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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/142332 A1

(51) International Patent Classification:
H04W 40/02 (2009.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2009/057208

(22) International Filing Date:
10 June 2009 (10.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS GMBH & CO. KG** [DE/DE]; St. Martin Str. 76, 81541 München (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PITTMANN, Frank** [DE/DE]; Götzstr. 51, 12099 Berlin (DE). **UDUGAMA, Asanga** [LK/DE]; Im Hollergrund 15, 28357 Bremen (DE).

(74) Common Representative: **NOKIA SIEMENS NETWORKS GMBH & CO. KG**; COO RTP IPR/Patent Administration, St. Martin Str. 76, 81541 München (DE).

(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, 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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, 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))*

(54) **Title**: NETWORK ENTITIES AND METHODS CONFIGURED FOR SUPPORTING OF FLOW IDENTIFICATION IN COMMUNICATIONS NETWORKS

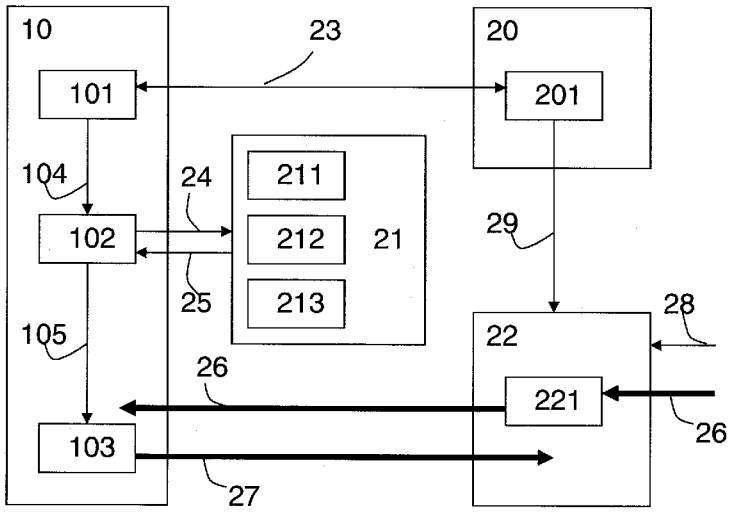

Fig. 2

(57) **Abstract**: The present invention refers to supporting of flow identification in a communications network, within scope of which a first network entity is provided, which comprises a data processing module configured to: transmit a flow identifier to a second entity of said communications network; receive a flow filter data from said second entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and provide said flow filter data for identification of traffic flows in said communications network. The second network entity, in turn, comprises: a receiving module configured to receive a flow identifier from the first network entity; a data processing module configured to determine a flow filter data based on said flow identifier; and a transmitting module configured to transmit said flow filter data to said first network entity.

WO 2010/142332 A1

Network entities and methods configured for supporting of flow identification in communications networks

FIELD OF THE INVENTION

The present invention relates to supporting of flow identification in communications networks at side of mobile nodes or user equipments respectively. Particularly, the present invention refers to network entities, methods, computer program products, and data carriers enabling the supporting of the flow identification.

BACKGROUND OF THE INVENTION

With the development of a multitude of wireless access systems in communications networks, the need for developing sophisticated means for resource allocation and handover control has become imminent, in particular, in heterogeneous wireless environments of communications networks. Allocation mechanisms for heterogeneous resources are expected to take responsibility for mapping of mobile devices or user equipments (UE) respectively to different access technologies based on load conditions in radio access and core, user application requirements, and/or current geographic location without sacrificing the user experience in terms of quality of service and seamless service. Network architectures enabling such mapping of mobile devices or UEs respectively must incorporate information from various sources including means for network operators to efficiently manage their networks by assisting (e.g., guiding and/or steering) mobile devices as much as possible or as much as intended with information provided by network entities in cases the network has the best or most knowledge of traffic flows in the network and/or to save resources of mobile devices or UEs to enlarge user's perception of mobile services.

However, the known methodologies do not allow to support mobile devices or UEs in a flexible and resource saving way

when decision with regard to an access point in a multi access point situation has to be met.

In particular, mobile devices or UEs respectively comprise flow identification (FI) devices for identifying the correct or at least most suitable traffic way or network access point for data to be transmitted, said traffic flow leading through one access point of the multiple access points being the correct or at least the most suitable access point. Such flow identification (FI) device performs the identification by use of a flow identification (FI) scheme. The FI scheme comprises several conditions for deciding on the correct or at least most suitable traffic way for data received or to be transmitted. With the development of multitude of wireless access systems in communications networks, these conditions to be covered and taken into account by the FI scheme become very sophisticated. This, in turn, leads to inefficient use and handling of resources (e.g., processing power, battery lifetime, storage capacity etc.) of the corresponding mobile device or UE respectively, which are limited and/or valuable in the most cases. The known methodologies for handling and supporting FI in communications networks still require too much resources of mobile devices or UEs respectively and still do not utilize the FI schemes in the required efficient way.

Furthermore, a plurality of FI schemes is available for FI in communications network. Here, an efficient, flexible, and FI scheme independent solution for supporting identification of correct or at least most suitable traffic way for data received or to be transmitted is desirable.

Thus, there is still a need for improving of flow identification (FI) in communications networks, in particular, in heterogeneous environments of communications networks comprising a multitude of wireless access systems.

SUMMARY OF THE INVENTION

Object of the present invention is improving of flow identification in communications networks by means of efficient and flexible network support.

This object is achieved by a network entity comprising features according to claim 1, a method comprising features according to claim 12, a computer program product comprising features according to claim 13, a data carrier comprising features according to claim 14, a network entity comprising features according to claim 15, a method comprising features according to claim 16, a computer program product comprising features according to claim 17, and a data carrier comprising features according to claim 18.

Further embodiments of the present invention are provided with the corresponding dependent claims.

The object of the present invention is achieved by a network entity, comprising a data processing module configured to:

- transmit a flow identifier to a second entity of said communications network, said second entity being configured to determine a flow filter data based on said flow identifier;

- receive a flow filter data from said second entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and

- provide said flow filter data for identification of traffic flows in said communications network.

In this way, a flexible, efficient, and resource saving way of flow identification is enabled by the present invention. In particular, by use of the data processing module, a module configured for performing flow identification (in following referred to as flow identification module) is unloaded with

regard to plurality of tasks to be performed by the module when performing the flow identification. The data processing module performs configuration of the flow identification module with regard to several ways of routing data in the communications network, and the flow identification module gets more free capacities for performing further tasks and/or for supporting more than one flow identification scheme and/or simply for saving its resources. Thus, also use sophisticated flow identification schemes is enabled by the present invention without requiring too much resources. Moreover, also performance of flow identification is improved according to the present invention. The data processing module enables a flexible, comprehensive, and effective supporting of flow identification. The flow identification supported by the data processing module becomes more flexible, powerful, flow identification scheme independent (i.e., independent from use of only some preset flow identification schemes), and uses at the same time always current information for routing of data in the communications network.

As regards the terms used, a flow identifier is an identifier representing a set of instructions that describe a (traffic) flow in the communications network. Flow filter data, in turn, represents a set of conditions (e.g., parameters, values, ranges, patterns, pattern strings, etc) used to identify one or more of traffic flows for handling or routing of data in the communications network. Flow identification refers to identification of traffic flows for data received or to be transmitted in the communications network, wherein the identification is performed based on the flow filter data. In particular, it is checked whether the data received or to be transmitted corresponds to the conditions of the flow filter data. Based on the identified flow, further handling or routing of the data is performed.

According to an embodiment of the present invention, said network entity comprises the flow identification module configured to identify a traffic flow of said communications

network for data to be transmitted by use said flow filter data and to route said data by use of said traffic flow. Here, said data processing module is configured to provide said flow filter data to said flow identification module. In this way, the data processing module performs configuration of the flow identification module directly with current flow filter data.

According to an embodiment of the present invention, said flow identification module is configured to integrate said flow filter data into a flow identification scheme and to identify said traffic flow by use of said flow identification scheme. In this way, the data processing module performs a configuration of the flow identification module, which is independent of the flow identification scheme implemented and used by the flow identification module. It has to be pointed out, that the flow identification module can be configured to use more than one flow identification scheme for identification of flows.

According to an embodiment of the present invention, said data processing module is further configured to provide a flow steering command for identification of traffic flows in said communications network, wherein said flow steering command is related to said flow identifier.

According to an embodiment of the present invention, said flow identification module is configured to identify said traffic flow also by use of said flow steering command. Here, the flow steering command defines the further handling or routing of data (received or to be transmitted) in communications network if the conditions defined by the flow filter data and determined by the flow identifier apply to the data.

According to an embodiment of the present invention, said flow identification module is configured to integrate said flow filter data and said flow steering command into a flow

identification scheme and to identify said traffic flow by use of said flow identification scheme.

According to an embodiment of the present invention, said data processing module configured to receive said flow identifier, said flow identifier being provided by a third entity of a communications network.

According to an embodiment of the present invention, said data processing module is configured to receive said flow steering command, said flow steering command being provided by said third entity of said communications network.

According to a further embodiment of the present invention, said network entity comprises a receiver configured to receive said flow identifier from said second entity of said communications network.

According to an embodiment of the present invention, said receiver is configured to receive said flow steering command from said second entity of said communications network.

According to an embodiment of the present invention, said network entity is a user equipment or a module arranged in a user equipment.

The object of the present invention is achieved also by a method, comprising:

- transmitting of a flow identifier to an entity of said communications network, said entity being configured to determine a flow filter data based on said flow identifier;

- receiving of a flow filter data from said entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and

- providing of said flow filter data for identification of traffic flows in said communications network.

This method is performed at or by the network entity sketched above and described in more detail below. According to an embodiment of the present invention, the network entity performing said method is a user equipment or a module arranged in a user equipment.

Further, the object of the present invention is achieved by a computer program product comprising a code, the code being configured to implement and/or perform said method.

According to an embodiment of the present invention, the code is embodied on a data carrier. According to a further embodiment of the present invention, the computer program product is configured to perform said method when the computer program product is executed by a processing unit like a processor, for example.

Moreover, the object of the present invention is achieved by a data carrier comprising said computer program product.

The object of the present invention is achieved also by a network entity, comprising:

- a receiving module configured to receive a flow identifier from a user equipment;

- a data processing module configured to determine a flow filter data based on said flow identifier; and

- a transmitting module configured to transmit said flow filter data to said user equipment.

Here, said network entity can be a component of a communications network or a module of said component.

Further, the object of the present invention is achieved by a method, comprising:

- receiving of a flow identifier from a user equipment;

- determining of a flow filter data based on said flow identifier; and

- transmitting of said flow filter data to said user equipment.

This method is performed at or by the network entity sketched above and described in more detail below. According to an embodiment of the present invention, the network entity performing said method is a component of the communications network or a module of said component.

Furthermore, the object of the present invention is achieved by a computer program product comprising a code, the code being configured to implement and/or perform said method.

According to an embodiment of the present invention, the code is embodied on a data carrier. According to a further embodiment of the present invention, the computer program product is configured to perform said method when the computer program product is executed by a processing unit like a processor, for example.

Additionally, the object of the present invention is achieved by a data carrier comprising said computer program product.

Thus, the present invention refers to supporting of flow identification in a communications network, within scope of which a first network entity is provided, which comprises a data processing module configured to: transmit a flow identifier to a second entity of said communications network, said second entity being configured to determine a flow filter data based on said flow identifier; receive a flow filter

data from said second entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and provide said flow filter data for identification of traffic flows in said communications network. The second network entity, in turn, comprises: a receiving module configured to receive a flow identifier from the first network entity; a data processing module configured to determine a flow filter data based on said flow identifier; and a transmitting module configured to transmit said flow filter data to said first network entity.

In this way, the present invention enables a flexible, effective, and powerful supporting of flow identification in the communications network, which in turn leads to a flexible, effective, and powerful flow identification itself.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more clearly understood from the following description of the preferred embodiments of the invention read in conjunction with the attached drawings, in which:

Fig. 1 shows a mobile node or UE respectively in a heterogeneous environment of a communications network in which the present invention can be implemented;

Fig. 2 shows network entities configured according to an embodiment of the present invention;

Fig. 3 shows supporting of flow identification according to an embodiment of the present invention;

Fig. 4 shows the architecture of the present invention according to an embodiment of the present invention;

Fig. 5 shows the architecture of the present invention provided and incorporated into 3GPP EPS (Evolved Packet Sys-

tem) architecture according to an embodiment of the present invention;

Fig. 6 shows implementation of the present invention according to an embodiment of the present invention;

Fig. 7 shows implementation of the present invention according to an embodiment of the present invention;

Fig. 8 shows implementation of the present invention according to an embodiment of the present invention;

Fig. 9 shows implementation of the present invention according to an embodiment of the present invention; and

Fig. 10 shows implementation of the present invention according to an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 shows a mobile node or UE 10 respectively in a heterogeneous environment 1 of a communications network in which the present invention can be implemented.

In Fig. 1, a mobile node 10 or UE respectively has two access networks 11 and 12 like LTE (Long Term Evolution) or WLAN (Wireless Local Area Network), for example, in the communications network. The access networks 11, 12 are such parts of the communications network, which connect the mobile node or UE 10 to its immediate service provider, to which data to be transmitted by the mobile node or UE 10 is directed or from which data is received at the mobile node or UE 10.

Heterogeneity or heterogeneous environment 1 of a communications network, as used within the scope of the present invention, means a communications network environment with multiple access networks 11, 12, the multiple access networks 11, 12 having same or different access technologies. Here, it can

be distinguished, e.g., between 3GPP and non-3GPP accesses like LTE or WLAN, for example. Each mobile node or UE 10 can be connected to at least some (at least one or two) of the multiple access networks 11, 12. Further, the number of the access networks 11, 12 is not limited by the present invention. Additionally, the present invention can be applied with regard to different kinds of access networks 11, 12.

When deciding for a certain data, to be transmitted from the mobile node or UE 10 or received at the mobile node or UE 10, by use of which traffic way or which access network 11, 12 this data should be routed in the communications network from the mobile node or UE 10, several kinds of FI schemes can be used. In particular, according to the present embodiment, the mobile node or UE 10 comprises a corresponding FI device or module configured for identification of traffic flows in the communications network. The FI device or module uses at least one FI scheme to identify the appropriate traffic way in dependence of, e.g., contents and/or kind of data.

In following, three FI schemes are sketched exemplary. However, it has to be noted that the present invention is not restricted to these FI schemes only. According to the present invention, several FI schemes can be used. In particular, the use of sophisticated FI schemes is supported according to the present invention in a flexible, efficient, and resource saving way.

According to a known (sophisticated) FI scheme, FI through port numbers are used in TCP/UDP (Transmission Control Protocol / User Datagram Protocol) communications to name the ends of logical connections involved in data transfer. Distinct port numbers are used by servers to provide different services to their clients - mobile nodes or UEs 10. Therefore, by looking at contact port number of a packet it is possible to guess about the service and, hence, the traffic flow to which that packet belongs. Port numbers range from 0 to

65.535 both for UDP and TCP communications. Here, port numbers can be divided into following three ranges:

- Well Known Ports: Well known ports have been assigned by IANA (Internet Assigned Numbers Authority) and range from 0 to 1.023. Most of the legacy applications like email, www, FTP (File Transfer Protocol), and/or SSH (Secure Shell Protocol), for example, contact to their respective servers at port numbers that fall into this range. Therefore, traffic flows consisting of packets going and/or coming to a well known port number can be identified with sufficient accuracy.

- Registered Ports: Registered ports are in the range from 1.024 to 49.151 and can be registered to a certain protocols by software companies like domain name registration, for example. Examples of applications with registered port numbers include Sun's NEO Object Request Broker (port numbers 1.047 and 1.048) and Shockwave (port number 1.626).

- Dynamic/Private Ports: These ports range from 49.152 to 65.535. They are not permanently assigned to any publicly defined application and, therefore, can be used by any user for communication over TCP/UDP without registration requirements.

However, it should be noted that these port assignments by IANA are only recommendations and are not enforced. Therefore, sometimes ports might be used for applications and/or protocols being different from those designated officially by IANA.

According to a further known (sophisticated) FI scheme, which can be used when implementing and performing the methodology of the present invention, Deep Packet Inspection (DPI) devices examine packet contents (i.e., payload) rather than just inspecting the header portion of a packet. DPI can help to get hints how packets should be routed towards the destination. DPI devices are configured to identify packet flows,

allowing control actions to be based on accumulated flow information (rather than packet-by-packet analysis).

DPI uses following three types of identification technologies:

- Signature Matching - usually protocols have distinct fingerprints that can be used to identify a traffic flow belonging to a particular application. The fingerprints may be a special port, string, or bit sequence. These fingerprints are collected in a first stage from RFCs (Remote Function Calls), public documents, or by reverse engineering and empirically deriving a set of distinct bit strings by monitoring protocols. Signature matching can be divided into three tributary technologies: signature matching in a fixed position, signature matching in changing positions, and signature matching at a particular state of communication.

Once a database of fingerprints is built up, protocol's signature matching is performed by inspecting packet contents and/or header.

- Application Layer Gateway Identification - in some services control flows (control plane signalling) are separated from service flows (user plane signalling). Therefore, such user plane traffic has no characteristic based on which it can be identified. Application layer gateway identification technology is targeted for such service types. According to this technology, the control flow is identified at first and parsed. Then, a specific application layer gateway is selected to inspect corresponding service flow(s) based on control flow protocol information.

For example, SIP (Session Initiation Protocol) and H323 protocol communications can be identified by use of this technique. Both of these protocols exchange control plane signalling before acquiring data (i.e., user plane) channels. Further, data channels are always voice flows encapsulated in

RTP (Real-time Transport Protocol) format. However, only inspecting RTP flow cannot give any information about protocol used to setup the flow. Therefore, complete analysis requires inspection of SIP and H323 protocol signalling by distinct application gateways.

- Behaviour Pattern Identification - this identification technology requires a prior study of behaviour of mobile devices or UEs respectively and/or corresponding protocols used for communication in order to setup a behaviour pattern identification model. This model can help to judge previous or prior actions and/or subsequent or following actions of the user of a mobile node or UE respectively. The technology of Behaviour Pattern Identification is used particularly in cases in which the FI identification cannot be performed or cannot be performed successfully by use of protocols and/or above outlined flow identification technology.

Thus, for example, according to a protocol and contents of data, received or to be transmitted, an ordinary email is not different from a spam email. However, in terms of sending frequency, destination addresses, source addresses, and/or frequency of rejection a spam email has behaviour which is different from the behaviour of an ordinary email.

The three identification technologies of DPI as sketched above are applicable to different types of protocols used for communication and cannot replace each other.

Deploying a DPI device or machine in a mobile node or UE for uplink traffic (and in the network for downlink traffic) realizes the service detection and service control as relevant for "SbH (service based handover) -like" services being relevant for FI. When considering service detection in mobile nodes or UEs respectively (in particular, in mobile nodes or UEs to be developed and provided in future), within the scope of the present invention it is necessary to detect services activated by operators and services activated by users and so

"only" to be monitored by the operator. The former can be identified, e.g., by the IP (Internet Protocol) 5 tuplets of the service flow, the latter uses the outlined DPI technologies and gets the type of the service flow by analyzing the content of the IP data packets, finding out the signature, and making statistics of service-related behaviour. Thus, for example, after service detection has been performed, "SbH-like" functions control service flows, e.g., IP flows are directed via dedicated access networks (in the downlink) and via dedicated radio interfaces (in the uplink) based on their own mechanisms of making decisions.

A further known (sophisticated) FI scheme is the statistical signature-based FI. According to the statistical signature-based FI, at first stage, statistics from pre-existent traffic flows, which serve as training data for communication, are collected. These statistics include information about server IP address, server port, inter-arrival time and/or packet length mean and variance, flow size (e.g., in bytes) and/or transmission duration etc. Once these statistics are collected, classification of each flow based on available statistics is performed in a next step or phase. This classification results in a set of statistical signatures comprising at least one statistical signature per traffic flow. These statistical signatures can be used later in the process of FI in real communications networks.

The statistical signature-based FI scheme is more suitable for identification and classification of a set of flows, which belong to the same class of service or QoS (Quality of Service) requirements. In particular, the statistical signature-based FI scheme can be considered as valuable for 3GPP networks.

Yet another known (sophisticated) methodology, which also can be used for FI according to the present invention, is direct interface to applications. The direct interface to applications is a basic approach, in which an application informs

about the commencement of a at least one flow. When a mobile node or UE respectively wants to start a communication session, the application will request for a connection. This request will result in the operating system (e.g. Symbian OS) of the mobile node or UE initiating the connection. Once the connection is established, the application will start sending and/or receiving of data.

This concept can be used in particular to determine the flows when the application starts. According to an embodiment, before sending of data the application informs the "SbH-like" functions that a certain flow is to commence. Then, a corresponding "SbH-like" functional entity configured to perform the "SbH-like" functions sets appropriate "SbH-related" settings. Once the settings are done, the application can be informed to commence the flows.

Fig. 2 shows network entities configured according to an embodiment of the present invention.

The mobile node or UE 10 comprises a receiver or flow steering module 101 which is configured to exchange 23 flow steering commands and flow identifiers related to the flow steering commands. According to the present embodiment the receiver or flow steering module 101 is configured to exchange 23 this data with and, in particular, to receive 23 this data from a PCRF (Policy Control and Charging Rules Function) entity 20. In particular, the PCRF 20 comprises a corresponding data providing module 201 for providing the flow steering commands and flow identifiers to the mobile node or UE 10.

The data providing module can be, for example, a SbH agent and/or a decision engine. In case, the data providing module 201 is a SbH agent, the receiver or flow steering module 101 of the mobile node or UE 10 can be a SbH client.

In following, the present embodiment will be explained in context of service based handover (SbH). However, the present

invention is not restricted to this context only and can be implemented and used also within scope of further contexts of communications networks.

Before continuing explaining of the embodiment of Fig. 2, a brief description of the overall context of service based handover (SbH), used for the present embodiment, is explained in short in following.

In the context of 3GPP, a handover in general switches the complete communication (i.e., all traffic flows) between available accesses (i.e., here from 3GPP to non-3GPP access, or vice versa, or between non-3GPP accesses, for example). Within the present embodiment a potential application (or network function) utilizing the present invention according to the present embodiment is the SbH, which basically enhances mobility with a finer granularity, meaning that not all traffic flows (e.g., internet protocol (IP) traffic flows) are switched but just a distinct number of the traffic flows (e.g., as outcome of SbH decision making in a Policy Decision Point (PDP)). Inherent for directing (IP) traffic flows is of course (IP) FI in the communications network as well as in the mobile node or UE 10. If an (IP) flow is identified, functions like SbH steer routing of IP packets, for example, are made according to their decisions. Sophisticated FI mechanisms, as introduced above, differentiate services and flows at the application layer and further apply decisions from SbH on to be used accesses per flow.

SbH enhances mobility of a mobile node or UE 10 between accesses 11, 12, available in parallel, with a finer granularity. In particular, SbH directs individual (IP) traffic flows as decided in some decision point extended by the SbH agent 201 on network side (in case of network-controlled operation mode). Finally, (IP) flow steering in uplink and downlink is realized via communication between the SbH agent 201 and SbH client 101, provided in mobile node or UE 10, via some flow filters (e.g., mandating of video traffic via WLAN as one

available access and voice traffic via LTE as a further available access). Consequently, FI devices in the uplink are located in mobile nodes or UEs 10, whereas in downlink FI devices are located in the communications network. For steering of (IP) traffic flows, SbH uses these identification mechanisms to differentiate service (and its individual flows) at the application layer and further apply its decisions on to be used accesses per individual flow.

At this point, it has to be noted that SbH bases on an IETF flow management mechanism (as presented, e.g., by H. Soliman, N. Montavont, N. Fikouras, and K. Kuladinithi in "Flow Bindings in Mobile IPv6 and Nemo Basic Support", draft-soliman-monami6-flow-binding-04.txt, February, 2007) steering traffic to multiple, simultaneously available communications network (and mobile device) interfaces (see, e.g., Mastering Heterogeneous Networks (MHN) project, J. Tervonen (ed.), MHN System Architecture, v.1.0.0, June 2008; or Mastering Heterogeneous Networks (MHN) project, F. Pittmann (ed.), MHN System Specification, v.0.4.0, September 2008).

Further, according to the present embodiment, the PCC (Policy and Charging Control) architecture and its functions are extended to support SbH, e.g., via extended dynamic and predefined PCC rules which are configured for steering of (IP) traffic flows (or so-called Service Data Flows (SDFs)).

In particular, the PCC architecture is configured to discard packets that do not match any service data flow filter of active PCC rules. Further, for the operator it is allowed to define PCC rules with wild-carded service data flow filters, to allow for the passage and charging for packets that do not match any service data flow filter of any other active PCC rules.

Here, it is distinguished between dynamic PCC rules and predefined PCC rules. A dynamic PCC rule is a PCC rule for which the definition is provided into the PCEF (Policy and Charging

Enforcement Function) via the Gx reference point. In Fig. 2, the PCEF entity of the communications network has the reference number 22 and is configured to receive 29 the dynamic PCC rules from the PCRF entity 20, in particular, from the SbH agent 201. The pre-defined PCC rule, in turn, is a PCC rule that has been provisioned directly into the PCEF entity 22 by the operator. According to Fig. 2, the PCEF entity 22 is configured to receive 28 the pre-defined PCC rules provided by the operator. Further, the PCEF entity 22 comprises a FI device 221 for the downlink 26 in the communications network. Here, it has to be noted that the PCC rule represents in general a set of information enabling detection of a service data flow and providing parameters for policy control and/or charging control.

As standardized today, dynamic PCC rules do flow identification using IP 5 tuplets and pre-defined PCC rules may be used to support other, more sophisticated identification mechanisms (see, e.g., 3GPP TS 23.203 V8.3.1 (2008-09), Policy and charging control architecture (Release 8)).

According to the present embodiment, (radio and network) bearers in the transport layers are established via several, parallel wireless accesses based on PCC rules processing; the negotiation of IP flow filters to steer traffic in uplink 27 as well as in downlink 26 is done between the SbH agent 201 and the SbH client 101. Thus, when considering the embodiment of Fig. 2, SbH directs individual (IP) traffic flows as decided in some decision point (e.g., decision engine) extended by SbH agent 201 on network side. Thus, flow steering commands and corresponding flow identifiers are exchanged 23 between the SbH agent 201 and the SbH client 101, wherein each flow steering command is related to a flow identifier.

Here, for example, a command "Drop" and the corresponding identifier "ID-Terror#1" are provided by the SbH agent 201 to the SbH client 101. With regard to this example, it is intended to drop (discard) all traffic flows originating from

the mobile node or UE 10 in that (IP) packets match with one or more patterns linked with the identifier "ID-Terror#1".

The receiver or flow steering module 101 comprised in the mobile node or UE 10 is configured to provide 104 the flow steering commands and the corresponding flow identifiers to a data processing module 102 of the mobile node or UE 10. According to the present embodiment, the data processing module 102 is an IPFISF (IP Flow Identification Support Function) client.

The IPFISF client 102 resolves received identifier(s) to receive FI device 103 configuration data suitable for implemented FI scheme(s) on the mobile node or UE 10.

When considering the above provided example, for the identifier "ID-Terror#1" flow filters {“dicky.ohaareee”, “d.ohaareee”, “theTeeerr”} could be provided, for example. Here, it is assumed that some authorities requesting from network operator to search for these three patterns (the list might be dynamically be extended at some point in time). To derive such patterns, pre-defined PCC rules known by the PCRF 20 can be used on network side for downlink 26 traffic.

In particular, according to the present embodiment, the IPFISF client 102 provides 24 the flow identifier(s) to the IPFISF agent 21 located on the communications network side. The receiving module 211 of the IPFISF agent 21 receives the flow identifier(s). The data processing module 212 determines flow filter data based on the flow identifier(s) received by the receiving module 212. The transmitting module 213 of the IPFISF agent 21, in turn, transmits 25 the flow filter data determined by the data processing module 212 to the mobile node or UE 10, wherein the flow filter data is received by or provided to the IPFISF client 102 on the side of the mobile node or UE 10.

The IPFISF client 102 provides 105 then the flow filter data and the corresponding command(s) to the FI device 103. In particular, the IPFISF client 102 configures FI device 103 (e.g., with Deep Packet Inspection (DPI) FI scheme and pattern identification technology, both sketched above) with received filter data or three patterns respectively and the corresponding flow steering command(s).

When considering the example provided above, the IPFISF client 102 configures 105 the FI device 103 by use of the command "Drop" and the flow filter data or patterns {“dicky.ohaareee”, “d.ohaareee”, “theTeeerr”}. The FI device 103 discards, then, in the downlink 26 all packets belonging to (IP) traffic flow(s) in which at least one of these patterns is recognized. Here, it has to be noted that several ways of handling of data is possible. The above provided discarding represents just an example. The concrete way of handling of data, meeting the conditions defined by the flow filter data or patterns respectively, is pre-determined by the command specified by the corresponding flow filter data or patterns respectively.

Further, the FI device 103 can handle in an appropriate way also packets or data to be transmitted (i.e., data of the uplink 27) and comprising at least one of these patterns. E.g., this data can be discarded or provided to a service point handling packets or data with such patterns. As pointed out above, also here, several ways of handling of data is possible. Also here the concrete way of handling of data, meeting the conditions defined by the flow filter data or patterns respectively, is pre-determined by the command specified by the corresponding flow filter data or patterns respectively.

Fig. 3 shows an embodiment of the present invention, in which the user 10 is at home and where both 3GPP access 32 and a trusted or untrusted non-3GPP access 31 are available. The non-3GPP access 31 can be a domestic WiFi hotspot, for example. The user 10 is accessing different services with differ-

ent characteristics in terms of QoS requirements, bandwidth and charging:

- a Video Telephony call;

- a media file synchronization (e.g. a podcast and downloading of TV series); and

- a p2p download.

Based on operator's policies, the user's preferences, the characteristics of the application, and/or the accesses, the (IP) traffic flows are routed differently according to the present embodiment. Thus, for example, the audio media (e.g., conversational voice) of the VT call is routed via 3GPP access 32 by use of traffic flow 34, while the video media (e.g., conversational video or live streaming) of the VT, the p2p download (best effort), and media file synchronization are routed through the non-3GPP access 31. Here, the video media is routed by use of the traffic flow 37, the p2p download is routed by use of the traffic flow 38, and the media file synchronization is routed by use of the traffic flow 39. All of the flows lead, according to the present embodiment, through 3GPP EPC 33.

According to the present embodiment, the FI is supported also in scenarios where dynamic and/or private ports, which range from 49.152 to 65.535, are used by applications. Such ports are not permanently assigned to any publicly defined application and therefore can be used by any user for communication over TCP/UDP without registration requirements.

According to the present embodiment, from network operator' perspective, a data base located in the network (can be co-located with IPFISF agent 21, for example) can provide a flexible solution, if efficiently accessed by the mobile node or UE 10 (i.e., IPFISF client 101 on the mobile node or UE 10) on demand (in contrast to pushing the ports to all mobile

nodes or UEs 10 regardless whether to be used or not). Such a data base is then configured to manage and provide flow filter data. In following the data base will be referred to also as flow filter data base. The provision of the flow filter data can be performed by use of flow identifiers transmitted to the IPFISF agent 21 by the IPFISF client 102 and subsequently transmitted by the IPFISF agent 21 to this flow filter data base. The interface between such a data base and IPFISF agent 21 can be implemented, e.g., with standard protocols like Lightweight Directory Access Protocol (LDAP) etc., for example. The IPFISF agent 21 is then configured to request the data base for the flow filter data by use of the flow identifiers and to receive the flow filter data, corresponding to the flow identifiers comprised in the requests and determined by the data base by use of the flow identifiers, from the data base. Here, several ways of deriving of flow filter data from the data base are possible according to the present invention.

Fig. 4 shows the architecture of the present invention according to an embodiment of the present invention.

In general, the present invention as shown in the present embodiment allows flexible and efficient flow identification (FI) in the mobile node or UE 10, particularly for uplink traffic, by utilizing at least one FI scheme, in particular, at least one sophisticated FI scheme as sketched above. According to the present invention as shown in the present embodiment an additional IPFISF layer 43 is introduced, which is configured to

- resolve flow identifiers and, hence, to provide flow filters to the mobile node or UE 10;

- provide resources in the network on behalf of the mobile node or UE 10;

- control FI device's configuration data maintenance in the network on behalf of the mobile node or UE 10.

Implementing of the IPFISF architecture according to the present embodiment intends to gain at least the following advantages:

- providing necessary information to the mobile node or UE 10 in a quite flexible manner; and/or

- introducing efficiency by shifting scarce resources from the mobile node or UE 10 to the communications network.

Consequently, the IPFISF architecture provided according to the present embodiment separates tasks to reach the efficiency and flexibility mentioned above. In particular, the separation of the tasks is enabled by the following three layers of the IPFISF architecture provided according to the present embodiment.

The first layer is the FI layer. Here, the FI device (implementing one or more FI schemes) provided in the mobile node or UE 10 identifies IP flows by use of received FI device specific configuration data. Here, the FI device of the mobile node or UE 10 can look at transport protocol (e.g., TCP/UDP) ports, IP header information, and/or the payload.

The second layer is the IPFISF layer. Here, properties of the mobile node or UE 10 (i.e., resources and FI scheme(s)) are considered by:

(i) resolving received dedicated flow identifiers;

(ii) potentially, if necessary, triggering flow analysis and flow filter maintenance in the network;

(iii) and, hence, using resources provided by the network.

When resolving the received dedicated flow identifiers, FI device's configuration data, suitable for FI scheme(s) implemented on the mobile node or UE 10, are provided via communication of the mobile node or UE 10 with the communications network.

The third layer is the control layer or, here, (IP) traffic flow steering layer. The granularity here is on service (application) level and its constituting (IP) traffic flow(s). I.e., this third layer focuses on steering and/or guiding of the (IP) traffic flows via dedicated access points without being aware or utilizing knowledge of properties of the mobile node or UE 10 like implemented FI scheme(s), for example. The individual (IP) traffic flow(s) are identified by means of dedicated identifiers. Hence, FI-related identity management solely implemented and performed in this third layer.

Also according to the present embodiment, in the architecture of the present invention the network function Service-based Handover (SbH) is used exemplary to highlight the advantages of the present invention in a more clear way. Hence, existing FI schemes relevant for SbH, such as briefly introduced above, are used according to the present embodiment. Here, it has to be pointed out, that the architecture of the present invention is not restricted to the network function SbH and/or the finally chosen FI scheme only. The present invention can be applied in several contexts and can use several FI schemes.

Due to resource limitations of mobile nodes or UEs respectively and due to high resource consumption by conventional methodologies enabling or supporting FI, the conventional mobile devices or UEs respectively do not support every FI scheme. However, the present invention allows deployment of sophisticated FI schemes that are chosen out of a variety of schemes addressing dedicated needs and intentions of, e.g., network operators or regulatory bodies (e.g., to prevent

spamming, prevent proliferation of pornographically material or "terror-suspect" communication etc.).

According to the present embodiment, a new reference point (RP) 42 is provided which is referred to as S20 in following. This RP 42 resides between the IPFISF level 43 and the mobile node or UE 10, wherein the mobile node or UE is connected to two access points 41 according to the present embodiment. According to the present embodiment, the two access points 41 are the 3GPP IP Access and the non-3GPP IP Access, which can be a trusted or un-trusted non-3GPP IP Access. Further, the architecture according to the present embodiment provides a further RP - a new interface 44, which allows getting of knowledge of properties of the mobile device or UE 10, in particular, information about the implemented FI scheme(s) for the uplink traffic in communications network. This interface 44 is referred to as S6x in following and is used in the architecture presented in Fig. 4 for mobility services between the IPFISF layer 43 and HSS (Home Subscriber Server) 45, in particular, for (IP) traffic flow mobility services to enable the transfer of subscriber related data, including properties of the mobile device or UE 10 like software versions, supported RAT types, or equipment status, for example. Further, the interface S6x 44 performs the following two new commands according to the present embodiment: 'Update-FI-Device-Request' and 'Update-FI-Device-Answer', which are used to request an update of flow filter data for an existing flow identifier or to request an incorporation of flow filter data for a new flow identifier in IPFISF layer 43 with a corresponding acknowledgement in the answer message.

According to the present embodiment, the reference point or interface S20 42 is specified as follows.

The RP or interface S20 42 resides between the IPFISF 43 and the mobile node or UE 10. The RP or interface S20 42 enables the mobile node or UE 10, in particular, the IPFISF client of the mobile node or UE 10 to resolve the received flow identi-

fiers. In case of unsuccessful resolution, flow analysis and flow filter maintenance is triggered in the network, hence resources are provided by the communications network on behalf of the mobile node or UE 10. At the end, configuration data of the FI device of the mobile node or UE 10, said configuration data being suitable for implemented FI scheme(s) on the mobile node or UE 10, is provided via RP or interface S20 42 to support IP flow mobility commands (as from SbH, for example).

Within this scope, the RP or interface S20 42 supports the following functions according to the present embodiment:

- establishment and termination of S20 session; and

- providing, updating, and removing of flow filters between the IPFISF 43 and the mobile node or UE 10, in particular:

  o requesting for configuration data for the FI device of the mobile node or UE 10 from the mobile device or UE 10 to the IPFISF 43 (Pull mode); and

  o providing of this configuration data from the IPFISF 43 to the mobile node or UE 10 (Push mode).

When considering the IPFISF 43, the IPFISF 43 is configured according to the present embodiment to incorporate information received via the RP or interface S6x 44 into the configuration data for the FI device of the mobile node or UE 10, said configuration data to be provided to the mobile node or UE 10. Hence, IPFISF 43, having knowledge of properties of the mobile node or UE 10 like implemented FI scheme(s), for example, provides to the mobile node or UE 10, by use of this knowledge, all necessary information (i.e., flow filter(s) adequate for the FI device of the mobile node or UE 10) to configure this FI device correctly. The UE can request for FI device configuration data in a Pull mode, or the UE can re-

ceive such data in an unsolicited manner (Push mode). In this way, and considering now the new aspect of FI scheme(s) implemented in FI device or the mobile node or UE 10, the HSS 45 becomes able to address requirements arising out of network support of sophisticated FI scheme(s) on mobile devices or UEs 10 in the context of (IP flow) mobility services of the HSS 45.

Fig. 5 shows the architecture of the present invention provided and incorporated into 3GPP EPS (Evolved Packet System) architecture according to an embodiment of the present invention.

In Fig. 5 the following components or network entities comprised also in the 3GPP EPS architecture are provided: 3GPP access 511 with serving gateway 512; HSS 45 being connected via interface S6a 513 with the 3GPP access 511; PCRF 20 being connected to the serving gateway 512 via the interface Gxc 516; PDN (Public Data Network) gateway 517 being connected to the PCRF 20 via the interface Gx 518 and to the serving gateway 512 via the interface S5 519; 3GPP AAA (Authentication, Authorization and Accounting) Server 515 being connected to the HSS 45 via the interface SWx 514 and to the and to the PDN gateway 517 via the interface S6b 523; Operator's IP Services (e.g., IMS (IP Multimedia Subsystem), PSS, etc) entity 520 being connected to the PCRF 20 via the interface Rx 521 and to the PDN gateway 517 via the interface SGi 522; ePDG 524 connected to the PCRF 20 via the interface Gxb 525 and to the 3GPP AAA server 515 via the interface SWm 526; un-trusted non-3GPP IP access 527 being connected to the ePDG 524 via the interface SWn 528 and to the 3GPP AAA server 515 via the interface SWa 529; the trusted non-3GPP IP access 530 being connected to the PCRF 20 via the interface Gxa 531 and to the 3GPP AAA server 515 via the interface STa 532; the mobile node or UE 10 being connected to the PDN gateway 517 over the un-trusted non-3GPP IP access 527 via the interface S2c 533, over the trusted non-3GPP IP access 530 via the interface S2c

534, and over the serving gateway 512 via the interface S2c 535.

The dashed line 538 in Fig. 5 divides the components or network entities of the architecture, provided according to the present embodiment, in components or network entities of two sub networks: the non-3-GPP network 536, and the HPLMN (Home Public Land Mobile Network) 537.

Further, according to the present embodiment, the architecture comprises the following components or entities explained above with regard to Fig. 4: RP or interface S20 42, the IPFISF 43, and the RP or interface S6x 44.
As regards the PCFR 20, according to the present embodiment the PCRF 20 is extended by some further communications network functions like Service Based Handover (SbH), for example, to steer (IP) traffic flows via SbH communication between the SbH agent 201 (provided in PCRF 20) and the SbH client 101 (provided in the mobile node or UE 10).

As regards the HSS 45, according to the present embodiment the HSS 45 is extended by new commands (or some information elements) that are provided (via the RP or interface S6x 44) for network support of sophisticated FI scheme(s) in the mobile node or UE 10, in particular, in the FI device 103 or the mobile node or UE 10.

For downlink traffic, the flow identification (FI) devices are located according to the present embodiment in PDN gateway 517 and for uplink traffic in the mobile node or UE 10. Further, according to the present embodiment, sophisticated FI schemes beyond simple IP 5 tuplets can be used in the FI devices.

Moreover, according to the present embodiment, subscription data, terminal information etc from HSS 45 is required for IPFISF 43 processing. Here, according to the present embodiment, the RP or interface S6x 44 is provided between the

IPFISF 43 and the HSS 45 as an extension of the already specified S6 interface for HSS 45; currently for EPS Release 8 two new 3GPP applications (for S6a with id 1677251 and S13 with id 1677252) are defined (see, e.g., 3GPP TS 29.272 V8.0.0 (2008-09), EPS; MME and SGSN Related Interfaces Based on Diameter Protocol (Release 8)). In particular, according to the present embodiment, the RP or interface S6x 44 is provided as Diameter based S6 interface (see, e.g., specifications provided in 3GPP TS 29.272 V8.0.0 (2008-09), EPS; MME and SGSN Related Interfaces Based on Diameter Protocol (Release 8)), which is extended or configured to support also information provisioning for FI scheme(s) etc. Here, it has to be noted that also further appropriate realizations of the RP or interface S6x 44 are possible according to the present invention.

Further, according to the present embodiment, the RP or interface S20 42 is provided between the IPFISF 43 and the mobile node or UE 10. According to the present embodiment, the RP or interface S20 42 is realized by utilizing an extended OMA (Open Mobile Alliance) Device Management (DM) protocol. However, also further appropriate realizations of the RP or interface S20 42 are possible according to the present invention.

Additionally, according to the present embodiment, related 3GPP message sequence charts (MSCs) are extended to show the applicability of the proposed architecture.

Thus, in particular when considering the embodiments of Fig. 4 and Fig. 5, a new architecture for layered network support for sophisticated FI scheme(s) in communications networks like 3GPP networks, for example, with a new functional entity IPFISF 43 interfacing to the mobile node or UE 10 (via the RP or interface S20 42) and to the HSS 45 (via the RP or interface S6x 44) is provided according to the present invention, as provided exemplary by the embodiments presented above. Here, the scope and/or functionality of HSS 45 and/or the mo-

bile node or UE 10 is extended towards sophisticated (IP) traffic flow mobility support. Further, in the embodiments provided above, new procedures (MSCs) have been described particularly for the 3GPP deployment.

According to the embodiments of Fig. 4 and Fig. 5, IP flow mobility between 3GPP and non-3GPP accesses is supported. Here, it has to be pointed out that the present invention is applicable also to further accesses and is not restricted to 3GPP and non-3GPP accesses only.

In following, embodiments representing exemplary possible ways of implementation of the present invention are provided in more detail.

Fig. 6 shows implementation of the present invention according to an embodiment of the present invention. Here, MSC for pull operation mode during extended IP-CAN session establishment is implemented.

Fig. 6 shows in particular the MSC for IP-CAN session establishment and IP address assignment to the mobile node UE 10. Also according to embodiment of Fig. 6, network function SbH is considered exemplary to explain the present invention. According to the present embodiment, establishment of a second, in parallel available network connection via an additional access is provided. Hence, after finalizing session establishment FI scheme(s) of the mobile device or UE 10 (provided in the FI device 103) are configured, as described above, and SbH-related signalling addresses (IP) traffic flow mobility issues. IPFISF's 43 HSS 45 interrogation is not depicted in the present embodiment, but it should be done with step 607 if IPFISF 43 has not the necessary information concerning the mobile device or UE 10. When considering the SbH, the handover is done according to the present embodiment per (IP) flow and is supported by the PCRF 20 and the mobile node or UE 10.

According to the present embodiment, MSC focuses on non-roaming scenario. However, according to the present invention the same principles can be applied also to the roaming scenario.

In addition to the entities and components explained above, the present embodiment utilizes also the following entities for implementing the present invention: BBERF (Bearer Binding and Event Reporting Function) entity 61 or gateway respectively, data base 62 configured to manage and provide flow filter data as explained above, SPR (Subscription Profile Repository) entity 63, and OCS (Online Charging System) entity 64.

According to the present embodiment, in step or phase 601, a gateway and control session establishment is performed. Then, in step or phase 602 an IP-CAN bearer request is established, wherein the PCEF 22 receives a request for IP-CAN bearer establishment and wherein subsequently the PCE 61 accepts the request and assigns an IP address for the user or mobile device or UE 10 respectively. Here, with regard to SbH, the IP address assignment for the user refers to a second IP address for the second in parallel available access network.

Further, in step or phase 603 indication of IP-CAN bearer session establishment is performed. In particular, the PCEF 22 determines that the PCC authorization is required, requests the authorization of allowed service(s) and PCC Rules information. The PCEF 22 includes the following information: UE Identity (e.g. MN NAI), a PDN identifier (e.g. APN), the IP-CAN type and the IP address(es) and, if available, the default charging method and the IP-CAN bearer establishment modes supported. The PDN identifier, IP address(es) and UE identity enables identification of the IP-CAN session. The IP-CAN Type identifies the type of access from which the IP-CAN session is established. If the service data flow is tunnelled at the BBERF 61, the PCEF 22 can provide information about the mobility protocol tunnelling encapsulation header

in the message. For the PCC authorization it has to be noted here that the PCC authorization, concerning the authorization of allowed service(s) and PCC Rules information, refers to the second in parallel available access.

In step or phase 604, profile request and response are performed. In particular, if the PCRF 20 does not have the subscriber's subscription related information, it sends a request to the SPR 63 in order to receive the information related to the IP-CAN session. The PCRF 20 provides the subscriber ID and, if applicable, the PDN identifier to the SPR 63. The PCRF 20 may request notifications from the SPR 63 on changes in the subscription information. Subsequently, the PCRF 20 stores the subscription related information containing the information about the allowed service(s) and PCC rules information.

In step or phase 605, policy decision is performed. In particular, the PCRF 20 makes the authorization and policy decision also considering IP flow mobility issues, e.g., as specified for SbH in general.

In step or phase 606 SbH, communication for flow steering and flow identity distribution is performed. Here, a SbH-related signalling between the SbH agent 201 and SbH client 101 may negotiate, e.g., that an additional access will be used for video traffic flow (from originally started video-telephony (VT) application), which was before not possible due to missing access network resources. Consequently, AF (Application Function) interactions may be required and FI schemes supported by that mobile node or UE 10 may need configuration data to address video traffic flow identification, for example.

In step or phase 607 FI scheme signalling is performed (in pull operation mode (optionally)). In particular, the mobile node or UE 10 requests with message FI scheme configuration request necessary information for its sophisticated FI

scheme(s) to be able to enforce, e.g., decisions made by SbH control logic. Then, the IPFISF agent 21 provides requested information to the mobile node or UE 10 following also, e.g., network operator's policies and, not depicted in the Fig. 6, by interrogating HSS if IPFISF has not already UE-related necessary information (via the two new commands for implementing S6x 'Update-FI-Device-Request' and 'Update-FI-Device-Answer'). The provided FI scheme(s) configuration data comprising related flow identification details can comprise, e.g., the following information:

- (variable) port numbers (as recommended by IANA), which can support also dynamic procedures, especially when considering registered/dynamic/private port numbers;

- protocol's fingerprints for DPI in signature matching type; and/or

- pattern in IP packets.

Here it has to be noted that the above provided list of information is an exemplary list and that the present invention is not restricted to this list only.

In step or phase 608, SbH communication acknowledgement is performed. Here, if the provided configuration data for the FI scheme(s) implemented in the mobile node or UE 10 is successfully downloaded to the FI device 103 of the mobile node or UE 10, the SbH communication can be acknowledged.

In step or phase 609, IP-CAN bearer session establishment is acknowledged. Here, the PCRF 20 sends decision(s), including the chosen IP-CAN bearer establishment mode, to the PCEF 22. The gateway or PCEF 22 enforces the decision. The PCRF 20 may provide the default charging method. The message may include the following information: the PCC rules to activate and the event triggers to report. The policy and charging rules allow the enforcement of policy associated with the IP-CAN session.

The event triggers indicate to the PCEF 22 what events must be reported to the PCRF 20. Additionally, the decision(s) of the PCRF 20 include also (IP) traffic flow mobility issues, e.g., such as specified for SbH in general.

In step or phase 610, credit request and response is performed. In particular, if online charging is applicable, and at least one PCC rule was activated, the PCEF 22 shall activate the online charging session, and provide relevant input information for the OCS 64 decision. Depending on operator configuration PCEF 22 may request credit from OCS 64 for each charging key of the activated PCC rules. Further, if online charging is applicable, the OCS 64 provides the possible credit information to the PCEF 22 and may provide re-authorisation triggers for each of the credits.

In step or phase 611, IP-CAN bearer signalling is performed. In particular, if network control applies, establishment of additional IP-CAN bearers can be initiated.

In step or phase 612, IP-CAN bearer response is established. In particular, if at least one PCC rule was successfully activated and if online charging is applicable, credit was not denied by the OCS 64, the gateway or PCEF 22 acknowledges the IP-CAN bearer establishment request.

Here, it has to be noted with regard to the embodiment of Fig. 6 that the principles provided above for the IP-CAN session establishment can be applied also for IP-CAN session termination in a corresponding way.

Fig. 7 shows implementation of the present invention according to a further embodiment of the present invention.

The present embodiment is directed to IP-CAN session modification.

The IP-CAN session modification can be initiated by the gateway or PCEF 22, wherein such modification includes IP-CAN bearer establishment and termination as well as modification if the triggering conditions given to the PCEF 22 are fulfilled. In a potential scenario the network operator modifies its policies, e.g., related to spam emails, hence modifies sophisticated FI schemes via pre-defined PCC rules at concerned PCEF(s) 22 to enforce his intention.

The principles of the present embodiment can be applied also to IP-CAN session modification that is PCRF 20 initiated.

Further, the principles of the present embodiment can be applied also when user's subscription changes, e.g., when saying that non-3GPP IP accesses can now be used for IP flow mobility that are implemented by network services like SbH, for example.

According to the present embodiment, the IP-CAN session modification is initiated by the gateway or PCEF 22. Here, the AF (Application Function) entity 71 may be involved. For example, the AF 71 may be informed about dropping of emails marked as spam.

In the following, MSC focuses on a non-roaming scenario. However, the same principles can be applied to the roaming scenario.

According to the present embodiment, optionally, the AF 71 can provide or revoke service information to the PCRF 20 due to AF 71 session signalling. The AF 71 may subscribe at this point to notification of bearer level events related to the service information. For the PCRF 20 to generate the applicable events, the PCRF 20 can instruct the PCEF 22 to report events related to the corresponding PCC rules. Then, the PCRF 20 stores the service information and responds with an acknowledgement to the AF 71.

In step or phase 701 gateway or PCEF 22 internal decision, e.g., due to modified operator policies is made. In particular, the gateway or PCEF 22 either makes an internal decision or receives a request for IP-CAN session modification. Here, the network operator modifies its policies, e.g., related to spam emails, and hence modifies sophisticated FI schemes via pre-defined PCC rules at concerned PCEF(s) 22 to enforce his intention.

In step or phase 702 indication of IP-CAN session modification is performed. Here, the gateway or PCEF 22 determines that the PCC interaction is required and sends an indication of IP-CAN session modification (e.g., event report, affected PCC Rules) to the PCRF 20 and, if changed, the new IP-CAN bearer establishment modes supported. If there is a limitation or termination of the transmission resources for a PCC rule, the gateway or PCEF 22 reports this to the PCRF 20. Here, it may be no new IP-CAN bearer establishment modes to be supported, but affected PCC rules are in the context of the present embodiment valuable information when it comes to step or phase 704 and, e.g., SbH related decision making.

In step or phase 703, application and/or service information is correlated with IP-CAN session. In particular, the PCRF 20 correlates the request for PCC rules with the IP-CAN session and service information available at the gateway or PCEF 22.

Further, the PCRF 20 may need to report to the AF 71 an event related to the transmission resources if the AF 71 requested it at initial authorisation. The AF 71 acknowledges then the event report and/or responds with the requested information.

In step or phase 704, policy decision is done. Here, the PCRF 20 makes the authorization and policy decision. In particular, the PCRF 20 makes the authorization and policy decision also by considering (IP) flow mobility issues, such as specified for SbH in general, for example.

In step or phase 705, SbH communication for flow steering and flow identity distribution is performed. In particular, SbH-related signalling between the SbH agent 202 and the SbH client 101 may now negotiate, e.g., that an additional access will be used for video traffic flow (from originally started video-telephony (VT) application), which was before not possible due to missing access network resources. Consequently, AF 71 interactions may be required now and FI schemes supported by that mobile node or UE 101 may need configuration data to address video traffic flow identification, for example.

In step or phase 706, FI scheme signalling is performed (e.g., in pull operation mode). In particular, the mobile node or UE 10 requests with message FI scheme configuration request necessary information for its sophisticated FI scheme(s) to be able to enforce decisions made, e.g., by SbH control logic. The IPFISF 21 provides then the requested information to the mobile node or UE 10 following also, e.g., network operator's policies and, not depicted in the figure, by interrogating HSS if IPFISF 21 has not already UE-related necessary information (via commands for implementing S6x 'Update-FI-Device-Request' and 'Update-FI-Device-Answer'). For provided FI scheme(s) configuration data about related flow identification details it is referred to steps or phases 606 to 608 of Fig. 6.

In step or phase 707, SbH communication acknowledgement is performed. In particular, if the provided FI scheme(s) configuration data is successfully downloaded to the FI device 103 of the mobile node or UE 10, SbH communication can be acknowledged.

In step or phase 708, IP-CAN session modification is acknowledged. Here, the PCRF 20 sends an acknowledgement of IP-CAN session modification (e.g., PCC rules, event triggers and, if changed, the chosen IP-CAN bearer establishment mode) to the gateway or PCEF 22. The gateway or PCEF 22 enforces then the

decision. In particular, the gateway or PCEF 22 enforces the decision also if it comes to IP flow mobility.

In step or phase 709, credit request and response is performed. Here, if online charging is applicable, the gateway or PCEF 22 may request credit for new charging keys from and/or shall issue final reports and return remaining credit for charging keys no longer active to the OCS 64. If OCS 64 was contacted, the OCS 64 provides the credit information to the gateway or PCEF 22, and/or acknowledges the credit report.

In step or phase 710, IP-CAN session signalling is performed. In particular, the gateway or PCEF 22 acknowledges or rejects any IP-CAN Session signalling received in step 701. An IP-CAN bearer establishment or modification is accepted if at least one PCC rule is active for the IP-CAN bearer and in case of online charging credit was not denied by the OCS 64. Otherwise, the IP-CAN bearer establishment or modification is rejected. An IP-CAN bearer termination is acknowledged by the gateway or PCEF 22. An IP-CAN bearer modification not upgrading the QoS and not providing traffic mapping information is acknowledged by the gateway or PCEF 22. In case of a gateway or PCEF 22 internal decision the gateway or PCEF 22 initiates any additional IP-CAN session signalling required for completion of the IP-CAN session modification. Finally, the gateway or PCEF 22 receives the response for the IP-CAN session signalling request.

In step or phase 711, provision acknowledgement is performed. In particular, the gateway or PCEF 22 sends a provision ack (accept or reject of the PCC rule operation(s)) to inform the PCRF 20 about the outcome of the gateway or PCEF 22 actions related to the decision(s) received in step 708.

In step or phase 712, gateway control and QoS rules provision is performed. Here, the PCRF 20 initiates a gateway control

and QoS rules provision procedure, if required, to keep the PCC and QoS rules aligned.

In step or phase 713, notification of bearer level event level events and acknowledgement is performed. In particular, if the AF 71 requested it, the PCRF 20 notifies the AF 71 of related bearer level events (e.g. transmission resources are established/released/lost). Based on the outcome reported in this step the AF 71 can perform the appropriate action, e.g. starting charging or terminating the AF 71 session. Finally, the AF 71 acknowledges the notification from the PCRF 20.

Within the scope of the present embodiment the SbH is done per (IP) flow and supported by the PCRF 20 and the mobile node or UE 10.

Further, the principles of the present embodiment can be applied also when user's subscription changes, e.g., in a scenario saying, for example, that non-3GPP IP accesses can now be used for IP flow mobility that are implemented by network services like SbH, for example.

Fig. 8 shows implementation of the present invention according to another embodiment of the present invention. In particular the implementation is performed with regard to MSC for pull operation mode during update of the subscription information in the PCRF 20.

In step or phase 801, the SPR 63 detects that the related subscription profile of an IP-CAN session has been changed. If requested by the PCRF 20, the SPR 63 notifies the PCRF 20 on the changed profile (assumed in this scenario) and the PCRF 20 stores the updated profile and makes resulting PCC decisions considering also IP flow mobility with SbH as a potential implementation.

In step or phase 802, the PCRF provides all new PCC and/or SbH decisions to the PCEF 22 by utilizing an IP-CAN session modification baseline procedure initiated by PCRF 20.

As regards the following steps or phases 803 to 808, the step or phase 803 corresponds to the steps or phases 702 and 703 of Fig. 7, the step or phase 804 corresponds to the step or phase 704 of Fig. 7, the step or phase 805 corresponds to the step or phase 705 of Fig. 7, the step or phase 806 corresponds to the step or phase 706 of Fig. 7, the step or phase 807 corresponds to the step or phase 707 of Fig. 7, and the step or phase 808 corresponds to the steps or phases 708 to 713 of Fig. 7.

Fig. 9 shows implementation of the present invention according to an embodiment of the present invention. Here, the implementation is performed with regard to MSC for pull operation mode during update of the subscription information in the PCRF 20 and covers cases in which flow filter identifier(s) is (are) unknown (baseline MSC from Fig. 8).

In the present embodiment, the step or phase 901 corresponds to the step or phase 801 of Fig. 8. Further, the step or phase 902 corresponds to the step or phase 803 of Fig. 8, and step or phase 903 corresponds to the step or phase 804 of Fig. 8. The step or phase 904, in turn, corresponds to the step or phase 705 of Fig. 7.

In step or phase 905, FI scheme signalling is performed, particularly for an error case (in a pull operating mode (optionally)). In particular, the mobile node or UE 10 requests with message FI scheme configuration request necessary information for its sophisticated FI scheme(s) to be able to enforce decisions made, e.g., by SbH control logic. Here, the identifier resolution is not successful, since, e.g., identifier is not known in the IPFISF 21 (i.e. in IPFISF agent 210) and/or in the data base for flow data 62. Hence, an error

code is returned to the IPFISF client 102 provided in the mobile node or UE 10.

In step or phase 906, SbH communication negative acknowledgement is performed. Here, since FI scheme(s) configuration is not successful, SbH communication is negative acknowledged.

In step or phase 907, error resolution is performed. In particular, the PCRF or SbH agent 201 alerts for an unknown flow identifier or for unknown flow identifiers. The following procedure is not described in more detail for this step or phase 907, since pre-defined PCC rules allowing maintenance of sophisticated FI schemes in the network can be used. However, this maintenance is extended for flow filter data base 62 so that finally, e.g., unknown flow filters are added or inserted in the data base 62 in case of an alert. Following the error resolution, the PCRF or SbH agent 201 starts again SbH communication with the SbH client 101 provided in the mobile node or UE 10. Here, it has to be pointed out that the present invention does not exclude other error handling procedures like the case that other identifiers are used, for example, without mentioned data base maintenance actions.

As regards the further steps or phases of the present embodiment, the step or phase 908 corresponds to the step or phase 705 of Fig. 7, the step or phase 909 corresponds to the step or phase 706 of Fig. 7, the step or phase 910 corresponds to the step or phase 707 of Fig. 7, and the step or phase 911 corresponds to the step or phase 808 of Fig. 8.

Fig. 10 shows implementation of the present invention according to a further embodiment of the present invention. In particular, the implementation concerns MSC for push operation mode during update of the subscription information in the PCRF 20 in case additional flow filter(s) configured in flow filter data base (baseline MSC from Fig. 8).

Here, the push mode is discussed by starting after complete (successful) MSC of Fig. 8. The point is that patterns or protocol fingerprints or dynamic or private port numbers can be modified or added at any point of time, in particular in step or phase 101_2. Hence, in a running system the IPFISF agent 210 has to check the relevance for concerned mobile nodes or UEs 10 (step or phase 101_3) and in case of relevance the related FI device' configuration data has to be pushed to the mobile node or UE 10 (step or phase 101_4).

The step or phase 10_1 corresponds according to the present embodiment to steps or phases 801 to 808 of Fig. 8.

In step or phase 10_2, (pre-defined) flow filter modification is performed. In step or phase 10_3, relevance for the mobile node or UE 10 is performed. In step or phase 10_4, in turn, FI scheme signalling is performed (e.g., in a push operation mode).

While embodiments and applications of this invention have been shown and described above, it should be apparent to those skilled in the art, that many more modifications (than mentioned above) are possible without departing from the inventive concept described herein. The invention, therefore, is not restricted except in the spirit of the appending claims. Therefore, it is intended that the foregoing detailed description should be regarded as illustrative rather than limiting.

LIST OF REFERENCES:

1	heterogeneous environment of a communications network
10	mobile node or user equipment respectively
11	access network
12	access network
101	flow steering module
102	data processing module
103	FI device
104	providing of data
105	providing of data
20	PCRF entity
201	data providing module
21	IPFISF agent
211	receiving module
212	data processing module
213	transmitting module
22	PCEF entity
221	FI device
23	exchange of data
24	exchange of data
25	exchange of data
26	downlink
27	uplink
28	receiving of pre-defined PCC rules
29	receiving of dynamic PCC rules
31	access network
32	access network
33	3GPP EPC
34	traffic flow
35	traffic flow
36	traffic flow
37	traffic flow
41	access point
42	interface S20
43	IPFISF

44	interface S6x
45	HSS
511	3GPP access
512	serving gateway
513	interface S6a
514	interface SWx
515	3GPP AAA server
516	interface Gxc
517	PDN gateway
518	interface Gx
519	interface S5
520	operators IP services
521	interface Rx
522	interface SGi
523	interface S6b
524	ePDG
525	interface Gxb
526	interface SWm
527	untrusted non-3GPP IP access
528	interface SWn
529	interface Swa
530	trusted non-3GPP IP access
531	interface Gxa
532	interface STa
533	interface S2c
534	interface S2c
535	interface S2c
536	non-3GPP network
537	HPLMN
538	dashed line separating entities of the non-3GPP network and HPLMN
61	gateway BBERF
62	flow filter data base
63	SPR
64	OCS
601	gateway control session establishment
602	establish IP-CAN bearer request

603	indication of IP-CAN bearer session establishment
604	profile request and response
605	policy decision
606	ShH communication for flow steering and flow identity distribution
607	FI scheme signalling
608	SbH communication acknowledgement
609	acknowledge IP-CAN bearer session establishment
610	credit request and response
611	IP-CAN bearer signalling
612	establish IP-CAN bearer response
71	AF
701	gateway (PCEF) internal decision
702	indication of IP-CAN session modification
703	correlate application/service information with IP-CAN session
704	policy decision
705	SbH communication for flow steering and flow identity distribution
706	FI scheme signalling
707	SbH communication acknowledgement
708	acknowledge IP-CAN session modification
709	credit request and response
710	IP-CAN session signalling
711	provision Ack
712	gateway control and QoS rules provision
713	notification of bearer level event level events and Ack
801	PCC decision
802	PCC decision provision
803	steps or phases 702 and 703 of Fig. 7
804	policy decision
805	SbH communication for flow steering and flow identity distribution
806	FI scheme signalling
807	SbH communication acknowledgement
808	steps or phases 708 to 713 of Fig. 7

901	PCC decision
902	steps or phases 702 and 703 of Fig. 7
903	policy decision
904	SbH communication for flow steering and flow identity distribution
905	FI scheme signalling (error case)
906	SbH communication negative acknowledgement
907	error resolution
908	SbH communication for flow steering and flow identity distribution
909	FI scheme signalling
910	SbH communication acknowledgement
911	steps or phases 708 to 713 of Fig. 7
10_1	steps or phases 801 to 808 of Fig. 8
10_2	(pre-defined) flow filter modification
10_3	checking of relevance of UE
10_4	FI scheme signalling

CLAIMS:

1. A network entity, comprising a data processing module configured to:
- transmit a flow identifier to a second entity of a communications network, said second entity being configured to determine a flow filter data based on said flow identifier;
- receive a flow filter data from said second entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and
- provide said flow filter data for identification of traffic flows in said communications network.

2. The network entity according to claim 1, wherein said network entity comprises a flow identification module configured to identify a traffic flow of said communications network for data to be transmitted by use said flow filter data and to route said data by use of said traffic flow, wherein said data processing module is configured to provide said flow filter data to said flow identification module.

3. The network entity according to claim 2, wherein said flow identification module is configured to integrate said flow filter data into a flow identification scheme and to identify said traffic flow by use of said flow identification scheme.

4. The network entity according to at least one of claims 1 to 3, wherein said data processing module is further configured to provide a flow steering command for identification of traffic flows in said communications network, wherein said flow steering command is related to said flow identifier.

5. The network entity according to claim 4, wherein said flow identification module is configured to identify said traffic flow also by use of said flow steering command.

6. The network entity according to claim 5, wherein said flow identification module is configured to integrate said flow

filter data and said flow steering command into a flow identification scheme and to identify said traffic flow by use of said flow identification scheme.

7. The network entity according to at least one of claims 1 to 6, wherein said data processing module configured to receive said flow identifier, said flow identifier being provided by a third entity of a communications network.

8. The network entity according to claim 7, wherein said data processing module is configured to receive said flow steering command, said flow steering command being provided by said third entity of said communications network.

9. The network entity according to at least one of claims 1 to 8, wherein said network entity comprises a receiver configured to receive said flow identifier from said second entity of said communications network.

10. The network entity according to claim 9, wherein said receiver is configured to receive said flow steering command from said second entity of said communications network.

11. The network entity according to at least one of the preceding claims, wherein said network entity is a user equipment or a module arranged in a user equipment.

12. A method, comprising:
- transmitting of a flow identifier to an entity of a communications network, said entity being configured to determine a flow filter data based on said flow identifier;
- receiving of a flow filter data from said entity of said communications network, wherein said flow filter data represents data determined based on said flow identifier; and
- providing of said flow filter data for identification of traffic flows in said communications network.

13. A computer program product comprising a code, the code being configured to implement a method according to claim 12.

14. A data carrier comprising a computer program product according to claim 13.

15. A network entity, comprising:
- a receiving module configured to receive a flow identifier from a user equipment;
- a data processing module configured to determine a flow filter data based on said flow identifier; and
- a transmitting module configured to transmit said flow filter data to said user equipment.

16. A method, comprising:
- receiving of a flow identifier from a user equipment;
- determining of a flow filter data based on said flow identifier; and
- transmitting of said flow filter data to said user equipment.

17. A computer program product comprising a code, the code being configured to implement a method according to claim 16.

18. A data carrier comprising a computer program product according to claim 17.

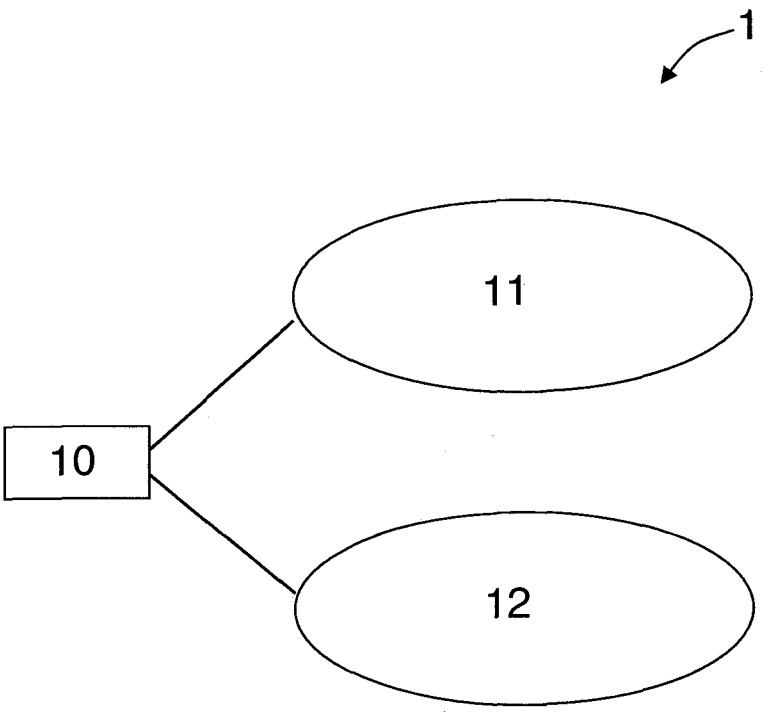

Fig. 1

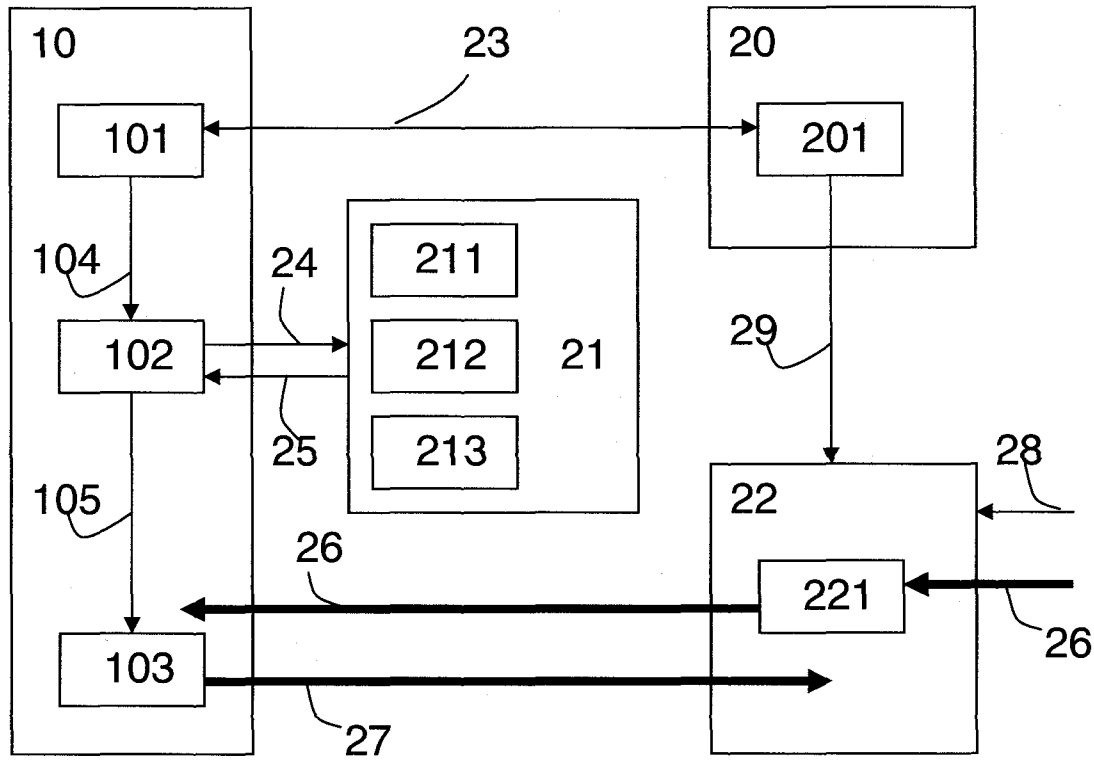
10
23
20
101
201
104
24
211
102
212
21
29
25
213
28
105
22
26
221
26
103
27

Fig. 2

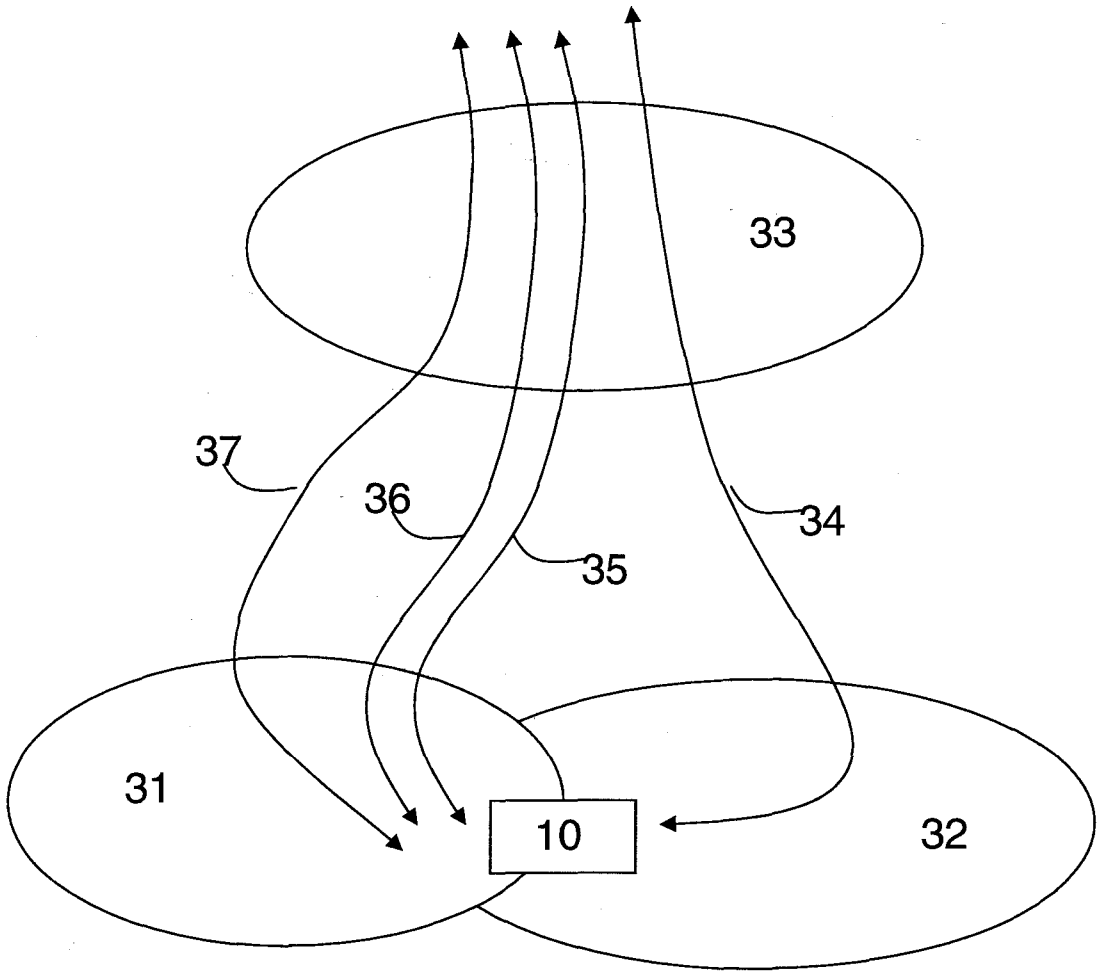

Fig. 3

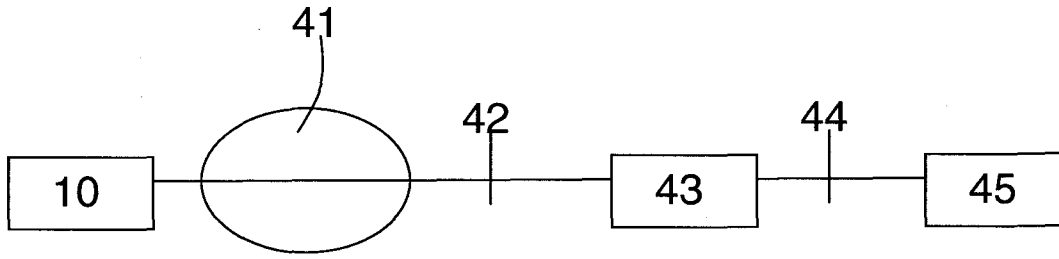

Fig. 4

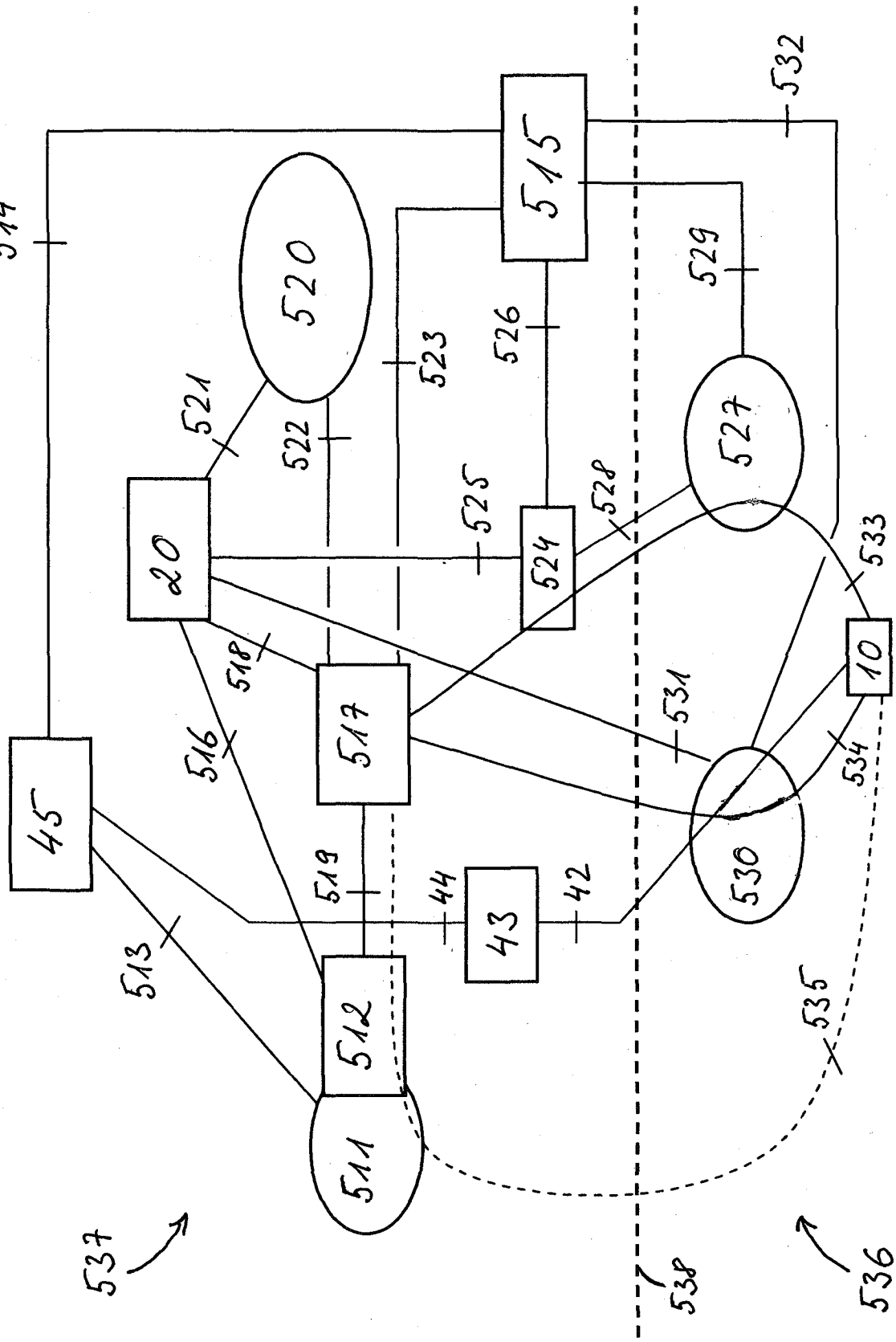
514
515
532
520
529
523
526
521
522
527
525
528
524
20
533
518
517
531
10
516
534
45
519
44
42
43
530
513
512
535
511
537
538
536

Fig. 5

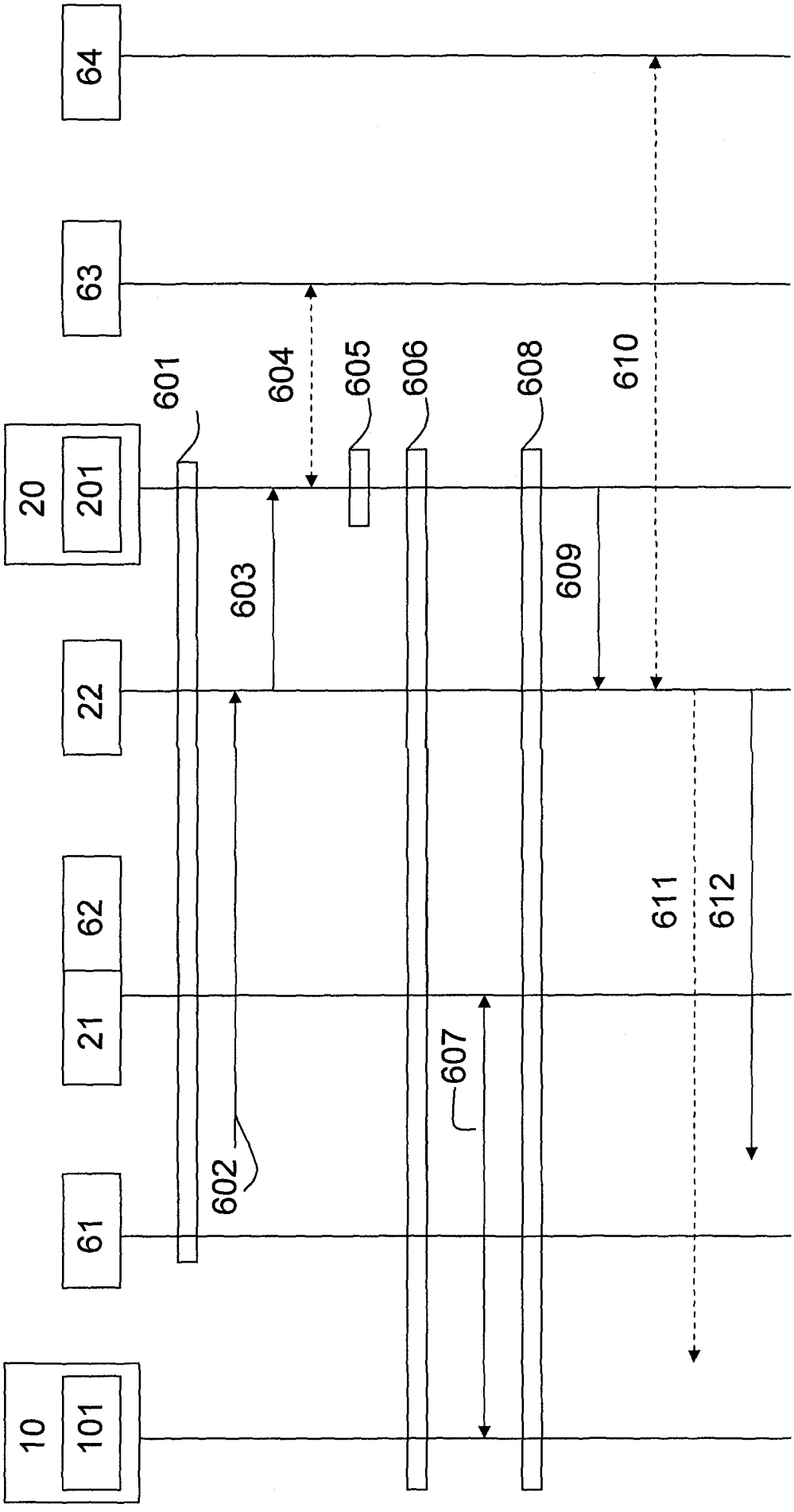
64
63
601
604
605
606
608
610
20
201
603
609
22
62
611
612
21
607
602
61
10
101

Fig. 6

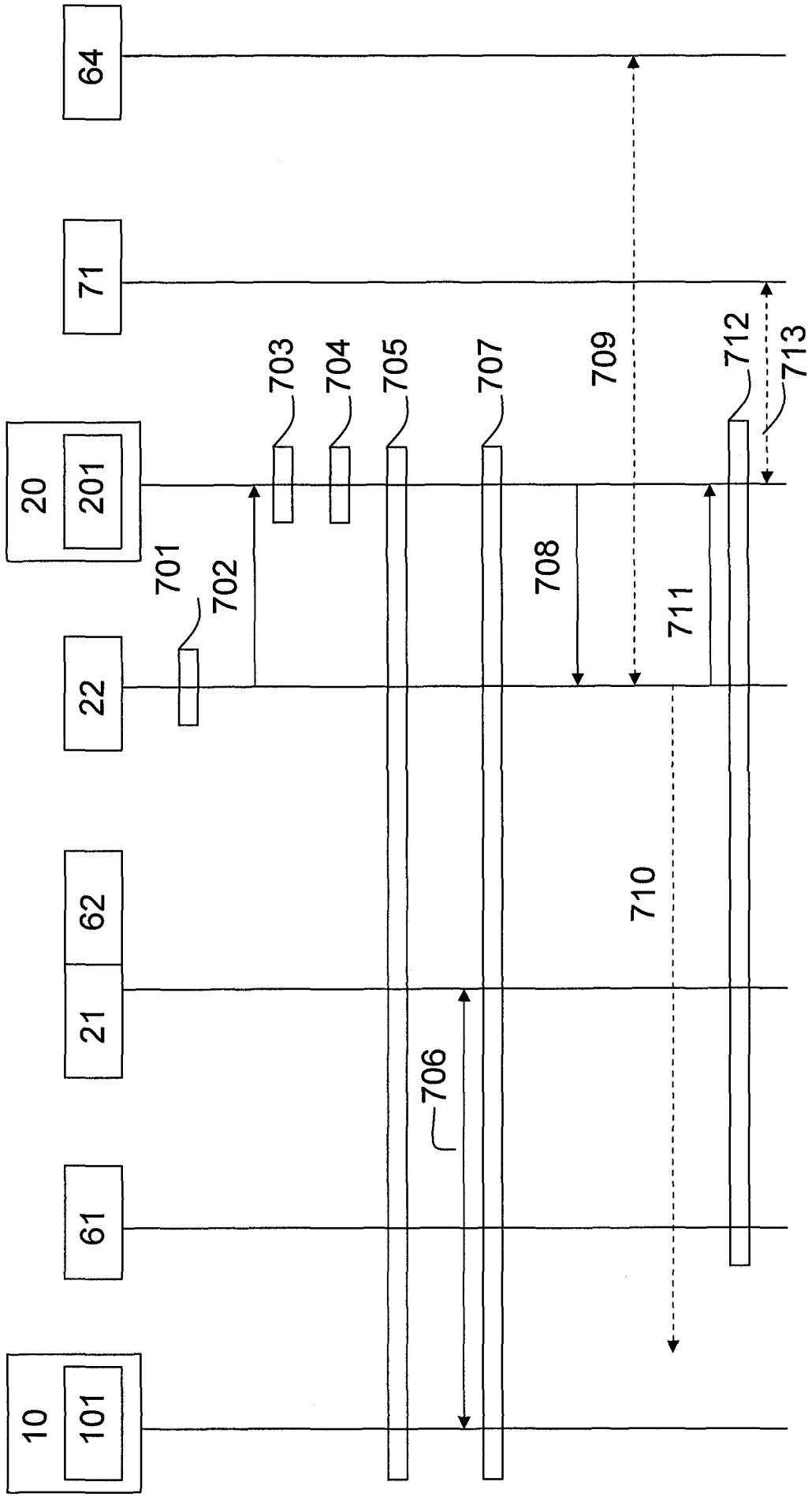
64
71
703
704
705
707
709
712
713
20
201
701
702
708
711
22
62
710
21
706
61
10
101

Fig. 7

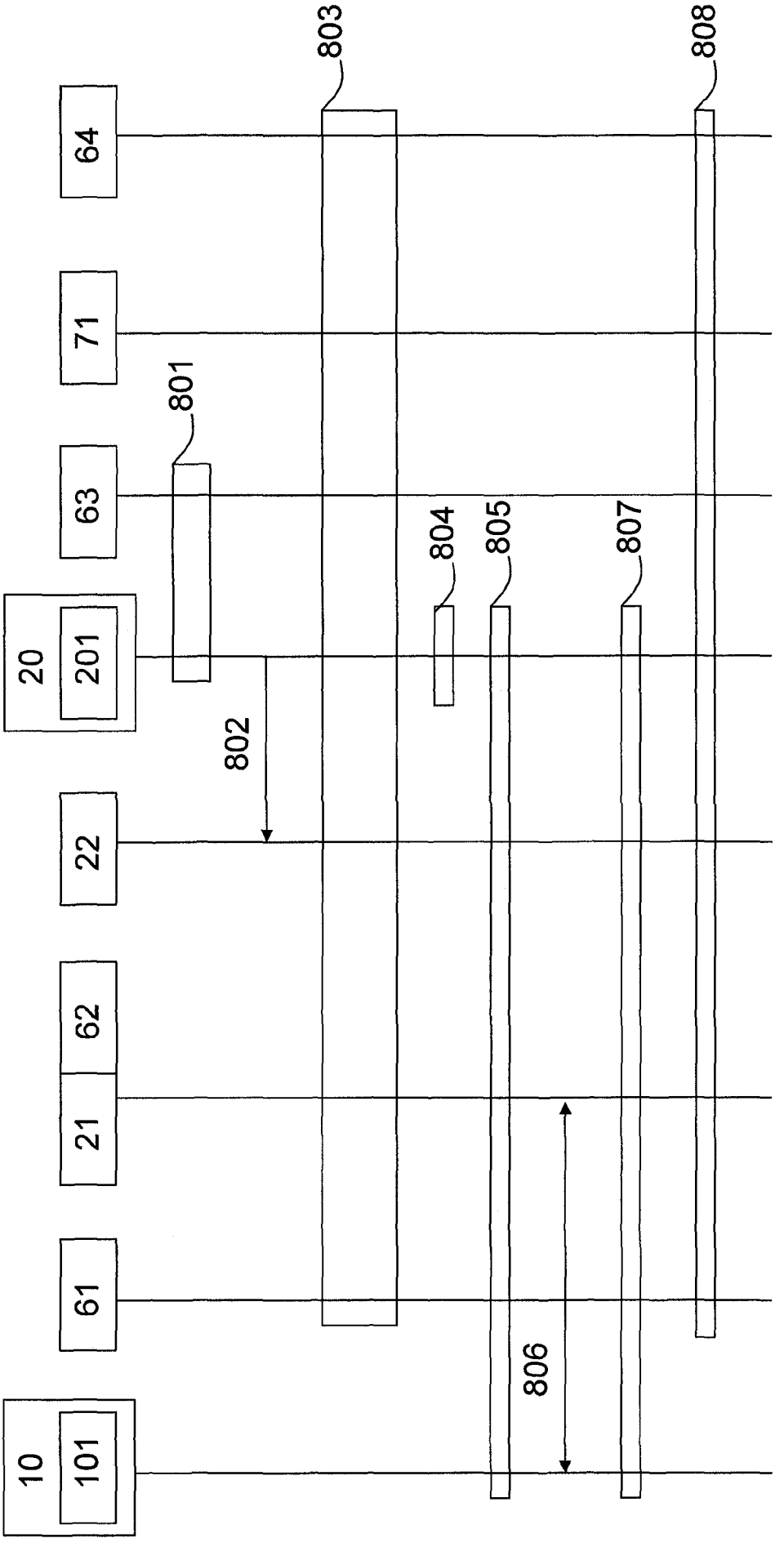

Fig. 8

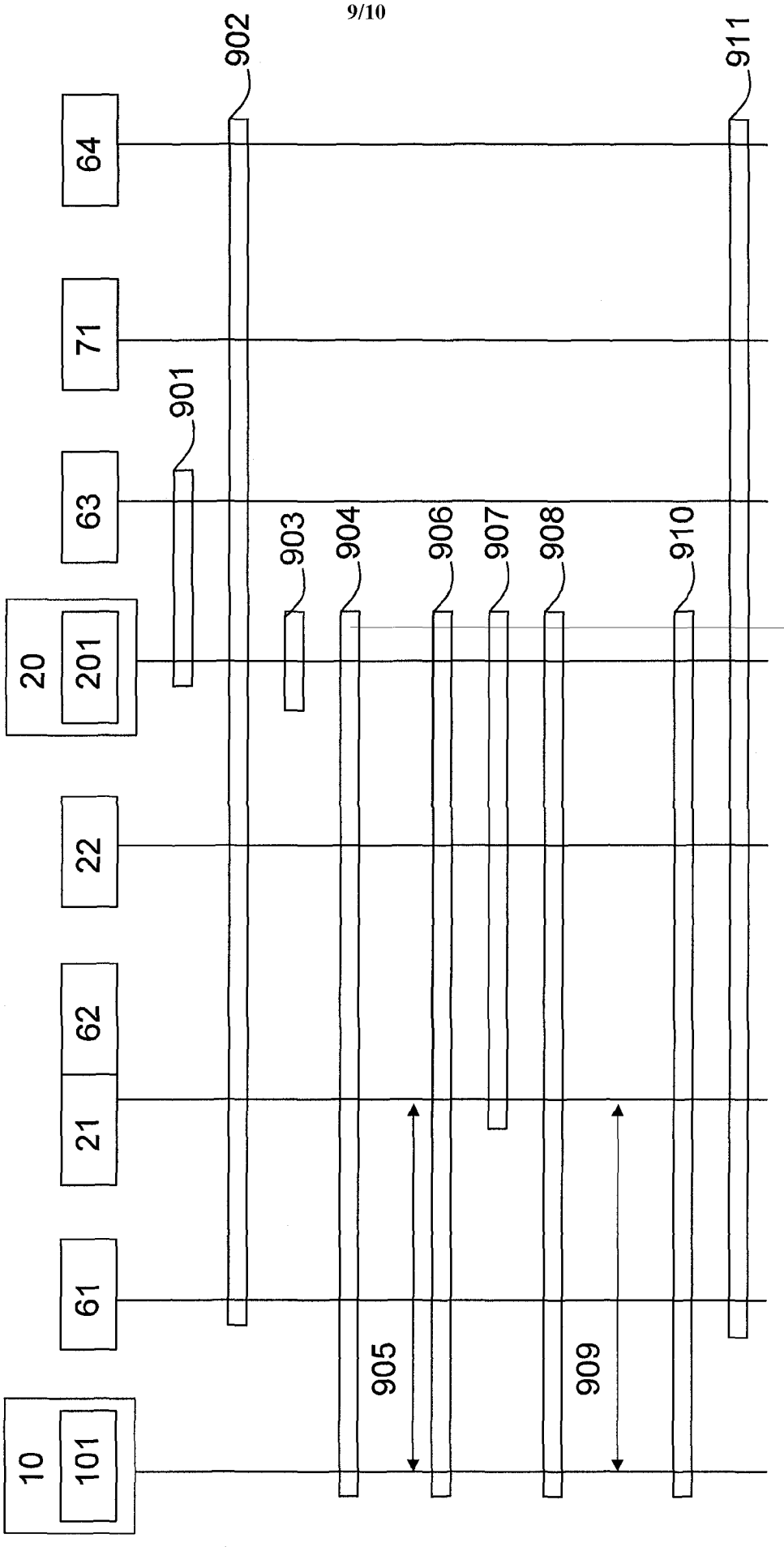
902
911
64
71
901
63
903
904
906
907
908
910
20
201
22
62
21
61
905
909
10
101

Fig. 9

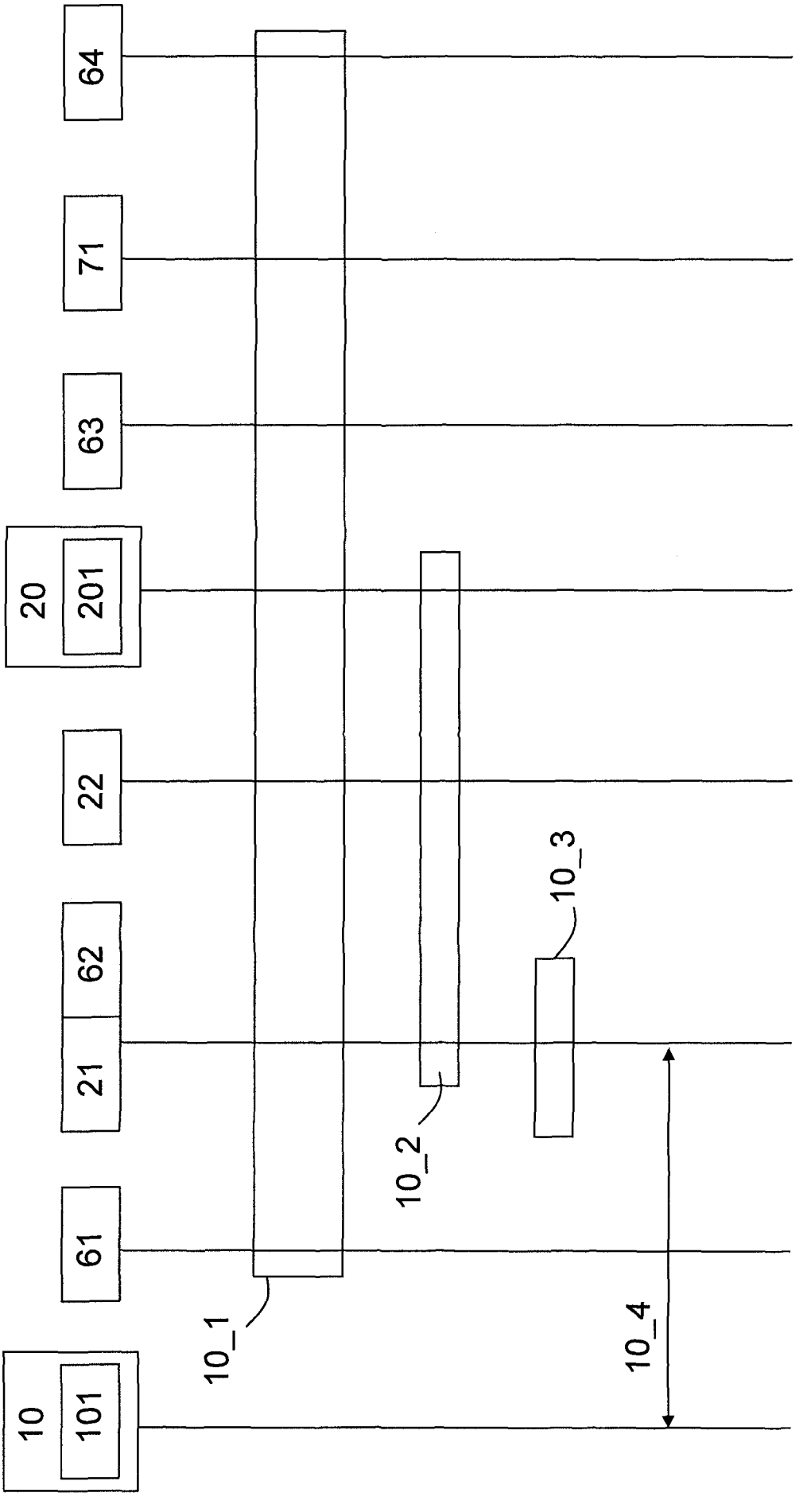

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/057208

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W40/02 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)
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 practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/068076 A1 (ERICSSON TELEFON AB L M [SE]; RUNE JOHAN [SE]) 4 June 2009 (2009-06-04) page 3, line 32 - page 11, line 20 page 15, line 29 - page 16, line 20; figure 4	1-18
X	EP 1 432 198 A1 (MOTOROLA INC [US]) 23 June 2004 (2004-06-23) paragraph [0022] - paragraph [0039]	1-18
A	US 2009/022126 A1 (DAMLE AMEYA [US]; FACCIN STEFANO [US]; ZHAO FAN [US]) 22 January 2009 (2009-01-22) paragraph [0021] - paragraph [0034] paragraph [0075] - paragraph [0111]	1-18

-/--

[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
1 October 2009	09/10/2009

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	Plata-Andres, Isabel

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	LARSSON H LEVKOWETZ H MAHKONEN T KAUPPINEN ERICSSON C: "A Filter Rule Mechanism for Multi-access Mobile IPv6; draft-larsson-monami6-filter-rules-02.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 2, 5 March 2007 (2007-03-05), XP015050112 ISSN: 0000-0004 Chapters 3, 5	1-18
A	KULADINITHI N A FIKOURAS C GOERG COMNETS-IKOM K; UNI BREMEN KOLTSIDAS GEORGIOS FOTINI-NIOVI PAVLIDOU ARISTOTLE UNIVERSITY OF THESS: "Filters for Mobile IPv6 Bindings (NOMADv6); draft-nomadv6-mobileip-filters-03.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, no. 3, 1 October 2005 (2005-10-01), XP015042945 ISSN: 0000-0004 Introduction Chapter 4	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/057208

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009068076 A1	04-06-2009	NONE	
EP 1432198 A1	23-06-2004	AT 365418 T	15-07-2007
		AU 2003303163 A1	14-07-2004
		WO 2004057826 A1	08-07-2004
		US 2006129630 A1	15-06-2006
US 2009022126 A1	22-01-2009	WO 2009015015 A2	29-01-2009