emergency response center is added to said emergency call conference after said emergency caller is added to said emergency call conference.

10. Apparatus for connecting an emergency caller with an emergency response center, comprising:

means for establishing an emergency call conference;

means for adding said emergency caller to said established emergency call conference; and

means for adding said emergency response center to said emergency call conference;

wherein said emergency call is established after said emergency caller and said emergency response center are both added to said emergency call conference.

11. Apparatus for connecting an emergency caller with an emergency response center according to claim 10, further comprising:

means for adding a third party to said emergency call conference;

12. The apparatus for connecting an emergency caller with an emergency response center according to claim 10, wherein:

at least three parties are present in said emergency call conference at least at a beginning of said emergency call.

13. The apparatus for connecting an emergency caller with an emergency response center according to claim 10, wherein said emergency response center comprises:

a public safety access point (PSAP).

14. The apparatus for connecting an emergency caller with an emergency response center according to claim 11, wherein said third party comprises:

a police dispatcher.

15. The apparatus for connecting an emergency caller with an emergency response center according to claim 11, wherein said third party comprises:

a fire department.

16. The apparatus for connecting an emergency caller with an emergency response center according to claim 11, wherein said third party comprises:

an ambulance company.

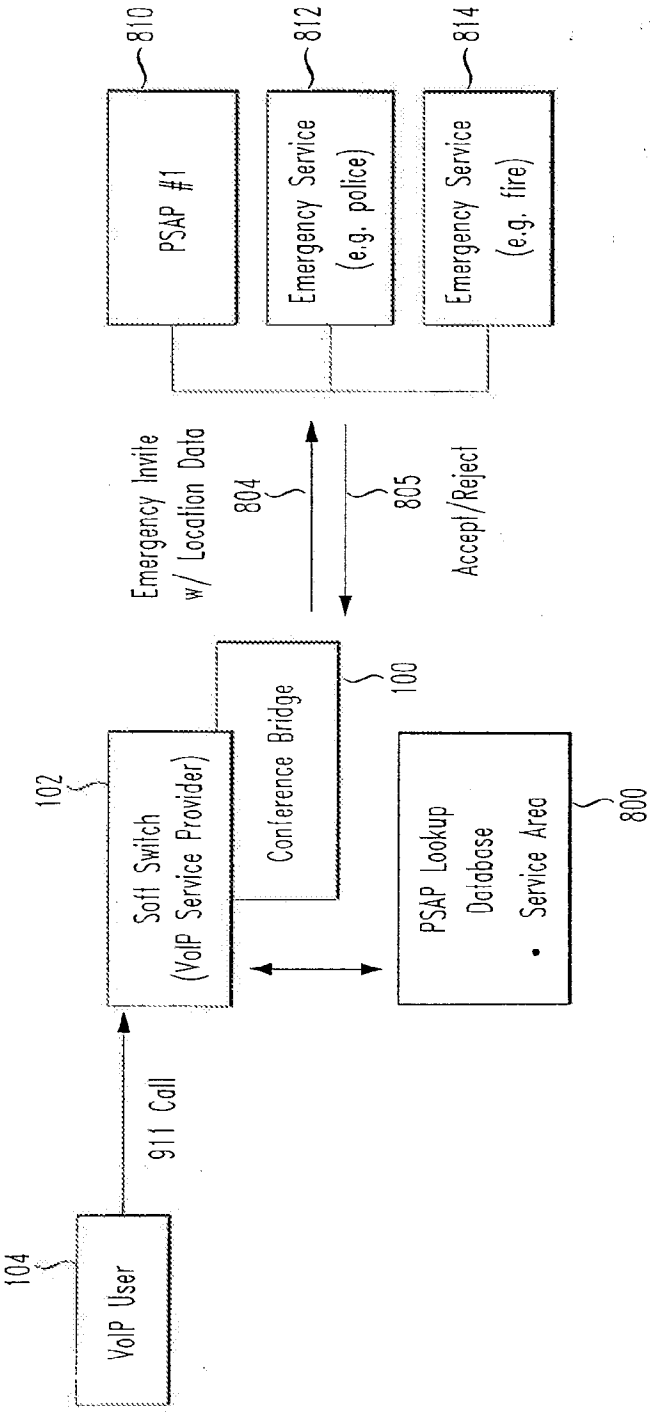
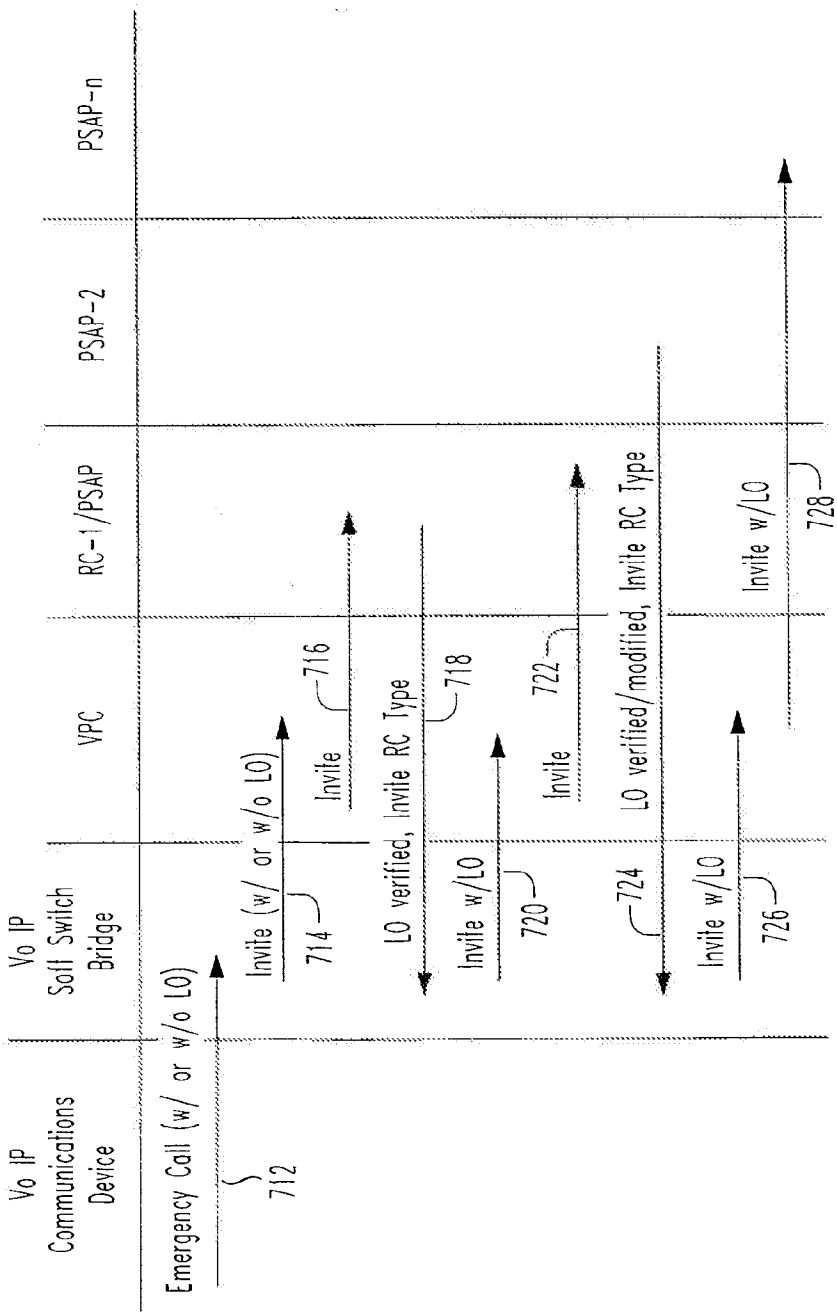

810
PSAP #1
812
Emergency Service
(e.g. police)
814
Emergency Service
(e.g. fire)
Emergency Invite
w/ Location Data
804
805
Accept/Reject
100
Conference Bridge
102
Soft Switch
(VoIP Service Provider)
PSAP Lookup
Database
• Service Area
800
911 Call
104
VoIP User

FIG. 1

FIG. 2


104
Vo IP Communications Device
102
Vo IP Soft Switch Bridge
701
VPC
702
RC-1/PSAP
703
PSAP-2
704
PSAP-n
Emergency Call (w/ or w/o LO)
712
Invite (w/ or w/o LO)
714
Invite
716
LO verified, Invite RC Type
718
Invite w/LO
720
Invite
722
LO verified/modified, Invite RC Type
724
Invite w/LO
726
Invite w/LO
728

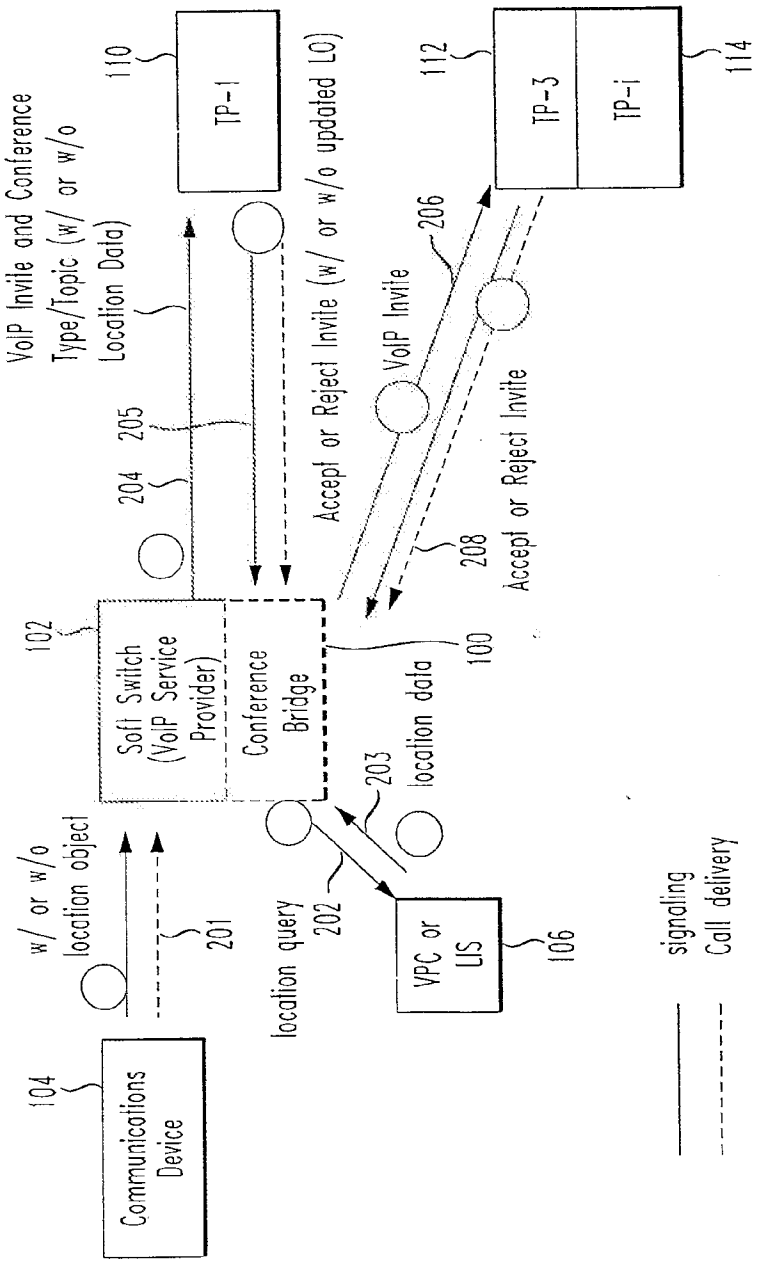

Communications Device
104
w/ or w/o location object
201
Softi Switch (VoIP Service Provider)
102
Conference Bridge
100
location query
202
203
location data
VPC or LIS
106
VoIP Invite and Conference Type/Topic (w/ or w/o Location Data)
204
205
110
TP-1
Accept or Reject Invite (w/ or w/o updated LO)
VoIP Invite
206
112
TP-3
TP-i
114
208
Accept or Reject Invite
signaling
Call delivery

FIG. 3

FIG. 4

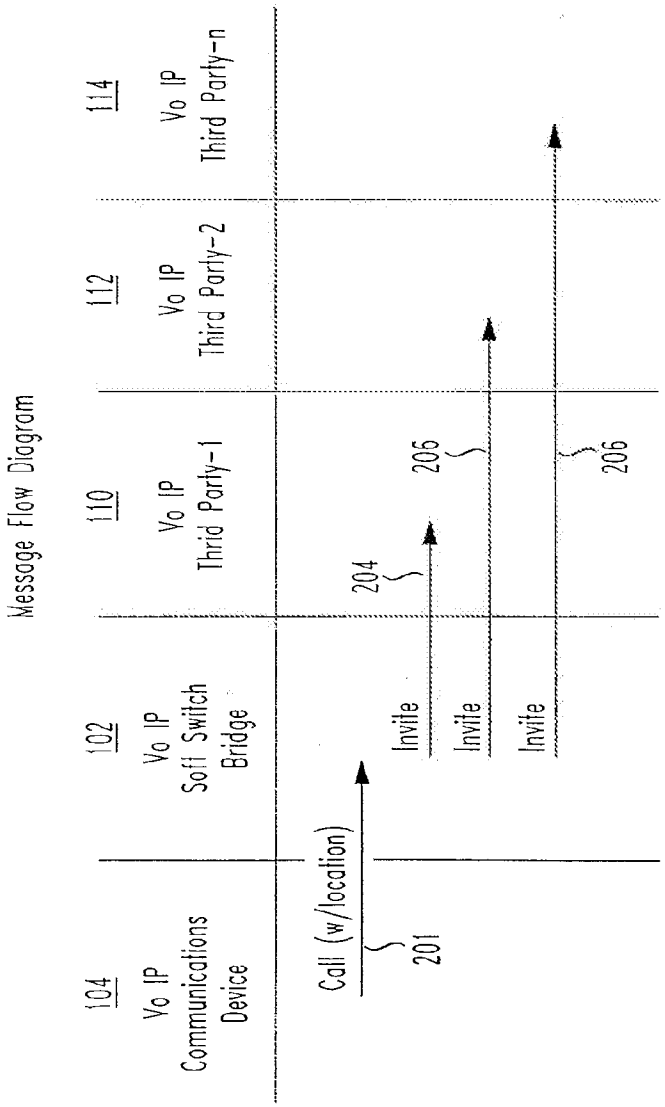
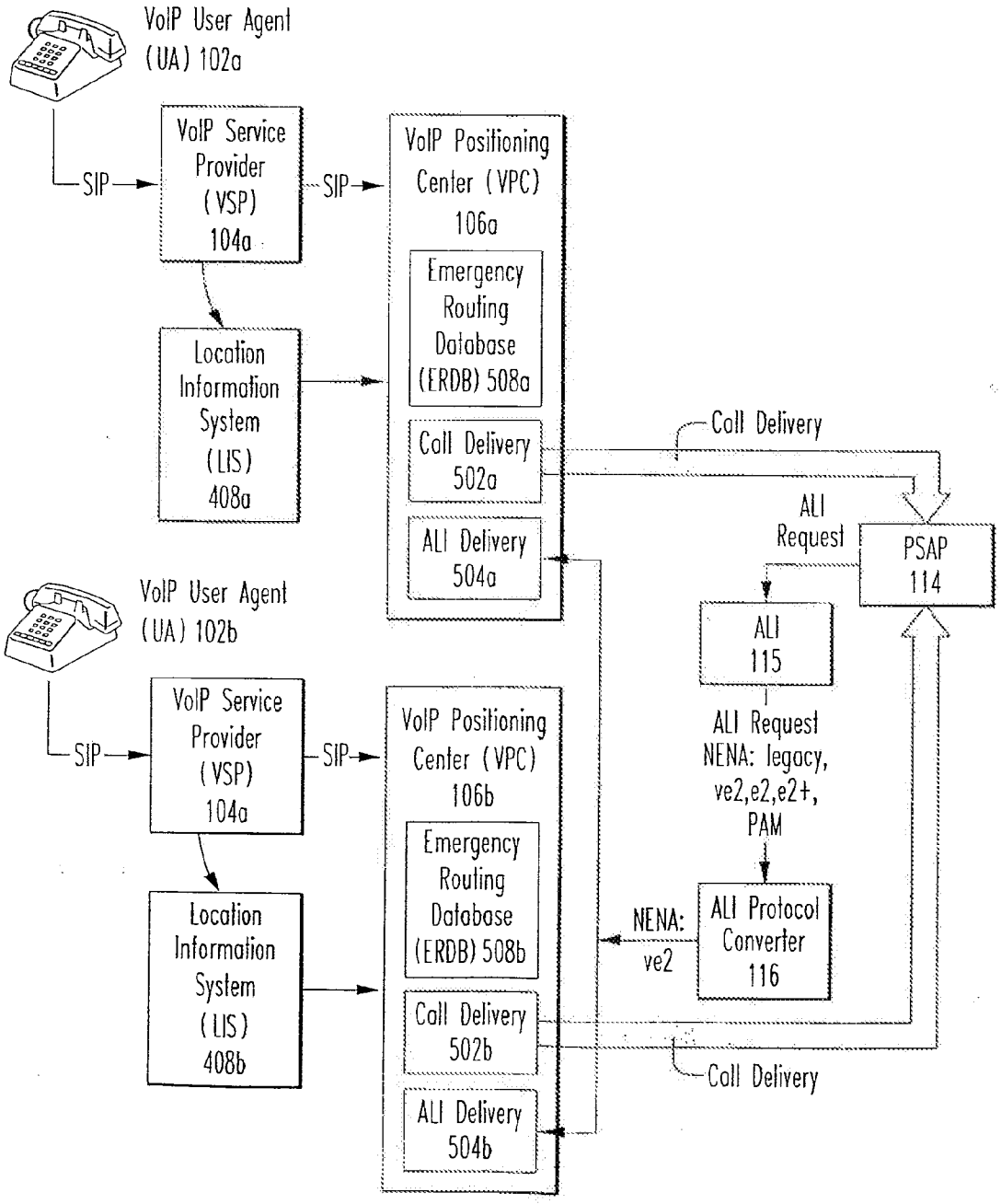

Message Flow Diagram
104
Vo IP
Communications
Device
102
Vo IP
Soft Switch
Bridge
110
Vo IP
Third Party-1
112
Vo IP
Third Party-2
114
Vo IP
Third Party-n
Call (w/location)
201
Invite
Invite
Invite
204
206
206

FIG. 5
(PRIOR ART)



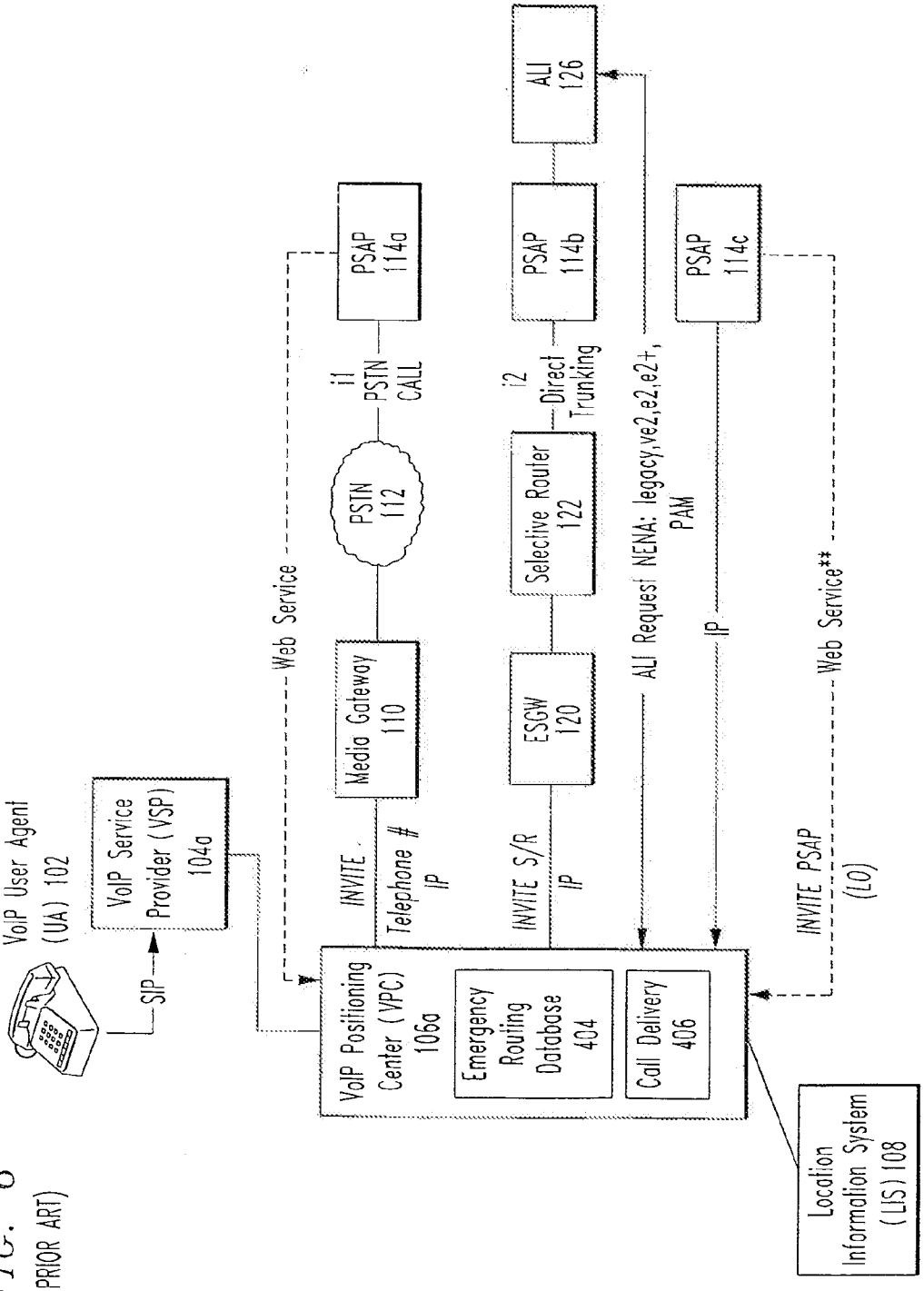


FIG. 6
(PRIOR ART)

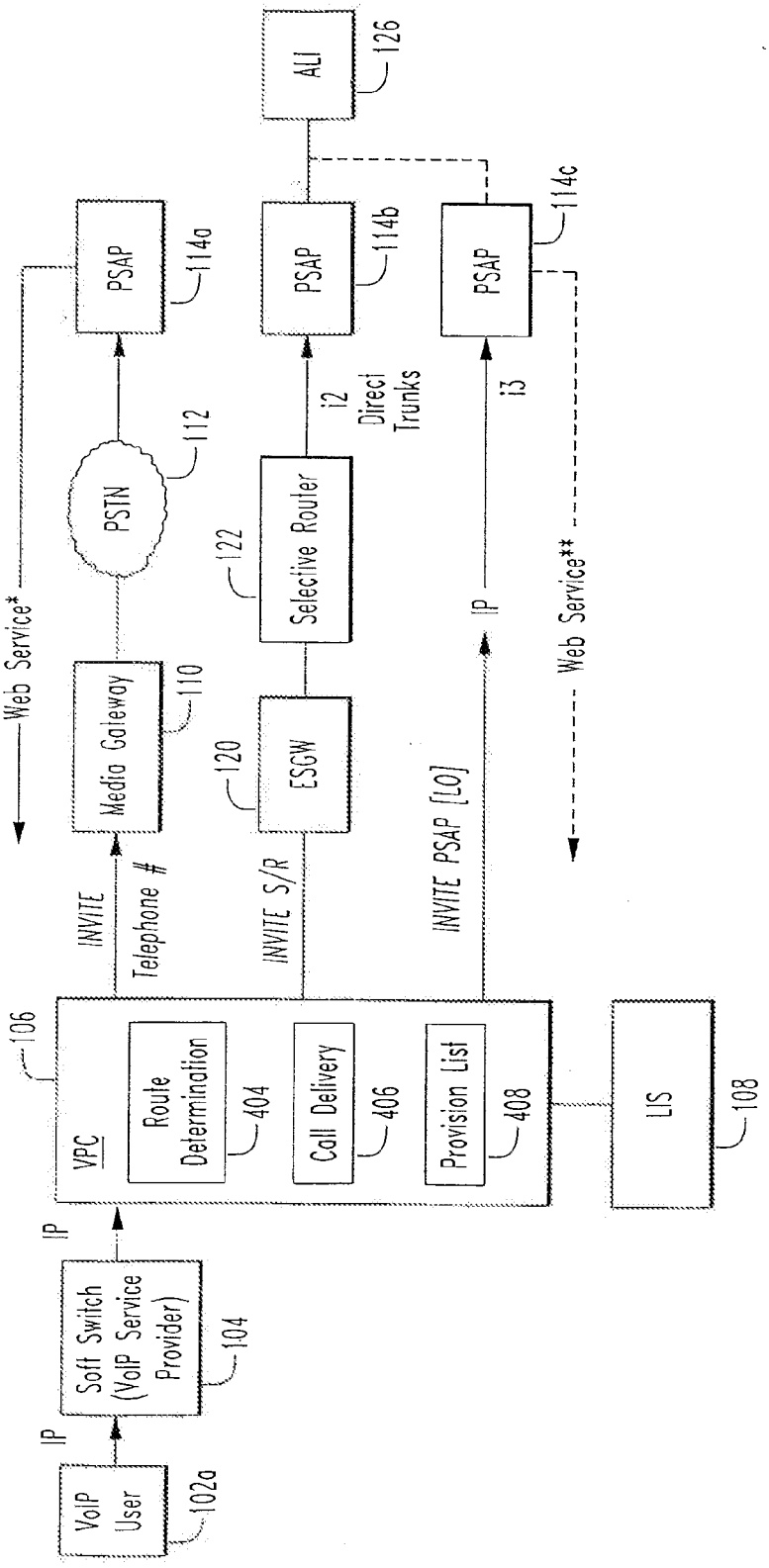


FIG. 7
(PRIOR ART)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 August 2007 (02.08.2007)

PCT

(10) International Publication Number
WO 2007/087077 A2

(51) International Patent Classification:
H04Q 7/20 (2006.01)

(21) International Application Number:
PCT/US2006/049603

(22) International Filing Date:
28 December 2006 (28.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/759,524 17 January 2006 (17.01.2006) US

(71) Applicant *(for all designated States except US)*: **MEDICAL ENVELOPE L.L.C.** [US/US]; 1555 Riviera Avenue, Apt. 306, Walnut Creek, CA 94596 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PATEL, Subodh, M.** [US/US]; 1555 Riviera Avenue, Apt. 306, Walnut Creek, CA 94596 (US). **BROOKS, Antoine, P.** [US/US]; 1240 Saratoga Avenue, Palo Alto, CA 94303 (US).

(74) Agents: **ALBERT, Peter, G., Jr.** et al.; Foley & Lardner LLP, 11250 El Camino Real, Suite 200, San Diego, CA 92130 (US).

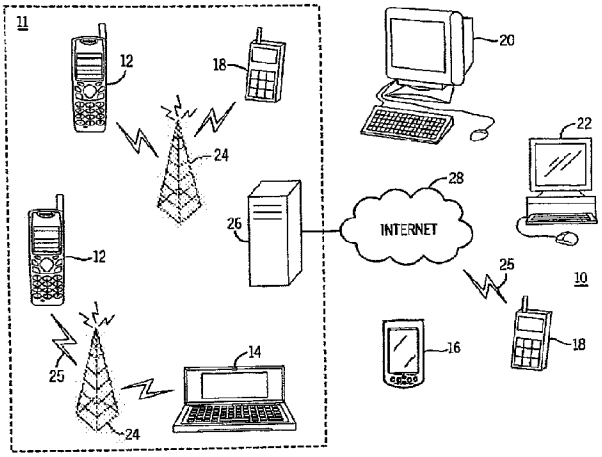
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, 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, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

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

(54) Title: SYSTEM AND METHOD FOR PROVIDING MEDICAL AND CONTACT INFORMATION DURING AN EMERGENCY CALL



(57) Abstract: A system and method for providing medical and contact information of a subscriber initiating an emergency 911 call, directly to a response center at the time of the receipt of the emergency 911 call. Upon the initiation of an emergency 911 call, the existing infrastructure equipment of a communication service provider are able to access a central server containing the medical and contact information of a subscriber, and relay that information directly to a response center to speed response time and response effectiveness. Alternatively, an agent resident on a communications device used by a subscriber can store and maintain medical and contact information of the subscriber, as well directly transmit the medical and contact information to the response center. In addition, a subscriber has the ability to access, view, and modify his or her medical and contact information through an appropriate interface allowing interaction with either the central server or the agent.

WO 2007/087077 A2

SYSTEM AND METHOD FOR PROVIDING MEDICAL AND CONTACT INFORMATION DURING AN EMERGENCY CALL

FIELD OF THE INVENTION

[0001] The present invention relates generally to the field of emergency communications. More specifically, the present invention relates to a communication network and associated method for quickly and easily storing and retrieving information related to the subject of an emergency communication.

BACKGROUND OF THE INVENTION

[0002] This section is intended to provide a background or context to the invention that is recited in the claims. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and claims in this application and is not admitted to be prior art by inclusion in this section.

[0003] Emergency notification systems have been in use for many years, routing emergency calls to proper response authorities such as the local police, fire department, ambulance service, etc., where dialing 9-1-1 denotes that a call is an emergency call. In approximately over 93% of locations in the United States and Canada, dialing 9-1-1 from any telephone will connect a caller to an emergency dispatch center called a Public Safety Answering Point (PSAP), which can send emergency response personnel to the caller's location in an emergency. Figure 4 shows a typical communications network in which basic 911 service is implemented. A user makes a 911 call using telephone 400 indicating that the user is in some sort of distress. The call is routed to a local exchange carrier (LEC) switch 405 and forwarded to a 911 tandem switch 410. Upon receipt of the 911 call, the 911 tandem switch 410 routes the 911 call to one of a plurality of PSAPs 415a, 415b, or 415c. Alternatively, the LEC switch 405 can route the 911 call directly to one of the PSAPs 415a, 415b, 415c. It should be noted that a PSAP is a designation used to describe a

location where the 911 call is terminated, answered, processed, and the nature of the distress or emergency is determined and assessed. An automatic call distributor (ACD), a call center, or a private branch exchange (PBX) switch can function as a PSAP, or PSAP equipment can include an ACD, call center, or PBX switch . An operator (not shown) of PSAP 415b processes the 911 call and forwards it to an appropriate response center or agency, e.g., an ambulance service 420, a local fire department 425, or a local police department 430.

[0004] In some areas, enhanced 911 (e911) is available, which automatically gives the PSAP the caller's location, if available. Figure 5 is an example of a communications network in which e911 service is implemented. The network operates as described with reference to Figure 4. However, instead of only voice data being sent from telephone 400, Automatic Number Identification (ANI) information is also sent through the communication network. Originally, ANI information was utilized to assist a telephony company in accessing toll charges for long distance calls. Advances in technology, however, allowed ANI information to be used in relaying needed information to a PSAP for 911 response as well. Therefore, upon receipt of a 911 call at the 911 tandem switch 410, the ANI information associated with telephone 400 is read, thereby allowing 911 tandem switch 410 to send the callback number of telephone 400 to the display of a workstation at the appropriate PSAP 415a, 415b, or 415c. With this callback number information, the appropriate PSAP is able to access a 911/Automatic Location Identifier (ALI) database 540 and retrieve the caller's physical address or ALI.

[0005] However, when 911 calls are made from mobile telephones, the call may not be routed to the closest PSAP, and the call taker does not receive a callback phone number or the location of the caller. This presents life threatening problems due to lost response time if callers are unable to speak or don't know where they are, or if they don't know their mobile telephone callback number and the call is dropped. The National Emergency Number Association (NENA) is an organization that was created to foster technological advancements, availability, and implementation of a universal emergency telephone number system. To address the problems present in wireless 911, a three phase plan was enacted.

[0006] The most basic of these phases, sometimes called Wireless Phase 0, simply provides that when a caller dials 9-1-1 from a wireless telephone, an operator at a PSAP answers. The operator may be at a state highway patrol PSAP, at a city or county PSAP up to hundreds of miles away, or at a local PSAP, depending on how the wireless 911 call is routed.

[0007] Wireless Phase I is the first step in providing better emergency response service to wireless 911 callers. When Wireless Phase I has been implemented, a wireless 911 call will come into a PSAP with the mobile telephone callback number. This is important in the event the call is dropped, and may even allow PSAP operators to work with a wireless company to identify the wireless subscriber. However, Wireless Phase I still does not help call takers locate emergency victims or callers.

[0008] To locate wireless 911 callers, Wireless Phase II must be implemented in an area by local 911 systems and wireless carriers. Wireless Phase II will allow operators to receive both the caller's mobile telephone number and their location information. This is accomplished by requiring new mobile telephones to provide their latitude and longitude to PSAP emergency response operators in the event of a 911 call. Carriers may choose whether to implement this via GPS chips in each phone, or via triangulation between cell towers. In addition, Wireless Phase II requires carriers to connect 911 calls from any mobile telephone, regardless of whether that phone is currently active. Due to limitations in technology (of the mobile telephone, cell towers, and PSAP equipment), a mobile callers' geographical information may not always be available to the local PSAP.

[0009] The networks described above, however, remain very limited in functionality. For example, medical information relating to a caller must still be gleaned by a PSAP operator conversing with the caller. If the caller has become incapacitated or is otherwise unable to speak, the PSAP operator has no way of knowing how best to aid the caller. It is left to emergency response personnel to determine this and act upon arriving at the caller's location. Therefore, it would be helpful to know any pertinent medical information beforehand. It would also be helpful to inform interested parties, such as parents of a child, if the child has initiated a 911 call. There have been attempts to provide medical history information to PSAP

operators and systems have been developed to notify third parties of 911 calls. However, these systems and methods require additional infrastructure equipment that are not easy to integrate into existing communication networks. Moreover, these systems and methods still require extra steps of a PSAP operator and extra time, for example, manually accessing and retrieving medical data regarding a 911 caller.

SUMMARY OF THE INVENTION

[0010] Various embodiments of the present invention comprise a system and method for providing medical and contact information associated with a subscriber, to response personnel, such as PSAP operators, local fire and police departments, and the like. This information can include, but is not limited to a subscriber's name, blood type, date of birth, language(s) spoken, and emergency contact(s). When a subscriber initiates an emergency 911 call, an agent in the telephone sends an identifier through the communication network to a central server. The identifier allows the subscriber's associated medical and contact information to be retrieved from the central server, after which the information is relayed to response personnel. In addition, a message can be sent to any contact(s) retrieved in the subscriber's associated medical and contact information at substantially the same time the 911 call is initiated, alerting that contact(s) that a 911 call has been made.

[0011] Various embodiments of the present invention allow for better and easier implementation of emergency 911 services. PSAP operators can receive all the necessary information for aiding a subscriber in an emergency immediately without having to manually access outside data sources. Existing service providers do not have to invest in additional infrastructure, nor do service providers have to modify their respective system architectures. Moreover, allowing subscriber's to create and manage their own medical and contact information promotes consumer-driven healthcare objectives, as well as ensures that the most up-to-date information regarding a subscriber is transmitted to response personnel, should the subscriber find him or herself in need of emergency attention. Additionally, interested third parties or contacts can immediately be notified if a 911 call is initiated.

[0012] These and other advantages and features of the invention, together with the organization and manner of operation thereof, will become apparent from the following detailed description when taken in conjunction with the accompanying drawings, wherein like elements have like numerals throughout the several drawings described below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Figure 1 is an overview diagram of a system within which the present invention may be implemented;

[0014] Figure 2 is a perspective view of a mobile telephone that can be used with the implementation of the present invention;

[0015] Figure 3 is a schematic representation of the telephone circuitry of the mobile telephone of Figure 2;

[0016] Figure 4 is an overview diagram representing the communications between emergency 911 network elements in a basic emergency 911 network;

[0017] Figure 5 is an overview diagram representing the communications between emergency 911 network elements in an enhanced emergency 911 network;

[0018] Figure 6 is an overview diagram representing the communications between emergency 911 network elements in a wireless emergency 911 network;

[0019] Figure 7 is an overview diagram representing the communications between emergency 911 network elements in one embodiment of the present invention;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Figure 1 shows a system 10 in which the present invention can be implemented and utilized, comprising multiple communication devices that can communicate through a network. The system 10 may comprise any combination of wired or wireless networks including, but not limited to, a mobile telephone network, a wireless Local Area Network (LAN), a Bluetooth personal area network, an Ethernet LAN, a token ring LAN, a wide area network, the Internet, i.e., voice over Internet Protocol (VOIP), etc. The system 10 may include both wired and wireless communication devices.

[0021] For exemplification, the system 10 shown in FIG. 1 includes a mobile telephone network 11 and the Internet 28. Connectivity to the Internet 28 may include, but is not limited to, long range wireless connections, short range wireless connections, and various wired connections including, but not limited to, telephone lines, cable lines, power lines, and the like.

[0022] The exemplary communication devices of the system 10 may include, but are not limited to, a mobile telephone 12, a combination PDA and mobile telephone 14, a PDA 16, an integrated messaging device (IMD) 18, a desktop computer 20, and a notebook computer 22. The communication devices may be stationary or mobile as when carried by an individual who is moving. The communication devices may also be located in a mode of transportation including, but not limited to, an automobile, a truck, a taxi, a bus, a boat, an airplane, a bicycle, a motorcycle, etc. Some or all of the communication devices may send and receive calls and messages and communicate with service providers through a wireless connection 25 to a base station 24. The base station 24 may be connected to a network server 26 that allows communication between the mobile telephone network 11 and the Internet 28. The system 10 may include additional communication devices and communication devices of different types.

[0023] The communication devices may communicate using various transmission technologies including, but not limited to, Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), Transmission Control Protocol/Internet Protocol (TCP/IP), Short Messaging Service (SMS), Multimedia Messaging Service (MMS), e-mail, Instant Messaging Service (IMS), Bluetooth, IEEE 802.11, etc. A communication device may communicate using various media including, but not limited to, radio, infrared, laser, cable connection, and the like.

[0024] Figures 2 and 3 show one representative mobile telephone 12 within which the present invention may be implemented. It should be understood, however, that the present invention is not intended to be limited to one particular type of mobile telephone 12 or other electronic device. The mobile telephone 12 of Figures 2 and 3

includes a housing 30, a display 32 in the form of a liquid crystal display, a keypad 34, a microphone 36, an ear-piece 38, a battery 40, an infrared port 42, an antenna 44, a smart card 46 in the form of a UICC according to one embodiment of the invention, a card reader 48, radio interface circuitry 52, codec circuitry 54, a controller 56 and a memory 58. Individual circuits and elements are all of a type well known in the art.

[0025] A typical wireless emergency 911 network is shown in Figure 6. A caller using mobile telephone 600 initiates a wireless 911 call. The nearest serving cell tower 610 picks up the wireless 911 call and relays it to a mobile switching center (MSC) 620. The MSC 620 operates much like a landline LEC switch and forwards the wireless 911 call to 911 tandem switch 410. It should be noted that the MSC 620 is usually a part of or operated by one of a plurality of local wireless service providers. The wireless 911 call is then received at the PSAP 415b, along with wireless ANI data that indicates the wireless telephone callback number of mobile telephone 600. In addition, there are known methods of sending additional ANI-related data with the wireless 911 call, such as information regarding the cell face of the cell tower 610 that received the wireless 911 call, or the cell tower 610 itself. This information can be used to approximate within several hundred square meters, where the wireless 911 call was made from.

[0026] As mentioned above, Wireless Phase II promulgated by NENA requires the determination of the location of mobile telephones making 911 calls. One method of accomplishing this is through base station or cell tower triangulation. Each base station or cell tower, for example, cell tower 610, measures the amount of time it takes to receive a mobile telephone's signal when it makes a wireless 911 call. This time data is translated into the distance data, estimating how far the mobile telephone is from the base station or cell tower. This distance data is then cross-referenced with distance data from at least one other base station or cell tower that received the mobile telephone's signal to arrive at longitudinal and latitudinal coordinates for that mobile telephone. Alternatively, the mobile telephone itself can triangulate its location by cross-referencing time-synchronized signals sent from multiple base stations or cell towers. The angle at which a mobile telephone's signal arrives at a base station or cell tower can also be determined using antenna arrays. This angle data can also be

cross-referenced with angle data from other base stations or cell towers, and the mobile telephone's location can be triangulated. In addition, many mobile devices are now equipped with global positioning system (GPS) receivers that can receive GPS signals from GPS satellites to determine location.

[0027] Figure 7 shows one embodiment of the present invention for providing medical and contact information services to subscribers. The elements of the wireless emergency 911 network of Figure 6 are utilized in the system architecture of the present invention, with the exception of the 911 tandem switch 410. Replacing the 911 tandem switch 410 is a central server 700. The central server 700 implements and manages all application modules for effecting the medical information service. It should be noted that such an implementation of the present invention requires no infrastructure investment from service providers. Existing wireless networks and service providers, e.g., Verizon, Cingular, T-Mobile, Sprint/Nextel, USCellular, etc. need only install an agent on mobile telephones operating on their respective networks. The agent can be optimized for each service provider or can be coded as a universal application or module, capable of being utilized on any service provider equipment.

[0028] The agent for the mobile telephones can be added after being locked to a specific carrier by that service provider, or can be installed by the mobile telephone manufacturer, e.g., Nokia Corporation. Furthermore, the agent can be implemented directly in the mobile telephone itself or on a SIM card/microchip that can be removably installed/inserted into the mobile telephone. The agent is responsible for detecting dual tone multifrequency (DTMF) signals or a dedicated telephone keypad button/softkey representing 9-1-1. If logic in the mobile telephone is not present, the agent can also detect and distinguish between the actual dialing of a 911 call and when the digits 9-1-1 are merely a part of another telephone number or key-pressing sequence. The agent can even be coded to allow a 911 caller to input a unique identifier to identify him or herself in the event he/she must initiate a 911 call from a telephone other than their own, or if a person is initiating the 911 call on behalf of the person in distress. Additionally, a cancellation function can be provided by the agent to prevent false 911 calls from being routed.

[0029] Coding the agent can be done using, but not limited to, the Binary Runtime Environment for Wireless (BREW) platform, which is an air-interface independent platform originally used for downloading and running small mobile applications, Java Platform, Micro Edition (J2ME), a collection of Java application programming interfaces (APIs), or another OEM software platform.

[0030] In the one embodiment of the present invention, the central server 700 stores and maintains important medical and contact information for subscribers, including, but not limited to, a subscriber's name, date of birth, language(s) spoken, emergency contact(s), blood type, medications, allergies, weight, eye color, driver's license number, living will information, and organ donor information. The medical information services provided by the various embodiments of the present invention can be divided into subscription levels or packages, where all or some subset of the above medical information is stored and maintained for a subscriber. For example, a basic medical information services package can include storing and maintaining a subscriber's name, date of birth, language(s) spoken, emergency contact(s), and blood type. A premium medical information services package can include that information found in the basic service, plus the subscriber's medications, allergies, weight, eye color, driver's license number, living will information, and organ donor information.

[0031] In order to store and maintain subscribers' medical and contact information, a management console is provided through which a subscriber can create an emergency health profile. The management console can be a Web-based application/administration tool accessible to subscribers over the Internet or other data network. A subscriber logs onto a website and enters the appropriate medical and contact information into a webpage, after which, the information is loaded into and stored in the central server 700. Alternatively, the website or some other type of user interface, such as an interactive voice recognition (IVR) interface or a simple human operator interface can provide direct access to the central server 700. After creating an emergency health profile, a subscriber can revisit the profile and update or make changes to the information stored therein at his or her discretion. This can be performed using the website or using the subscriber's mobile telephone via the agent resident thereon. This allows a subscriber's relevant medical and contact information

to be as up-to-date as possible. Additionally, having personal access to one's medical information promotes consumer-driven healthcare and makes accessing one's medical information an easy task. Third parties, such as insurance companies and hospitals can also be given the authority to access and view or update a subscriber's medical and contact information, or even link their own databases and servers with the central server 700.

[0032] When a subscriber initiates a 911 call on his or her mobile telephone 600, the 911 call is routed through the cell tower 610, the MSC 620, and to the central server 700. A service set identifier (SSID), or other identifier capable of identifying the subscriber or the mobile telephone 600, is also sent from the mobile telephone 600 at the same time the 911 call is initiated. Once the subscriber and/or mobile telephone 600 is authenticated using the SSID or other identifier, the central server 700 retrieves the emergency health profile of the calling subscriber. The central server 700 substantially simultaneously instructs the service provider that is operating MSC 620 to send a short message service (SMS) message containing the emergency health profile of the calling subscriber to PSAP 415b, and to send an SMS, text, email, voice, or other type of message(s) to alert any contact(s) stored in the subscriber's emergency health profile to the fact that a 911 call was initiated.

[0033] It should be noted that prior to routing the 911 call to the PSAP 415b, the methods discussed above regarding how to determine a mobile telephone's location can be used to choose the nearest PSAP. Alternatively, the agent discussed above, can be further adapted to determine the PSAP nearest to the mobile telephone 600, to which the 911 call should be routed. Geographic areas can be divided into any one of a number of regions, based on various criteria. For example, a specified area of coverage for a PSAP may include an area within the borders of a town or county, whereas in an urban area, the specified area of coverage may be comprised of a predetermined number of blocks. This process of gleaning the relevant medical and contact information before the 911 call reaches a PSAP allows a PSAP operator to have all the necessary information to aid and direct emergency response personnel to the subscriber. In addition, the infrastructure and messaging functionality of existing

service providers is better, and more efficiently utilized than in past emergency 911 call systems and architectures.

[0034] In another embodiment of the present invention, the agent or the mobile telephone itself can be coded with a subscriber's medical and contact information, bypassing the need to access the control server 700 during the processing of a 911 call. The medical and contact information can be encrypted and password protected as well. This further speeds the process of responding to the 911 call. Additionally, a subscriber can travel anywhere in the world and have access to his or her medical and contact information via his or her mobile telephone. In yet another embodiment of the present invention, the control server 700 as well as routing the emergency 911 call through the MSC 620 or other conventional service provider equipment can be bypassed. This is possible with networks that utilize advanced cell towers that have call routing functionality.

[0035] It should be noted that although embodiments of the present invention discussed above are implemented in wireless emergency 911 networks, the present invention is also easily adaptable to landline emergency 911 networks. In addition, various embodiments of the present invention can be utilized on basic as well as e911 networks. The agent can also be installed in other mobile devices, as well as personal computers and voice over IP-based devices, allowing the same functionality discussed above to provided to non-mobile telephone subscribers. In fact, information other than or in addition to medical and contact information can be stored, maintained, and accessed for purposes such as Homeland Security.

[0036] The present invention is described in the general context of method steps, which may be implemented in one embodiment by a program product including computer-executable instructions, such as program code, executed by computers in networked environments. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable

instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps.

[0037] Software and web implementations of the present invention could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various database searching steps, correlation steps, comparison steps and decision steps. It should also be noted that the words "component" and "module," as used herein and in the claims, is intended to encompass implementations using one or more lines of software code, and/or hardware implementations, and/or equipment for receiving manual inputs.

[0038] The foregoing description of embodiments of the present invention have been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the present invention to the precise form disclosed, and modifications and variations are possible in light of the above teachings or may be acquired from practice of the present invention. The embodiments were chosen and described in order to explain the principles of the present invention and its practical application to enable one skilled in the art to utilize the present invention in various embodiments and with various modifications as are suited to the particular use contemplated.

WHAT IS CLAIMED IS:

1. A method for providing subscriber information to a response center upon initiation of a call from a communication device operating on a communication network comprising:

receiving an identifier identifying the communication device;

forwarding the identifier to a switch;

receiving the subscriber information from a central server communicatively connected to the switch upon authentication of the communication device using the identifier;

forwarding the subscriber information to a response center; and

forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

2. The method of claim 1, wherein the call is a 911 emergency call.

3. The method of claim 1, wherein the identifier is received from an agent resident on the communication device.

4. The method of claim 1, wherein the subscriber information includes a location of the communication device.

5. The method of claim 1, further comprising forwarding the subscriber information from the response center to at least one public agency located in a specified area, wherein the forwarding occurs substantially simultaneously with the forwarding of the at least one alert message.

6. The method of claim 1, wherein a subscriber is able to access and modify the subscriber information via an interface allowing interaction with the central server.

7. The method of claim 1, wherein the communication network comprises a wireless emergency 911 network

8. The method of claim 1, wherein the communication network comprises a landline emergency 911 network.

9. The method of claim 1, wherein the at least one alert message is an SMS message.

10. The method of claim 1, wherein the subscriber information is at least one type of information selected from a group consisting of name, date of birth, language spoken, emergency contact, blood type, medications, allergies, weight, eye color, driver's license number, living will information, and organ donor information.

11. A method for providing subscriber information in conjunction with a call initiated by a subscriber to a response center comprising:

receiving the call and the subscriber information from a communication device operating on a communication network;

forwarding the call and the subscriber information to the response center; and

forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

12. The method of claim 11, wherein the call is a 911 emergency call.

13. The method of claim 11, wherein the subscriber information is stored in an agent resident on the communication device.

14. The method of claim 11, wherein the subscriber information includes a location of the communication device.

15. The method of claim 11, further comprising:

forwarding the subscriber information from the response center to at least one public agency located in a specified area, wherein the forwarding occurs substantially simultaneously with the forwarding of the at least one alert message.

16. The method of claim 11, wherein the subscriber information is at least one type of information selected from a group consisting of name, date of birth, language spoken, emergency contact, blood type, medications, allergies, weight, eye color, driver's license number, living will information, and organ donor information.

17. A computer program product, embodied on a computer-readable medium, for providing subscriber information to a response center upon initiation of a call from a communication device operating on a communication network comprising:

computer code for receiving an identifier identifying the communication device;

computer code for forwarding the identifier to a switch;

computer code for receiving the subscriber information from a central server communicatively connected to the switch upon authentication of the communication device using the identifier;

computer code for forwarding the subscriber information to a response center; and

computer code for forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

18. A computer program product, embodied on a computer-readable medium, for providing subscriber information in conjunction with a call initiated by a subscriber to a response center comprising:

computer code for receiving the call and the subscriber information from an agent resident on a communication device operating on a communication network;

computer code for forwarding the call and the subscriber information to the response center; and

computer code for forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

19. A communications transceiver comprising:

a processor; and

a memory unit operatively connected to the processor and including:

computer code for receiving an identifier identifying the communication device;

computer code for forwarding the identifier to a switch;

computer code for receiving the subscriber information from a central server communicatively connected to the switch upon authentication of the communication device using the identifier;

computer code for forwarding the subscriber information to a response center; and

computer code for forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

20. A communications transceiver comprising:

a processor; and

a memory unit operatively connected to the processor and including:

computer code for receiving the call and the subscriber information from an agent resident on a communication device operating on a communication network;

computer code for forwarding the call and the subscriber information to the response center; and

computer code for forwarding at least one alert message to at least one contact stored as at least one part of the subscriber information.

21. A network architecture for providing subscriber information to a response center upon initiation of a call from a communication device operating on a communication network comprising:

a communications transceiver configured to receive an identifier identifying the communication device;

a switch communicatively connected to the communications transceiver equipment configured to receive the identifier upon forwarding of the identifier by the communications transceiver equipment; and

a central server communicatively connected to the switch configured to transmit the subscriber information through the switch, to the communications transceiver equipment upon authentication by the central server of the communication device using the identifier,

wherein the communications transceiver equipment forwards the subscriber information to a response center and substantially simultaneously forwards at least one alert message to at least one contact stored as at least one part of the subscriber information.

22. A network architecture for providing subscriber information in conjunction with a call initiated by a subscriber to a response center comprising:

a communications transceiver configured to receive the call and the subscriber information from an agent residing on a communication device operating on a communication network, forward the call and the subscriber information to the response center, and substantially simultaneously forward at least one alert message to at least one contact stored as at least one part of the subscriber information.

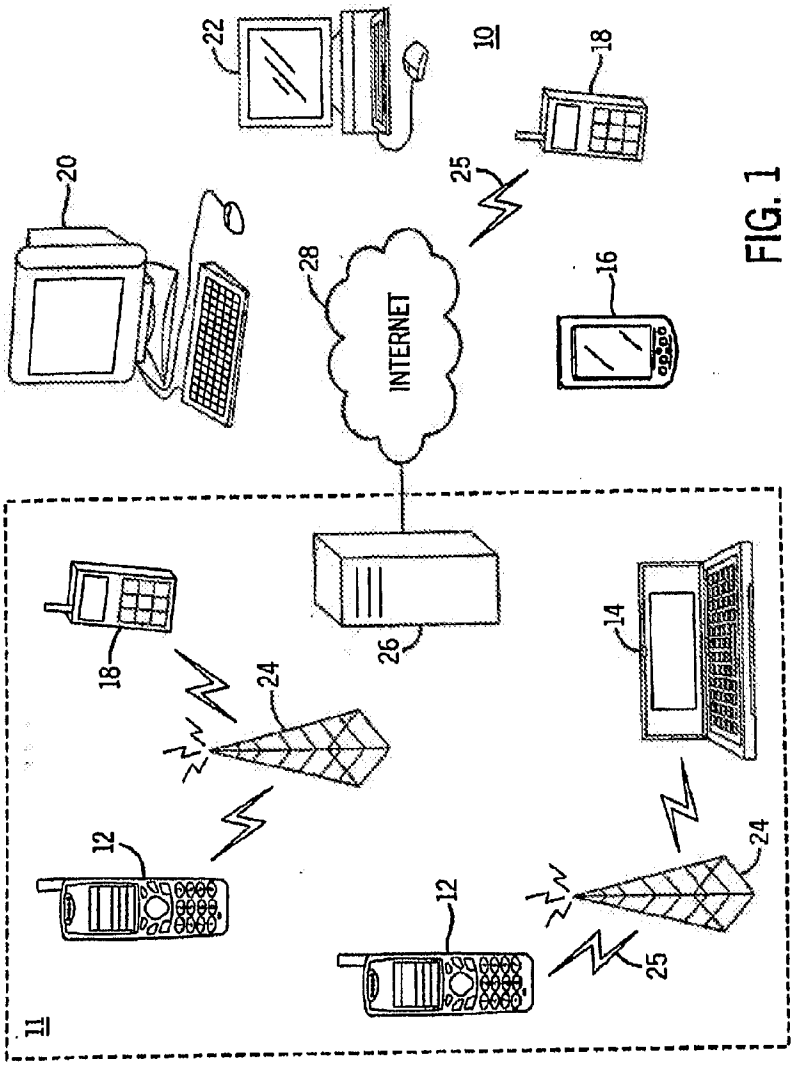


FIG. 1