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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2014 (06.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/032734 A1

(51) International Patent Classification:
H04W 4/22 (2009.01) *H04L 29/12* (2006.01)
H04W 4/02 (2009.01)

(21) International Application Number:
PCT/EP2012/067066

(22) International Filing Date:
3 September 2012 (03.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **TSCHOFENIG, Hannes** [AT/FI]; Niittytöyry 2 B 11, 02760 Espoo (FI). **BARCK, Esa Matti** [FI/FI]; Päiväkummuntie 4C 10, FI-02210 Espoo (FI).

(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, 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, 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))*

(54) **Title**: DETERMINATION OF CORRECT LOCATION INFORMATION SERVER

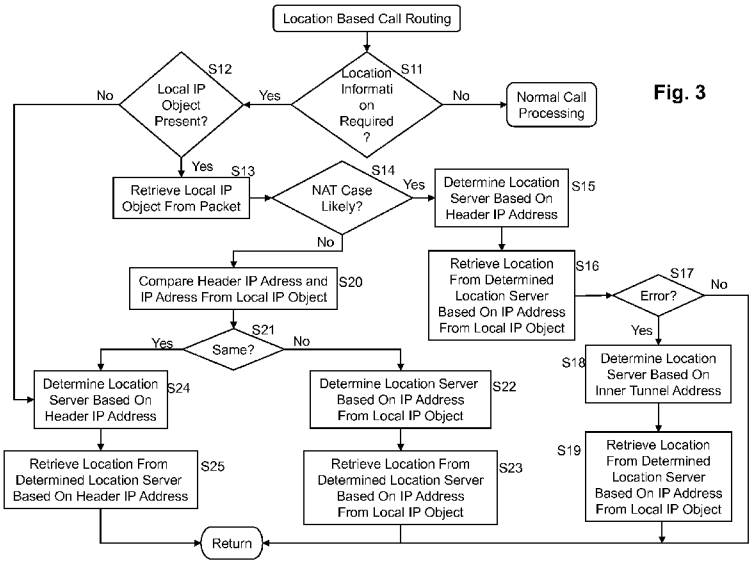


Fig. 3

(57) **Abstract**: An application service providing apparatus (50) of a communication network determines whether or not identification of a location of a calling end point (10) of an incoming call is required. In case the identification is required, an object is retrieved from data packets of the incoming call, the object including an IP address of the calling end point (10). A location server (60) for the calling end point (10), which provides information on the location of the calling end point (10), is determined based on at least one of the object retrieved and an IP address of an IP header of the data packets of the incoming call.

WO 2014/032734 A1

DESCRIPTION

Title

DETERMINATION OF CORRECT LOCATION INFORMATION SERVER

BACKGROUND OF THE INVENTION

Field of the invention

The present invention relates to determining the correct location information server and location based routing e.g. for emergency services.

Related background Art

Prior art which is related to this technical field can e.g. be found in:

[1] RFC5985, "HTTP-Enabled Location Delivery (HELD)", http://datatracker.ietf.org/doc/rfc5985

[2] RFC6155,"Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", http://www.rfc-editor.org/rfc/rfc6155.txt

[3] RFC5222, "LoST: A Location-to-Service Translation Protocol", http://tools.ietf.org/html/rfc5222

[4] RFC5986, "Discovering the Local Location Information Server", http://datatracker.ietf.org/doc/rfc5986

[5] "Location Information Server (LIS) Discovery using IP address and Reverse DNS", http://datatracker.ietf.org/doc/draft-ietf-geopriv-res-gw-lis-discovery

[6] "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments", http://datatracker.ietf.org/doc/draft-ietf-intarea-nat-reveal-analysis

The following meanings for the abbreviations used in this specification apply:

ASP	application service provider
DHCP	dynamic host configuration protocol
DNS	domain name service
ESRP	emergency service routing proxy
HELD	HTTP-enabled location delivery
HTTP	hypertext transfer protocol
ISP	Internet service provider
LIS	location information server
LoST	location-to-service translation protocol
NAT	network address translation
PSAP	public safety answering point
VSP	voice service provider

Various emergency services deployments consider an architecture that is called soft-switch-centric model, which is illustrated in Fig. 1. In step S1, a device (caller) initiates an emergency call and a serving soft-switch detects that the call is an emergency and initiates retrieving the caller's location from an LIS (steps S2 and S3), for example using HELD as described in reference [1] with identity extensions as described in reference [2], and then determining a route to a local PSAP, for example using LoST as described in reference [3]. That is, in step S4 the soft-switch uses a request "find service" towards a LoST server to retrieve the service (step S5). Finally, the soft-switch routes the call to the local PSAP (ESRP/PSAP) (step S6).

In the soft-switch-centric model, when a VSP receives an emergency call it will encounter difficulties because of the following reasons.

One of the big hurdles for the VSP is to determine the correct LIS to ask for location information. The standard approach for addressing this problem is to identify the responsible Internet access provider with a reverse DNS look-up.

There are various reasons why the IP address seen by the VSP, ESRP, or the PSAP is not the IP address in use by the end device. Examples include:

1) IP tunneling:

Various tunneling mechanisms provide a source IP address to the VSP that is different from the IP address provided to the end device's interface by an ISP. These tunneling mechanisms are common on the Internet.

2) Network address translation:

Many network operators deploy network address translation (NAT) devices to deal with IPv4 shortage. With NATs an original source IP address is replaced by an IP address of the NAT.

Some IPv6 transition techniques also make use of NAT techniques. As such, for a longer timeframe the number of NATs will increase even with the shift to IPv6.

Devices can connect to the Internet via different access network providers and, in case of nomadic or mobile use, they may even change the access network provider on a regular basis. The consequence is that a lookup by the VSP using the reverse DNS mechanism (which uses the IP address of the received packet as input) leads to the wrong access

network provider. Note that a user may choose an arbitrary VSP on the Internet and there is also typically no relationship between the VSP and the access network provider. As such, any subsequent location lookup will fail. The term "access network provider" encompasses both an Internet Access Provider (IAP) and an Internet Service Provider (ISP).

To address the problem of incorrect location lookups, additional intelligence may be added to an end host (end device). The end host's software knows when it establishes a tunnel and can use the correct IP address. It can even determine the access network provider's domain name using DHCP. Standardized solutions for this approach exist, see references [4] and [5].

Unfortunately, not all devices deploy such a solution nor will legacy devices support it. Furthermore, communications service providers may not want to trust the information they obtain from the end device and may want to rely on a solution that is more robust.

SUMMARY OF THE INVENTION

The present invention aims at overcoming the above drawbacks and providing a robust solution that enables an application service provider to determine the correct location information server.

This is, at least in part, achieved by the methods and apparatuses as defined in the appended claims. The invention may also be implemented by a computer program product.

The present invention provides a practical solution that enables to determine the correct location information server and emergency call routing without need to make any changes to the end device utilizing e.g. Local IP Object. Moreover, a process for a location based routing is determined based on the available IP address(es).

According to an embodiment of the invention, robust emergency call routing by VSPs and ASPs is enabled.

In the following the invention will be described by way of embodiments thereof with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figs. 1 shows a schematic block diagram illustrating a soft-switch-centric calling model.

Fig. 2A shows a schematic diagram illustrating forwarding of IP information without NAT reveal option.

Fig. 2B shows a schematic diagram illustrating forwarding of IP information with NAT reveal option.

Fig. 3 shows a flow chart illustrating location based call routing according to an embodiment of the invention.

Fig. 4 shows a schematic block diagram illustrating a calling model according to an embodiment of the invention.

Figs. 5A, 5B and 5C show flow charts illustrating processes according to an embodiment of the invention, executed by various electronic devices.

Fig. 6 shows a schematic block illustrating a configuration of control units in which examples of embodiments of the invention are implementable.

DESCRIPTION OF THE EMBODIMENTS

Several solution approaches have been proposed to add information, such as IP address and port number, to an outgoing IP packet by an access provider, see reference [6].

Figs. 2A and 2B aim to show the difference between an e2e communication with and without a NAT reveal option graphically.

According to Fig. 2A, a device 11 transmits IP packets with its inner IP address (step C1), a NAT 21a translates the inner IP address to an outer IP address and transmits the IP packets with the outer IP address to a server 31 (step C2a), and the server 31 transmits the IP packets with the outer IP address. In this example the NAT reveal option is not used.

Fig. 2B shows that the IP address as used by the device 11 (called inner IP address) is added to the outgoing packet. NAT 21b forwards the packet with the inner and the outer IP address to the server 31 (step C2b). This example illustrates the usage of the NAT reveal option.

While the NAT reveal option focuses on NATs as their use case, the ability of an access network operator to attach information about the local IP address used by the device has broader applicability.

According to an embodiment of the invention, this extended concept is applied to emergency calling and a "Local IP Object" is defined to provide an ASP (e.g. a VSP) with addi-

tional information to determine the correct LIS and to fetch the correct location information of the device without any changes to the device itself.

The Local IP Object may contain the following information:

- IP address
- Transport protocol identifier (e.g., UDP, TCP)
- Port number
- (optionally) access network domain identifier. This identifier may short-cut a lookup process by omitting a reverse DNS lookup. However, the additional content in the IP packet may lead to fragmentation, which may not be desirable in all cases.

According to an embodiment of the invention, in addition to the Local IP Object a packet contains, a process of location based call routing is implemented by the ASP. The following process of location based call routing illustrated in Fig. 3 shows interactions that are performed by the ASP to determine a correct location server, to (optionally) retrieve a location by reference (or even a location by value, if possible), and to obtain information to route the emergency call.

In certain deployment scenarios the access network provider may not want to convey location information of the end device to the ASP. For example, in order to protect the privacy of the end user the access provider may not want to transmit location information to an ASP without the user's consent or an indication that the information will only be used for emergency services. Since the access network provider is not actively involved in the emergency call signaling it cannot judge whether the request from the ASP is for an emergency situation or not. In such a case the access provider may not want to provide the location directly to the ASP but will instead want to provide two elements instead, namely

- A location reference that can only be resolved to location information by trusted parties. Entities in the emergency services network, such as a PSAP, are such trusted entities.
- Information about where to route the emergency call. In the generic description below this information is obtained in a two-step process, namely the first step is to request

and obtain location information and then, as a second step, this location information is used to request information where to route the PSAP (for example, via LoST). Instead of executing these steps separately, which would require the ASP to know the location information to perform the second step, the two interactions can also be collapsed into one: the request for location information immediately leads to a location reference as well as information where to route the call (such as a PSAP or an ESRP URI).

It is to be noted that there are two types of IP addresses in the process, namely an IP address from an IP header of data packets and an IP address included in a Local IP Object added to the data packets. This Local IP Object may also include a port number and a transport protocol identifier as well and not just the pure IP address. If the Local IP object is able to convey an access network identifier then the initial reverse DNS lookup can be omitted.

For the process illustrated in Fig. 3, the following assumptions are made:

1) An access network operator adds the Local IP Object to outgoing IP packets.

2) An ASP is able to process the Local IP Object.

3) If there is a provider offering tunneling services then it also needs to forward the Local IP Object and may even need to maintain state information about the IP address of the IP header from an outer tunnel as seen by its gateway.

4) An end host (calling end point) does not intentionally route the call through a provider that removes the Local IP Object.

Referring to Fig. 3, in step S11 it is checked whether or not an incoming call requires location information. For example, in case the incoming call is an emergency call, location information of the calling end point is required. In case no location information is required, normal call processing is carried out.

In case location information of the calling end point is required, the process advances to step S12 in which it is checked whether or not a Local IP Object is present in the data

packets of the incoming call. In case no Local IP Object is present, the process may advance to step S24 in which an IP address of an IP header of the data packets is used for a reverse DNS lookup to determine a location server for the calling end point. For example, the IP address in the header is used as input to the process described in reference [5]. Then, in step S25 information on the location of the calling end point is retrieved from the location server determined in step S24, based on the IP address in the header. For example, a HELD lookup with identity extension described in reference [2] is performed. After that, the process is completed. It is to be noted that the process flow S11 → S12 → S24→ S25 is the fall back case and may lead to a wrong result.

In case the Local IP Object is present in step S12, the process advances to step S13 in which the Local IP Object is retrieved from the data packets. In step S14 it is checked whether it is likely that a network address translation has been performed on the IP address of the IP header. For example, in case an IP address derived from the Local IP Object is a private address, network address translation has likely been performed. In that case, the process advances to step S15 in which the IP address of the IP header of the data packets is used for the reverse DNS lookup to determine the location server for the calling end point. For example, the IP address in the header is used as input to the process described in reference [5]. Then, in step S16 information on the location of the calling end point is retrieved from the location server determined in step S15, based on the IP address of the Local IP Object. For example, a HELD lookup with identity extension described in reference [2] is performed. In step S17 it is checked whether or not the information retrieval in step S16 caused an error. In case no error was caused, the process is completed.

In case an error was caused, a combination of NAT and tunneling is present. That is, the lookup performed in step S15 resulted in the provider of an endpoint of the tunnel. In step S18, an inner tunnel address is used for a reverse DNS lookup to determine a location server for the calling end point. For example, the inner tunnel address is used as input to the process described in reference [5]. Then, in step S19 information on the location of the calling end point is retrieved from the location server determined in step S18, based on the IP address of the Local IP Object. For example, a HELD lookup with identity extension described in reference [2] is performed. After that, the process is completed.

The ASP may retrieve the inner tunnel address from the provider of the tunnel endpoint and perform steps S18 and S19. Alternatively, the provider of the tunnel may perform step S18 and return the location server determined to the ASP. The provider of the tunnel may further perform step S19 and report the retrieved location information to the ASP.

In step S14, in case network address translation is not likely, the process advances to step S20 in which the IP address of the IP header is compared with the IP address of the Local IP Object. In case it is determined in step S21 that the addresses are not the same which means that the data packets were subjected to tunneling, step S22 follows in which the IP address of the Local IP Object is used for the reverse DNS lookup to determine the location server for the calling end point. For example, the IP address of the Local IP Object is used as input to the process described in reference [5]. Then, in step S23 information on the location of the calling end point is retrieved from the location server determined in step S22, based on the IP address of the Local IP Object. For example, a HELD lookup with identity extension described in reference [2] is performed. Then, the process is completed.

In case the address are the same in step S21, the process advances to step S24 in which the IP address of the IP header of the data packets is used for the reverse DNS lookup to determine the location server for the calling end point. For example, the IP address in the header is used as input to the process described in reference [5]. Then, in step S25 information on the location of the calling end point is retrieved from the location server determined in step S24, based on the IP address in the header. For example, a HELD lookup with identity extension described in reference [2] is performed. After that, the process is completed.

Fig. 4 shows a schematic block diagram illustrating a calling model according to an embodiment of the invention.

An end point 10 initiates a call towards an ASP 50 via a network access provider 30 (data flows T1 and T'1). The call may be subjected to network address translation by a NAT 20 (data flows T1a and T1b) and/or to tunneling by a tunnel provider 40 (data flows T'1a and T'1b). The ASP 50 performs the process shown in Fig. 3. In other words, the ASP determines whether the data packets of the incoming call include the Local IP Object, whether a network address translation has been performed, and whether tunneling has been performed. Depending on the determination results, the ASP 50 determines a location server 60 for the calling end point 10 based on the Local IP Object or the IP address of the IP header of the data packets of the incoming call.

Further, in case network address translation and tunneling have been performed, the ASP 50 may retrieve an inner tunnel address from the tunnel provider 40 (data flows T2a and T2b), and determine the location server 60 based on this inner tunnel address.

The ASP 50 may retrieve information on the location of the calling end point 10 from the location server 60 determined, based on the IP address of the calling end point or the IP address of the IP header (data flows T3 and T4). Then, the route to a local PSAP (ESRP/PSAP 80) is determined e.g. using a LoST server 70 (data flows T5 and T6), and finally the call is routed to the determined local PSAP (data flow T7).

Figs. 5A, 5B and 5C show flow charts illustrating processes according to an embodiment of the invention, executed by various electronic devices.

Fig. 5A illustrates a method for use by an application service providing apparatus of a communication network, e.g. the ASP 50 shown in Fig. 4.

In step S51 it is determined whether or not identification of a location of a calling end point of an incoming call is required. In case the identification is required, in step S52 an object (e.g. the Local IP Object) is retrieved from data packets of the incoming call, the object including an IP address of the calling end point. Then, in step S53 a location server for the

calling end point is determined based on at least one of the object retrieved and an IP address of an IP header of the data packets of the incoming call, the location server providing information on the location of the calling end point. In case no identification is required in step S51, normal call processing is carried out. Step S51 is associated with step S11, step S52 is associated with step S13, and step S53 is associated with steps S15, S18, S22 and S24.

Fig. 5B illustrates a method for use by an apparatus of an access network providing access to a communication network, e.g. the network access provider 30 shown in Fig. 4.

In step S31 data packets for a call towards the communication network are generated. In step S32 an object (e.g. the Local IP Object) is added to the data packets, the object including an IP address of a calling end point of the call.

Fig. 5C illustrates a method for use by an apparatus tunneling data packets between an access network, which provides access to a communication network, and the communication network, e.g. the tunnel provider 40 shown in Fig. 4.

In step S41 an object included in data packets of a call towards the communication network is forwarded, when the data packets are tunneled from the access network to the communication network, the object including an IP address of a calling end point of the call, and in step S42 information about an IP address of an IP header of the data packets is maintained as an inner tunnel address. This inner tunnel address corresponds to the inner tunnel address of step S18 in Fig. 3.

Now reference is made to Fig. 6 for illustrating a simplified block diagram of various electronic devices that are suitable for use in practicing the exemplary embodiments of this invention.

For example, control unit 300 may be part of or used by a network access provider (e.g. the network access provider 30 shown in Fig. 4). The control unit 300 comprises processing resources 311, memory resources 312 and interfaces 313 which are connected by a link 314. The control unit 300 may execute process 2 shown in Fig. 5B, using its processing resources 311, memory resources 312 and interfaces 313.

The control unit 300 is connected to another control unit 500, which may be part of or used by an ASP 50, via a link 135 through its interfaces 313. The control unit 500 comprises processing resources 511, memory resources 512 and interfaces 513 which are connected by a link 514. The control unit 500 may execute process 1 shown in Fig. 5A, using its processing resources 511, memory resources 512 and interfaces 513. The control unit 500 is connected to the control unit 300 via the link 135 through its interfaces 513.

Moreover, the control unit 500 may be connected to a control unit 400, which may be part of or used by a tunnel provider 40, via a link 245 through its interfaces 513. The control unit 400 comprises processing resources 411, memory resources 412 and interfaces 413 which are connected by a link 414. The control unit 400 may execute process 3 shown in Fig. 5C, using its processing resources 411, memory resources 412 and interfaces 413. The control unit 400 may be connected to the control unit 500 via the link 245 through its interfaces 413.

The terms "connected," "coupled," or any variant thereof, mean any connection or coupling, either direct or indirect, between two or more elements, and may encompass the presence of one or more intermediate elements between two elements that are "connected" or "coupled" together. The coupling or connection between the elements can be physical, logical, or a combination thereof. As employed herein two elements may be considered to be "connected" or "coupled" together by the use of one or more wires, cables and printed electrical connections, as well as by the use of electromagnetic energy, such as electromagnetic energy having wavelengths in the radio frequency region, the microwave region and the optical (both visible and invisible) region, as non-limiting examples.

The memory resources 312, 412, 512 may store programs assumed to include program instructions that, when executed by the associated processing resources 311, 411, 511, enable the electronic device to operate in accordance with the exemplary embodiments of this invention, as detailed above.

The exemplary embodiments of this invention may be implemented by computer software stored in the memory resources 312, 412, 512 and executable by the associated processing resources 311, 411, 511, or by hardware, or by a combination of software and/or firmware and hardware in any or all of the devices shown.

The memory resources 312, 412, 512 may be of any type suitable to the local technical environment and may be implemented using any suitable data storage technology, such as semiconductor-based memory devices, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory. The processing resources 311, 411, 511 may be of any type suitable to the local technical environment, and may include one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on a multi-core processor architecture, as non-limiting examples.

According to an aspect of the invention, an application service providing apparatus of a communication network, which may comprise or use the control unit 500, comprises means for determining whether or not identification of a location of a calling end point of an incoming call is required, means for, in case the identification is required, retrieving an object from data packets of the incoming call, the object including an IP address of the calling end point, and

means for determining a location server for the calling end point based on at least one of the object retrieved and an IP address of an IP header of the data packets of the incoming call, the location server providing information on the location of the calling end point.

The means for retrieving may retrieve the information on the location of the calling end point from the location server determined, based on the IP address of the calling end point

or the IP address of the IP header. The information on the location may comprises at least one of a location, a location reference, and information about where to route the incoming call.

The application service providing apparatus may comprise means for deciding whether or not network address translation has likely been performed on the IP address of the calling end point, wherein in case it is decided that network address translation has likely been performed, the means for determining may determine the location server based on the IP address of the IP header, and the means for retrieving may retrieve the information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

The application service providing apparatus may comprise means for, in case the retrieving fails, determining another location server based on an inner tunnel address.

The application service providing apparatus may comprise means for, in case it is decided that network address translation has not likely been performed, comparing the IP address of the IP header with the IP address of the calling end point, wherein in case the IP addresses are different, the means for determining may determine the location server based on the IP address of the calling end point, and the means for retrieving may retrieve the information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

In case the IP addresses are the same, the means for determining may determine the location server based on the IP address of the IP header, and the means for retrieving may retrieve information on the location of the calling end point from the location server determined, based on the IP address of the IP header.

The deciding whether or not network address translation has likely been performed on the IP address of the calling end point may be based on the kind of IP address of the calling end point.

A call requiring the identification of the location of the calling end point may comprise an emergency call.

The above means comprising the determining, retrieving, comparing and deciding means may be implemented by the processing resources 511, memory resources 512 and interfaces 513.

According to an aspect of the invention, an apparatus of an access network providing access to a communication network, which may comprise or use the control unit 300, comprises means for generating data packets for a call towards the communication network, and means for adding an object to the data packets, the object including an IP address of a calling end point of the call.

The object may further include at least one of following: a transport protocol identifier, a port number and an access network domain identifier.

The above means comprising the generation and adding means may be implemented by the processing resources 311, memory resources 312 and interfaces 313.

According to an aspect of the invention, an apparatus tunneling data packets between an access network, which provides access to a communication network, and the communication network, which may comprise or use the control unit 400, comprises means for forwarding an object included in data packets of a call towards the communication network, when the data packets are tunneled from the access network to the communication network, the object including an IP address of a calling end point of the call, and means for

maintaining information about an IP address of an IP header of the data packets as an inner tunnel address.

The above means comprising the forwarding and maintaining means may be implemented by the processing resources 411, memory resources 412 and interfaces 413.

It is to be understood that the above description is illustrative of the invention and is not to be construed as limiting the invention. Various modifications and applications may occur to those skilled in the art without departing from the true spirit and scope of the invention as defined by the appended claims.

CLAIMS:

1. A method for use by an application service providing apparatus of a communication network, the method comprising:

determining whether or not identification of a location of a calling end point of an incoming call is required;

in case the identification is required, retrieving an object from data packets of the incoming call, the object including an IP address of the calling end point; and

determining a location server for the calling end point based on at least one of the object retrieved and an IP address of an IP header of the data packets of the incoming call, the location server providing information on the location of the calling end point.

2. The method of claim 1, comprising:

retrieving information on the location of the calling end point from the location server determined, based on the IP address of the calling end point or the IP address of the IP header.

3. The method of claim 1 or 2, comprising:

deciding whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has likely been performed, determining the location server based on the IP address of the IP header.

4. The method of claim 3, comprising:

retrieving information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

5. The method of claim 4, comprising:

in case the retrieving fails, determining another location server based on an inner tunnel address.

6. The method of claim 1 or 2, comprising:

deciding whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has not likely been performed, comparing the IP address of the IP header with the IP address of the calling end point; and

in case the IP addresses are different, determining the location server based on the IP address of the calling end point.

7. The method of any one of claims 3 to 6, comprising:

retrieving information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

8. The method of claim 1 or 2, comprising:

deciding whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has not likely been performed, comparing the IP address of the IP header with the IP address of the calling end point;

in case the IP addresses are the same, determining the location server based on the IP address of the IP header; and

retrieving information on the location of the calling end point from the location server determined, based on the IP address of the IP header.

9. The method of any one of claims 3 to 8, wherein the deciding whether or not network address translation has likely been performed on the IP address of the calling end point is based on the kind of IP address of the calling end point.

10. The method of any one of claims 1 to 9, wherein a call requiring the identification of the location of the calling end point comprises an emergency call.

11. A method for use by an apparatus of an access network providing access to a communication network, the method comprising:

generating data packets for a call towards the communication network; and

adding an object to the data packets, the object including an IP address of a calling end point of the call.

12. The method of any one of claims 1 to 11, wherein the object further includes at least one of following: a transport protocol identifier, a port number and an access network domain identifier.

13. A method for use by an apparatus tunneling data packets between an access network, which provides access to a communication network, and the communication network, the method comprising:

forwarding an object included in data packets of a call towards the communication network, when the data packets are tunneled from the access network to the communication network, the object including an IP address of a calling end point of the call; and

maintaining information about an IP address of an IP header of the data packets as an inner tunnel address.

14. A computer program product including a program for a processing device, comprising software code portions for performing the steps of any one of claims 1 to 13 when the program is run on the processing device.

15. The computer program product according to claim 14, wherein the computer program product comprises a computer-readable medium on which the software code portions are stored.

16. The computer program product according to claim 14, wherein the program is directly loadable into an internal memory of the processing device.

17. An application service providing apparatus of a communication network, the apparatus configured to:

determine whether or not identification of a location of a calling end point of an incoming call is required;

in case the identification is required, retrieve an object from data packets of the incoming call, the object including an IP address of the calling end point; and

determine a location server for the calling end point based on at least one of the object retrieved and an IP address of an IP header of the data packets of the incoming call, the location server providing information on the location of the calling end point.

18. The apparatus of claim 17, configured to:

retrieve information on the location of the calling end point from the location server determined, based on the IP address of the calling end point or the IP address of the IP header.

19. The apparatus of claim 17 or 18, configured to:

decide whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has likely been performed, determine the location server based on the IP address of the IP header.

20. The apparatus of claim 19, configured to:

retrieve information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

21. The apparatus of claim 20, configured to:

in case the retrieval fails, determine another location server based on an inner tunnel address.

22. The apparatus of claim 17 or 18, configured to:

decide whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has not likely been performed, compare the IP address of the IP header with the IP address of the calling end point; and

in case the IP addresses are different, determine the location server based on the IP address of the calling end point.

23. The apparatus of any one of claims 19 to 22, configured to:

retrieve information on the location of the calling end point from the location server determined, based on the IP address of the calling end point.

24. The apparatus of claim 17 or 18, configured to:

decide whether or not network address translation has likely been performed on the IP address of the calling end point; and

in case it is decided that network address translation has not likely been performed, compare the IP address of the IP header with the IP address of the calling end point;

in case the IP addresses are the same, determine the location server based on the IP address of the IP header; and

retrieve information on the location of the calling end point from the location server determined, based on the IP address of the IP header.

25. The apparatus of any one of claims 19 to 24, wherein the decision whether or not network address translation has likely been performed on the IP address of the calling end point is based on the kind of IP address of the calling end point.

26. The apparatus of any one of claims 18 to 25, wherein the information on the location comprises at least one of a location, a location reference, and information about where to route the incoming call.

27. An apparatus of an access network providing access to a communication network, the apparatus configured to:

generate data packets for a call towards the communication network; and

add an object to the data packets, the object including an IP address of a calling end point of the call.

28. An apparatus for tunneling data packets between an access network, which provides access to a communication network, and the communication network, the apparatus configured to:

forward an object included in data packets of a call towards the communication network, when the data packets are tunneled from the access network to the communication network, the object including an IP address of a calling end point of the call; and

maintain information about an IP address of an IP header of the data packets as an inner tunnel address.

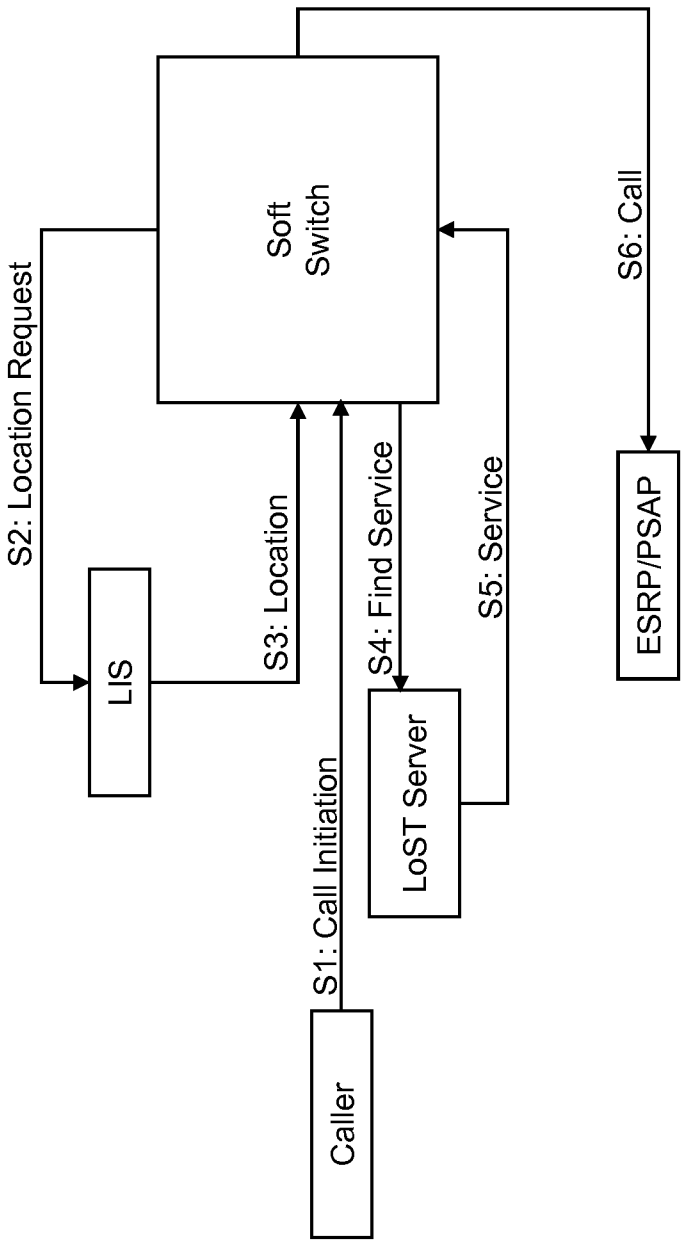

Soft Switch
S2: Location Request
S3: Location
S4: Find Service
S5: Service
S6: Call
LIS
LoST Server
ESRP/PSAP
S1: Call Initiation
Caller

Fig. 1

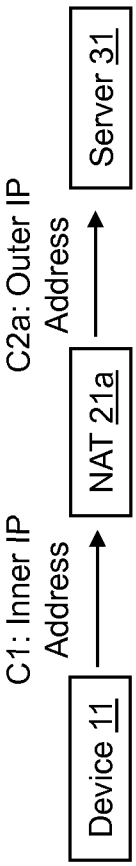


Fig. 2A

Fig. 2B

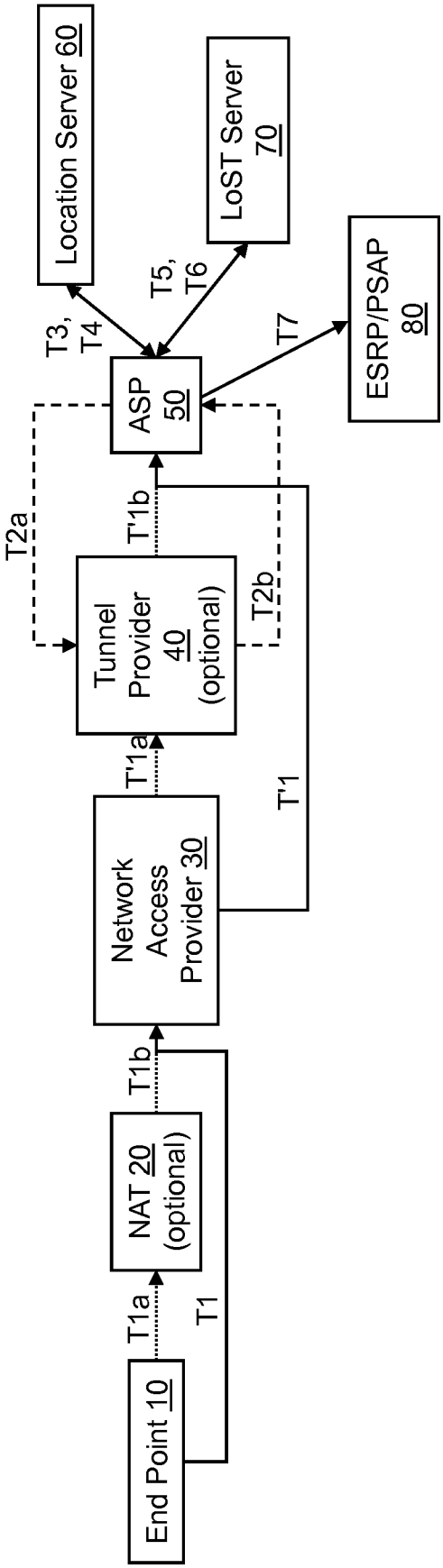
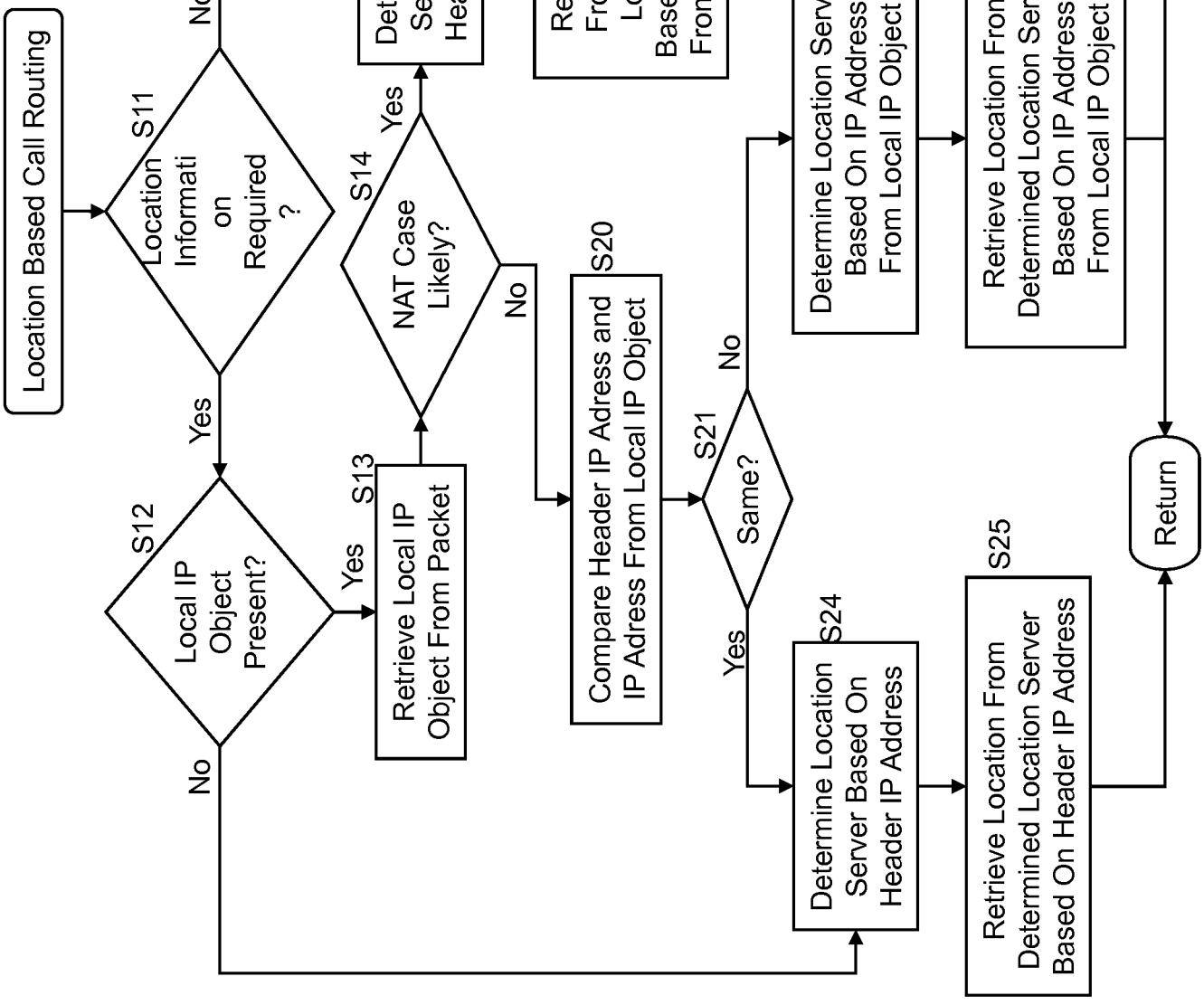


Fig. 4

Fig. 3


Location Based Call Routing
S11
Location Informati on Required ?
No
Normal Call Processing
Yes
S12
Local IP Object Present?
No
Yes
S13
Retrieve Local IP Object From Packet
S14
NAT Case Likely?
Yes
S15
Determine Location Server Based On Header IP Address
S16
Retrieve Location From Determined Location Server Based On IP Address From Local IP Object
S17
Error?
No
Yes
S18
Determine Location Server Based On Inner Tunnel Address
S19
Retrieve Location From Determined Location Server Based On IP Address From Local IP Object
No
S20
Compare Header IP Adress and IP Adress From Local IP Object
S21
Same?
No
S22
Determine Location Server Based On IP Address From Local IP Object
S23
Retrieve Location From Determined Location Server Based On IP Address From Local IP Object
Yes
S24
Determine Location Server Based On Header IP Address
S25
Retrieve Location From Determined Location Server Based On Header IP Address
Return

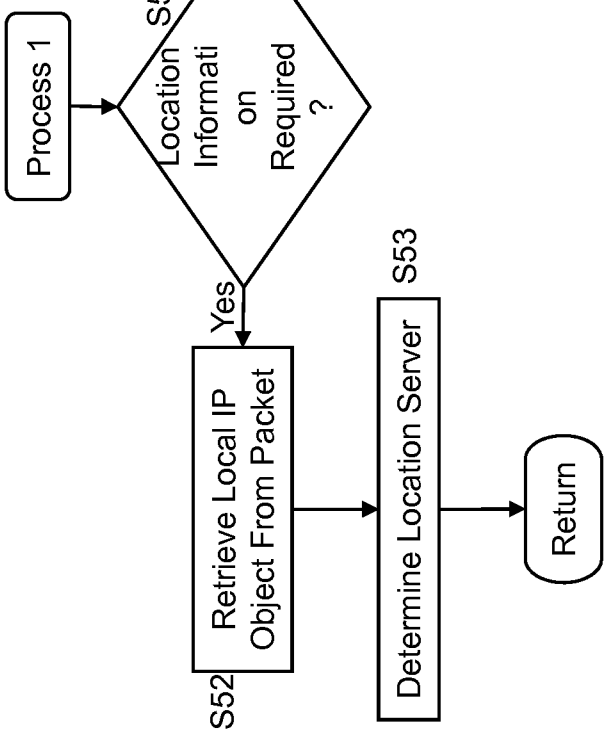


Fig. 5A

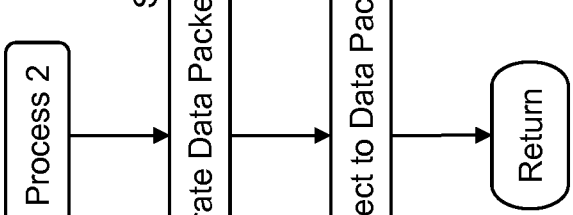


Fig. 5B

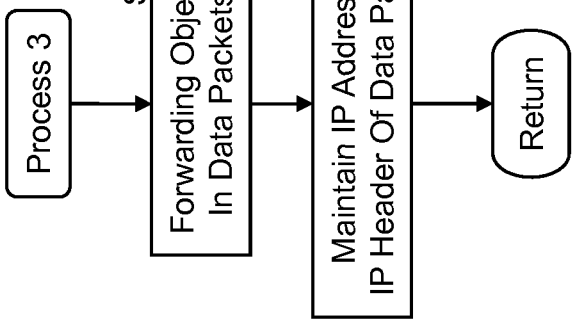


Fig. 5C

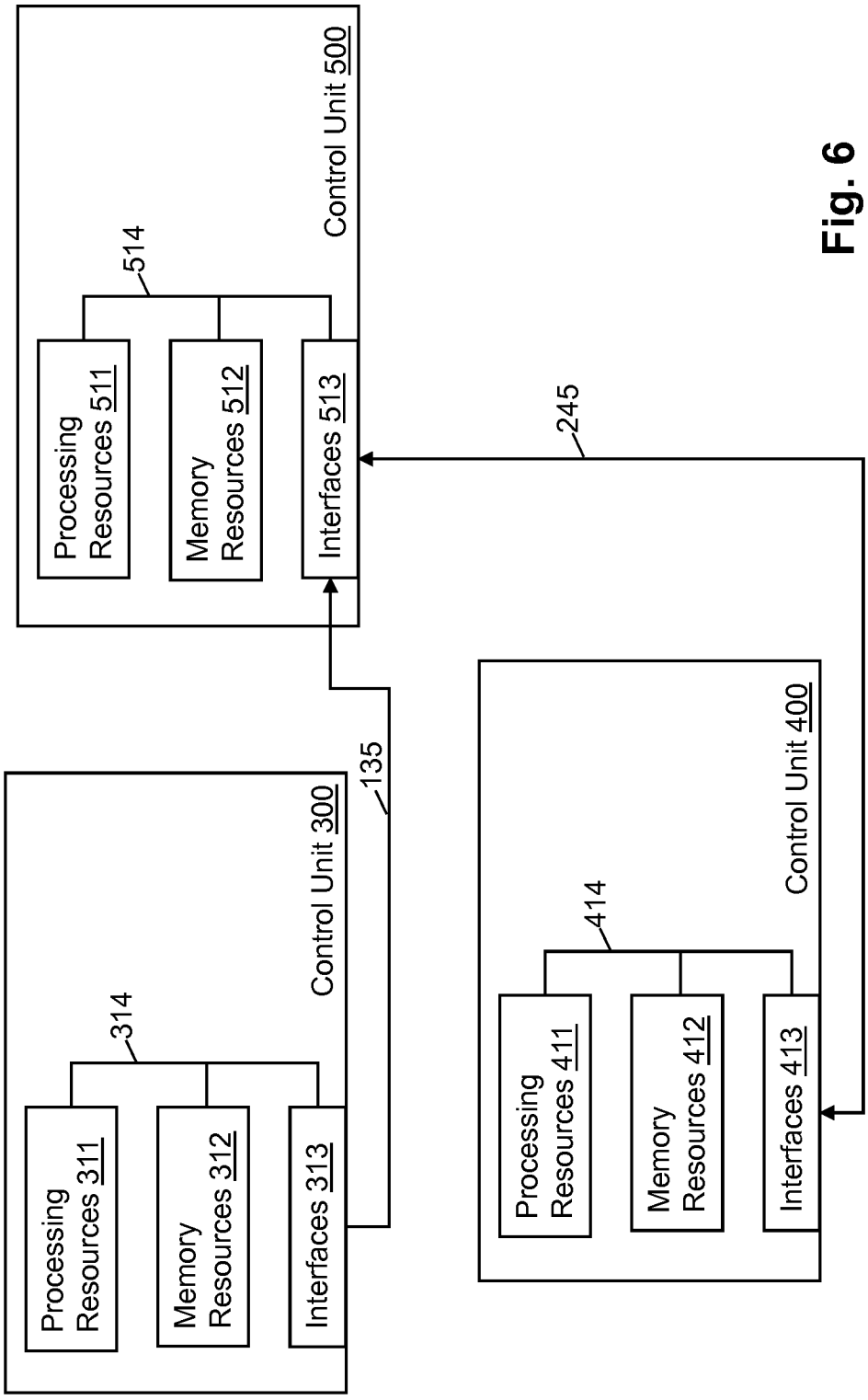

Control Unit 500
514
Processing Resources 511
Memory Resources 512
Interfaces 513
245
Control Unit 400
414
Processing Resources 411
Memory Resources 412
Interfaces 413
135
Control Unit 300
314
Processing Resources 311
Memory Resources 312
Interfaces 313

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/067066

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/22 H04W4/02 H04L29/12
ADD.

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)
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)

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HANNES TSCHOFENIG ET AL: "How secure is the next generation of IP-based emergency services architecture?", INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION, vol. 3, no. 1, 1 May 2010 (2010-05-01), pages 41-50, XP055065147, ISSN: 1874-5482, DOI: 10.1016/j.ijcip.2010.02.001 page 42, column 2 ----- -/--	1-28

[X] 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
6 June 2013	17/06/2013

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, Fax: (+31-70) 340-3016	de la Peña Álvarez

3

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	"Out of Jurisdiction Emergency Routing draft-winterbottom-ecrit-priv-loc-01.txt", , 16 July 2012 (2012-07-16), XP055064950, Retrieved from the Internet: URL:http://tools.ietf.org/pdf/draft-winterbottom-ecrit-priv-loc-01.pdf [retrieved on 2013-06-03] section 6.1	1-28
A	BOUCADAIR FRANCE TELECOM J TOUCH USC/ISI P LEVIS FRANCE TELECOM R PENNO CISCO M: "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments; draft-ietf-intarea-nat-reveal-analysis-04.txt", ANALYSIS OF SOLUTION CANDIDATES TO REVEAL A HOST IDENTIFIER (HOST_ID) IN SHARED ADDRESS DEPLOYMENTS; DRAFT-IETF-INTAREA-NAT-REVEAL-ANALYSIS-04.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAIS, 21 August 2012 (2012-08-21), pages 1-22, XP015086930, [retrieved on 2012-08-21] cited in the application section 4	1-28
A	THOMSON MICROSOFT R BELLIS NOMINET UK M: "Location Information Server (LIS) Discovery using IP address and Reverse; draft-ietf-geopriv-res-gw-lis-discovery-03.txt", LOCATION INFORMATION SERVER (LIS) DISCOVERY USING IP ADDRESS AND REVERSE; DRAFT-IETF-GEOPRIV-RES-GW-LIS-DISCOVERY-03.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH-1205 GENEVA, SWITZE, 29 March 2012 (2012-03-29), pages 1-19, XP015082233, [retrieved on 2012-03-29] cited in the application section 2	1-28