HU000028211T2

(19) **HU**

(11) Lajstromszám: **E 028 211**

(13) **T2**

MAGYARORSZÁG
Szellemi Tulajdon Nemzeti Hivatala

EURÓPAI SZABADALOM
SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 10 737907**
(22) A bejelentés napja: **2010. 07. 29.**

(96) Az európai bejelentés bejelentési száma:
EP 20100737907
(97) Az európai bejelentés közzétételi adatai:
EP 2599266 A1 **2012. 02. 02.**
(97) Az európai szabadalom megadásának meghirdetési adatai:
EP 2599266 B1 **2015. 10. 21.**

(51) Int. Cl.: ***H04L 12/24*** *(2006.01)*
H04L 128/51 *(2006.01)*
H04W 28/10 *(2006.01)*
H04W 72/10 *(2006.01)*

(86) A nemzetközi (PCT) bejelentési szám:
PCT/EP 10/061071
(87) A nemzetközi közzétételi szám:
WO 12013238

(72) Feltaláló(k):
LUDWIG, Reiner, 52393 Hürtgenwald (DE)
EKSTRÖM, Hannes, S-112 67 Stockholm (SE)

(73) Jogosult(ak):
Telefonaktiebolaget L M Ericsson (publ), 164 83 Stockholm (SE)

(74) Képviselő:
SBGK Szabadalmi Ügyvivői Iroda, Budapest

(54) **Hálózati forgalom kezelése rögzített címen keresztül**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 599 266 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
21.10.2015 Bulletin 2015/43

(21) Application number: **10737907.5**

(22) Date of filing: **29.07.2010**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***H04L 12/851*** *(2013.01)*
H04W 28/10 *(2009.01)* ***H04W 72/10*** *(2009.01)*

(86) International application number:
PCT/EP2010/061071

(87) International publication number:
WO 2012/013238 (02.02.2012 Gazette 2012/05)

(54) **HANDLING NETWORK TRAFFIC VIA A FIXED ACCESS**

HANDHABUNG VON NETZWERKVERKEHR ÜBER EINEN FESTEN ZUGANG

GESTION DU TRAFIC DE RÉSEAU VIA UN ACCÈS FIXE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(43) Date of publication of application:
05.06.2013 Bulletin 2013/23

(60) Divisional application:
15179533.3

(73) Proprietor: **Telefonaktiebolaget L M Ericsson (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **LUDWIG, Reiner**
  52393 Hürtgenwald (DE)
- **EKSTRÖM, Hannes**
  S-112 67 Stockholm (SE)

(74) Representative: **Sinn, Vincent et al**
Ericsson GmbH
Patent Department
Ericsson Allee 1
52134 Herzogenrath (DE)

(56) References cited:
WO-A1-2010/074619
US-A1- 2002 143 939
US-A1- 2005 243 837
US-A1- 2007 127 487
US-A1- 2007 242 627
US-B1- 7 283 468

EP 2 599 266 B1

Description

Technical Field

[0001] The present invention relates to methods and devices for handling network traffic via a fixed access and a corresponding computer program product.

Background

[0002] In communication networks, traffic separation is a concept which allows that different types of packet traffic receive different treatment in user plane traffic forwarding functions, e.g. with respect to queuing, scheduling error control, or the like. For implementing traffic separation, an edge node may classify packets into different traffic classes, e.g. voice traffic, multimedia traffic or internet traffic. On the basis of this traffic classification, the data packets may be provided with a marking which allows a user plane traffic forwarding function to associate the data packets with the respective traffic class and associated forwarding treatment.

[0003] If the edge node is a residential gateway communicating the data traffic with the network via a fixed access, e.g. using Digital Subscriber Line (DSL) or coaxial cable technology, it is known to accomplish traffic classification in the uplink direction, i.e. from the residential gateway to the network, on the basis of port mapping. In this case, the residential gateway is provided with multiple physical ports which are each dedicated to a certain type of end device, e.g. a voice port for connecting to a fixed phone, a TV port for connecting to a digital TV or to a digital set-top box, and an internet port for connecting to a computer or other type of multipurpose internet device. The internet port may also be coupled to an access point of a Wireless Local Area Network (WLAN), sometimes also referred to as a WiFi access point. In such a scenario, all traffic received in the voice port may be classified as voice traffic, all traffic received on the TV port may be classified as multimedia traffic, and all traffic received on the internet port may be classified as internet traffic. The data packets of the classified traffic may then be provided with the corresponding marking to be used in the uplink transmission via the fixed access.

[0004] As an alternative, the traffic classification may be based on a semi-static configuration of the residential gateway. For example, all data traffic sent to a certain Internet Protocol (IP) address or to a certain IP address range may be assigned to a certain traffic class. This approach may also be applied when the edge node is a mobile terminal communicating with a fixed access node using wireless access technology. Further, classification rules could be signaled from the network to the edge node.

[0005] However, using the above concepts of accomplishing traffic classification it may be difficult for a network operator to efficiently manage a large number of edge nodes in such a way that traffic classification is accomplished in a desired manner.

[0006] US 2007/0127487 A1 describes a method for managing a service bandwidth by a customer port and an EPON system using the same. In order to manage the service bandwidth by a customer, ONU and ONT allocate a service class according to a combination of information about a customer that receives a service, and a service type and a service priority of a service provided to a customer, allocate a bandwidth according to each service class and control a uplink bandwidth or a downlink bandwidth according to a service class. Also, a system manger collects information about a service provider, a service provided from a service provider, a customer that receives a service, and information for classifying a service. After collecting, the system manager provides the collected information to the ONU and the OLT.

[0007] Accordingly, there is a need for powerful and efficient techniques for handling network traffic via a fixed access.

Summary

[0008] A method, a communication device and a computer program product according to the independent claims are provided.

[0009] According to an embodiment of the invention, a method of handling network traffic in a communication device is provided. According to the method, incoming downlink data packets are received via a fixed access in the communication device. The downlink data packets include a first identifier and are assigned to a traffic class. In outgoing uplink data packets to be transmitted via the fixed access from the communication device, outgoing uplink data packets including a second identifier which is complementary with respect to said first identifier are detected. The first identifier includes a source address and the complementary second identifier includes a destination address which is the same as the source address of the first identifier. The detected outgoing uplink data packets having said second identifier are assigned to the same traffic class as the incoming downlink data packets having said first identifier.

[0010] According to a further embodiment of the invention, a communication device is provided. The communication device includes an interface configured to receive incoming downlink data packets via a fixed access from a network and an interface configured to send outgoing uplink data packets via the fixed access to the network. The communication device further includes a traffic classificator. The traffic classificator is configured to detect incoming downlink data packets including a first identifier and outgoing uplink data packets including a second identifier which is complementary to said first identifier. The first identifier includes a source address and the complementary second identifier includes a destination address which is the same as the source address of the first identifier. In addition, the traffic classificator is configured to assign said outgoing uplink data packets hav-

ing said complementary second identifier to the same traffic class as the incoming downlink data packets having the first identifier.

[0011] According to further embodiments of the invention described by the dependent claims, other methods or devices may be provided. Also, according an embodiment of the invention, a computer program product is provided, which comprises program code that, when executed by a processor of a communication device, causes the communication device to operate in accordance with the above method.

Brief Description of the Drawings

[0012]

Fig. 1 schematically illustrates a communication network environment in which concepts according to embodiments of the invention may be applied.

Fig. 2 schematically illustrates a communication system in which concepts according to embodiments of the invention may be applied.

Fig. 3 schematically illustrates an example of a data packet as used in an embodiment of the invention.

Fig. 4 schematically illustrates a further example of a data packet as used in an embodiment of the invention.

Fig. 5 schematically illustrates an identifier and a complementary identifier in data packets.

Fig. 6 schematically illustrates an information field in a header section of data packets.

Fig. 7 schematically illustrates a protocol frame supporting tagging of data packets.

Fig. 8 schematically illustrates an implementation of a communication device according to an embodiment of the invention.

Fig. 9 shows a flowchart for illustrating a method of handling UL data traffic according to an embodiment of the invention.

Detailed Description of Embodiments

[0013] In the following, the invention will be explained in more detail by referring to exemplary embodiments and to the accompanying drawings. The illustrated embodiments relate to handling of uplink (UL) data traffic of a communication device, i.e. data traffic from the communication device to a communication network. The communication network provides an access via a fixed access, i.e. implemented using DSL access technology, optical access technology or coaxial cable access technology. In addition, the communication network may also provide an access via a radio access node of a cellular mobile radio network. For example, the cellular mobile radio network may be implemented according to the 3GPP (Third Generation Partnership Project) technical specifications, e.g. as a Global System for Mobile Communications (GSM) network, as a Universal Mobile Telecommunications System (UMTS) network, or as a Service Architecture Evolution (SAE)/Long Term Evolution (LTE) network. However, it is to be understood that the concepts as described herein may also be applied to other types of communication networks. The embodiments as described herein accomplish UL traffic classification on the basis of UL traffic classification rules which are locally generated by monitoring downlink (DL) data traffic, in particular information in protocol headers of DL data packets.

[0014] Fig. 1 schematically illustrates a communication network environment in which concepts according to embodiments of the invention may be applied. As illustrated, the communication network environment includes a cellular mobile radio network domain 10 according to the 3GPP technical specifications. Further, a fixed access domain 20 is provided. In addition, the communication network environment includes a home domain 30, which includes various subscriber premises devices coupled to the fixed access domain 20. Components of the home domain 30 are typically located at the subscriber premises site. In the home domain, a residential gateway (RG) 35 is provided, which is a communication device at the subscriber premises site, which is used to couple the subscriber premises devices to the fixed access domain 20. In particlular, the RG 35 may couple a local area network (LAN) at the subscriber premises site to the fixed access domain 20 of the communication network.

[0015] In the illustrated example, the cellular mobile radio network domain 10 is implemented according to 3GPP SAE/LTE. As illustrated, the cellular mobile radio network domain 10 includes a Packet Data Network Gateway (PDN GW) which is coupled to Radio Access Networks (RANs) via a Serving Gateway (SGW). As illustrated, the RANs may include one or more GSM EDGE RAN (GERAN), UMTS Terrestrial RAN (UTRAN) or Evolved UTRAN (E-UTRAN). In the cellular mobile radio network domain 10, operator's IP services, e.g. IP Multimedia Subsystem (IMS) services, may be hosted by application servers or the like. A mobile terminal or user equipment (UE) 40, e.g. a mobile phone, a portable computer or the like, may access the operator's IP services via the PDN GW.

[0016] In addition, the cellular mobile radio network domain 10 includes control nodes, such as a Policy and Charging Rules Function (PCRF) and a Mobility Management Entity (MME), a subscriber database in the form of a Home Subscriber Server (HSS), and a 3GPP Authentication, Authorization and Accounting (AAA) server.

[0017] Further, for supporting the 3GPP Femto access

technology, the cellular mobile radio network domain 10 includes a Home eNodeB Gateway (HeNB GW) and a Security Gateway (Sec GW). For coupling to non-3GPP network domains, e.g. to the fixed access domain 20, the cellular mobile radio network domain 10 further includes an Evolved Packet Data Gateway (ePDG). Further details concerning the above components of the cellular mobile radio network domain 10 and the interfaces provided between these components can be taken from the 3GPP technical specifications.

[0018] The fixed access domain 20 includes operator infrastructure for providing fixed access to the communication network, e.g. using DSL access technology, optical access technology, or coaxial cable access technology. For this purpose, a Broadband Network Gateway (BNG) is provided, which communicates with the ePDG and/or the PDN GW in the cellular mobile radio network domain 10. Further, the BNG communicates with the RG 35 in the home domain 30 using fixed, e.g wire-based or cable based, communication links. Depending on the access technology used with respect to the RG 35, the fixed access domain 20 may be provided with a corresponding access node, e.g. a DSL Access Multiplexer (DSLAM), an Optical Network Terminal (ONT), or a coaxial cable head end.

[0019] Further, the fixed access domain 20 includes a policy control node in the form of a Broadband Policy and Charging Function (BPCF) and a Fixed Access (FA) Authentication, Authorization and Accounting (AAA) server. The policy control node in the cellular mobile radio network domain 10, i.e the PCRF, communicates with the policy control node in the fixed access domain 20, i.e. the BPCF. Further, the 3GPP AAA server communicates with the FA AAA server. In addition, the BNG in the fixed access domain 20 communicates with the Sec GW in the cellular mobile radio network domain 10. In this way, trusted interworking between the cellular mobile radio network domain 10 and the fixed access domain 20 is possible.

[0020] The home domain 30 includes the RG 35 and a number of subscriber premises devices connected thereto. In the illustrated example, the subscriber premises devices include a digital entertainment device in the form of a Media Center (MC), a multipurpose computing device in the form of a Personal Computer (PC), a television set (TV) coupled to the RG 35 via a Set-Top-Box (STB), and wireless access points, in particular a WiFi Access Point (AP), and a 3GPP Femto Access Point (AP).

[0021] In the communication network environment of Fig. 1, the UE 40 may move between accesses in the cellular mobile radio network domain 10, e.g. using GERAN, UTRAN or E-UTRAN, and between accesses via the fixed access domain 20, e.g. via the 3GPP Femto AP or the WiFi AP. This is illustrated by the dashed arrow.

[0022] Fig. 2 schematically illustrates a communication system in which UL data traffic is handled in accordance with an embodiment of the invention. The communication system includes a communication device 100, a fixed access node 250, and a network node 220. In addition, the communication system includes a control node 300. The illustrated communication system may be part of the communication network environment of Fig. 1. For example, the communication device 100 may correspond to the UE 40 or to the RG 35. The network node 220 may correspond to the BNG or the PDN GW. If the communication device 100 corresponds to the RG 35, the fixed access node 250 may be any type of access node coupled between the BNG and the RG 35 so as to implement the fixed access between the BNG and the RG. The fixed access node 250 may also be integrated in the BNG or in the RG 35. By way of example, the fixed access node 250 may be implemented by a DSLAM, an ONT, a cable modem, or the like. The fixed access node 250 may be located in the fixed access domain 20 or in the home domain 10. If the communication device 100 corresponds to the UE 40, the fixed access node may also be the RG 35. Accordingly, the communication device 100 may be a UE coupled to the network node 220 via a residential gateway or may be a residential gateway itself. The residential gateway has a fixed communication link to the network node, while a communication link between the UE and the residential gateway may be wireless. The residential gateway is typically authenticated using the fixed communication link to the network node 220, which for this purpose may communicate with an authentication server, e.g. the FA AAA server of Fig. 1. If a UE is connected via the residential gateway to the network node 220, independent authentication of the UE in a fixed access domain is then not necessary. The control node 300 may be the BPCF or the PCRF.

[0023] As further illustrated, the communication device 100 and the network node 220 communicate data packets in the DL direction and the UL direction. The data packets are assigned to different traffic classes 50, which is schematically illustrated by separate double headed arrows. The traffic classes may be, e.g., voice traffic, multimedia traffic, and internet traffic. For each of the traffic classes 50 a corresponding forwarding treatment in intermediate nodes, e.g. the fixed access node 250 or a transport node (not illustrated), may be defined. Each traffic class 50 may correspond to a certain Quality of Service (QoS) level. For example, the voice traffic class may have a higher QoS level than the internet traffic class. According to embodiments of the present invention, classification of UL data traffic in the communication device 100 is accomplished by detecting identifiers of outgoing UL data packets which are complementary to identifiers of incoming DL data packets. The DL data packets are already assigned to the traffic classes 50, e.g. by a traffic classificator 210 of the network node 220, which operates on the basis of DL packet classification rules 215. In the illustrated example, the traffic classificator 210 of the network node 220 is controlled by the control node 300, e.g. on the basis of policy data. The outgoing UL data packets carrying the complementary

identifier are assigned to the same traffic class 50 as the incoming DL data packets. For this purpose, the communication device 100 is provided with a traffic classificator 110, which can be operated in a reflective mode. In the reflective mode, the traffic classificator 110 monitors the DL data packets so as to locally generate UL packet classification rules 115.

[0024] In the communication device 100, the traffic class 50 to which the DL data packets are assigned may be detected on the basis of a marking of the DL data packets. Monitoring of the DL data packets may be accomplished by identifying a source of the received DL data packets, e.g. on the basis of a source identifier in the data packets. For example, the source identifiers may be source IP addresses. This information is then used to locally generate the UL packet classification rules 115. The UL packet classification rules operate to assign the UL data packets, which are directed to the identified source, to the same traffic class 50 as the DL data packets from this source. The classified UL data packets are marked according to the traffic class they are assigned to, e.g. using the same marking as in the DL data packets.

[0025] In the following, the reflective mode of the traffic classificator 110 will be explained in more detail by referring to exemplary structures of data packets and protocol frames used in transmitting the data packets.

[0026] Fig. 3 schematically illustrates IP data packets of the IP version 4 type. As illustrated, a header section of the data packets includes several information fields, which are referred to as "Version", "IHL (IP Header Length)", "Differentiated Services", "Total Length", "Identification", "Flags", "Fragment Offset", "Time to Live", "Protocol", "Header Checksum" "Source Address", "Destination Address", "Options", and "Padding". Details concerning these fields are defined in the RFC 791 Specification. The information field termed as "Differentiated Services" is defined in the RFC 2475 Specification. In addition, the header section of an IP data packet will also include information fields which are referred to as "Source Port" and "Destination Port". Corresponding information fields are defined, for example, by the Transport Control Protocol (TCP) defined in the RFC 793 Specification and the User Datagram Protocol (UDP) as defined in the RFC 768 Specification.

[0027] Following the header section, IP data packets are typically provided with a data section, in which different types of payload data traffic may be included.

[0028] Fig. 4 schematically illustrates IP data packets according to the IP version 6 type. Again, the header section includes a number of information fields, which are referred to as "Version", "Differentiated Services", "Flow Label", "Payload Length", "Next Header", "Hop Limit", "Source Address", and "Destination Address". This structure of the header section is defined in the RFC 2460 Specification. In addition, the header section may also comprise information fields termed as "Source Port" and "Destination Port", e.g. as defined by the TCP or UDP. Again, the header section will typically be followed by a data section which may carry various types of payload data.

[0029] For the purposes of the present disclosure, only the information fields referred to as "Differentiated Services", "Source Address", "Destination Address", "Source Port", and "Destination Port" will be further discussed. As regards the other information fields, further explanations can be taken from the above-mentioned RFC Specifications.

[0030] The information field "Source Address" indicates the IP address from which a data packet originates. Similarly, the information field "Destination Address" indicates the IP address for which the data packet is destined. In IP version 4, the source address and the destination address are 32 bit values. In IP version 6, the source address and the destination address are 128 bit values.

[0031] The information field "Source Port" indicates a port number at the source of the data packet, whereas the information field "destination port" indicates a port number at the destination point of the data packet.

[0032] On the basis of the source address, the destination address, the source port, and the destination port, an IP packet flow can be defined as a flow of IP packets between a first endpoint defined by the source address and the source port, and a second endpoint defined by the destination address and the destination port. An entity including the source address, the destination address, the source port, the destination port and a protocol identifier is also referred to as "IP 5-tuple".

[0033] The information field "Differentiated Services" is included in both IP version 4 data packets and in IP version 6 data packets. As defined in the RFC 2474 Specification, the information field "Differentiated Services" is an 8 bit value. The structure of this information field is schematically illustrated in Fig. 5.

[0034] As illustrated in Fig. 5, six bits of the information field, i.e. bits 0-5, are used to define the Differentiated Services Code Point (DSCP). The other two bits are unused. Using the DSCP, forwarding of the data packets by network nodes may be controlled. For data packets pertaining to different types of services different forwarding procedures may be selected. DSCPs may be standardized. Further, a range of non-standardized DSCPs is available.

[0035] Fig. 6 schematically illustrates the structure of a protocol frame according to the IEEE 802.1 q and 802.1p standards. The protocol frame is used on the media access control (MAC) layer and may be used to transmit the IP packets as explained in connection with Figs. 3, 4 and 5. The IP data packet would then be included into a data field of the protocol frame.

[0036] The protocol frame starts with a preamble, which is an alternating pattern of ones and zeros. The length of the preamble is seven bytes. The preamble is followed by a start-of-frame delimiter (SFD). The start-of-frame delimiter has a length of one byte and includes am alternating pattern of ones and zeros, ending with

two consecutive ones. The start-of-frame delimiter is followed by six bytes defining a destination MAC address (DA) of the protocol frame and by six bytes defining a source MAC address (SA) of the protocol frame. The next field includes a tagging protocol identification (TPID). A hexadecimal value of 8100 indicates the IEEE 802.1q/p protocol. The next field includes tag control information (TCI). As illustrated in the lower part of Fig. 6, the tag control information includes three priority bits, followed by one bit defined as canonical format indicator (CFI) and twelve bits of a virtual local area network identification (VLAN ID). The TCI field may also be referred to as VLAN tag. The TCI field is followed by a Type Length field, of two bytes length. This field indicates the number of MAC client data bytes contained in the data field of the protocol frame or the frame type identification if the frame is assembled using an optional format. The Type Length field is followed by the data field, which may be a sequence of 48 to 1500 bytes length. The data field is followed by a cyclic redundancy check (CRC) value, which is generated by the MAC source device and is used by the MAC destination device to check the integrity of received protocol frames.

[0037] In the TCI field, the priority bits define a user priority. Details concerning the mapping of the settings of the priority bits to user priorities are defined in the IEEE 802.1 p standard. The CFI bit is used to provide compatibility with both Ethernet and Token Ring type networks. The VLAN ID is used to distinguish between different virtual local area networks (VLANs).

[0038] According to concepts as described herein, information in DL data packets is used in the communication device 100 to locally generate packet classification rules for UL data packets. Here, it is to be noted that in many practical scenarios, a flow of IP data packets is typically bi-directional. Even if the transport of payload data occurs in only one direction, e.g. on the basis of TCP packets, the IP packet flow will typically also include control packets, e.g. TCP acknowledgement packets, transmitted in the opposite direction. Further, the source and destination IP addresses and port numbers of an IP packet flow are typically symmetrical, i.e. the destination endpoint (identified by an IP address and port number) in one direction is the same as the source endpoint (identified by IP address and port number) in the other direction, and vice versa. Due to the symmetry, oppositely flowing packets of the same IP packet flow will have "complementary" address identifiers, and "complementary" port identifiers, which means that the source identifier in one direction is the same as the destination identifier in the other direction.

[0039] According to the concepts as explained in the following, it will be assumed that the DL data traffic are in some way assigned to the traffic classes 50 and provided with a corresponding marking. This may be accomplished by the traffic classificator 210 of the network gateway node 220. In the illustrated example, the control node 300 signals the DL packet classification rules 215 to the network gateway node 220. However, other way of providing the DL packet classification rules 215 to the network gateway node 220 may be used as well. Using the DL packet classification rules 215, the traffic classificator 220 in the network gateway node 220 assigns the DL packets to the traffic classes 50 and marks the DL data packets accordingly. This marking may be accomplished by setting the DSCP field in the header of the data packets, by setting priority bits of the data packets, and/or by providing the data packets with a VLAN tag. Further, if the outgoing data packets are to be transmitted using a tunneling protocol, this marking of the outgoing data packets may also be accomplished by providing the data packets with a tunnel identification.

[0040] As explained above, the communication device 100 includes the traffic classificator 110 operating on the basis of UL packet classification rules 115 and supporting a reflective mode of generating the UL packet classification rules. In the reflective mode, the traffic classificator 110 is configured to detect incoming data packets including a first identifier and outgoing data packets including a second identifier which is complementary with respect to the first identifier. In the complementary second identifier, a destination endpoint element, e.g. destination IP adress and/or destination port, is the same as a source endpoint element, e.g. source IP adress and/or source port, in the first identifier. The first and the second identifier may each be the IP 5-tuple. By monitoring the received DL data packets, the traffic classificator 110 generates the UL packet classification rules 115 in such a way that the outgoing data packets having the complementary second identifier are assigned to the same traffic class 50 as the incoming data packets having the first identifier. In this way, it is not required to explicitly signal the UL packet classification rules 115 to the communication device 100. On the other hand, the UL packet classification rules 115 can be flexibly adapted to specific communication scenarios, which can be controlled by the network operator through the DL traffic classification.

[0041] In the reflective mode, if the traffic classificator 110 detects a new IP packet flow with incoming data packets in the DL direction, it can automatically generate a corresponding UL packet classification rule 115. If the incoming data packets of the IP packet flow each carry a specific IP 5-tuple, the UL packet classification rule 115 will be configured to assign outgoing data packets carrying a complementary IP 5-tuple to the same traffic class 50 as the incoming data packets are received. Further, the UL data packets are marked according to their classification, e.g. by using the same marking as in the DL data packets of this traffic class. This marking may be accomplished by setting the DSCP field in the header of the data packets, by providing the data packets with a VLAN tag, and/or by setting priority bits of the data packets. Further, if the outgoing data packets are to be transmitted using a tunneling protocol, this marking of the outgoing data packets may also be accomplished by providing the data packets with a tunnel identification.

[0042] The structure of an identifier and a complementary identifier, which are based on the IP 5-tuple, are illustrated in Fig. 7. However, it is to be understood that other types of identifiers and complementary identifiers are possible as well. In general, in the complementary identifier at least one element of identifier reappears as another element. For example, in the complementary identifier of the outgoing data packet the source element of the identifier in the incoming data packet may reappear as a destination element. According to an embodiment, the identifier includes a source address and a destination address and the complementary identifier includes a source address corresponding to the destination address of the identifier and a destination address corresponding to the source address of the identifier.

[0043] As shown in Fig. 7, an identifier on the basis of the IP 5-tuple may include a source address A, a destination address B, a source port C, a destination port D, and a protocol identifier X. The corresponding complementary identifier will then have a source address B, a destination address A, a source port D, a destination port C, and a protocol identifier X. In other words, in the complementary identifier the source address and the destination address are swapped as compared to the identifier. Similarly, in the complementary identifier the source port and the destination port are swapped as compared to the identifier. The protocol identifier remains unchanged. In other embodiments, different types of identifier and complementary identifier may be used, e.g. on the basis of only a part of the IP 5-tuple. For example, in the complementary identifier, only the source address and the destination address could be swapped as compared to the identifier.

[0044] In the following, a process of handling UL data packets in accordance with an embodiment of the invention will be explained in more detail by referring to the structures as shown in Fig. 1.

[0045] Initially, UL data packets, e.g. data packets relating to a specific service such as a Voice over IP service, may be transmitted from communication device 100 to the network gateway 220 while being assigned to a default traffic class among the traffic classes 50, e.g. the internet traffic class. The corresponding IP packet flow will then also include data packets transmitted in the DL direction, e.g. acknowledgement packets. Using the DL packet classification rules 215, the traffic classificator 210 in the network gateway node 220 will assign these DL data packets to a desired traffic class, e.g. voice traffic, and will accomplish a corresponding marking of the DL data packets. As mentioned above, this marking may involve setting the DSCP field in the header of the DL data packets, providing the DL data packets with a VLAN tag, providing the DL data packets with a tunnel identification, and/or setting priority bits of the DL data packets.

[0046] In the reflective mode, the traffic classificator 110 in the communication device 100 then detects the incoming DL data packets and generates a UL traffic classification rule 115, operating on the basis of an IP 5-tuple which is complementary to an IP 5-tuple in the received incoming data packets. Here, it is to be understood that different IP packet flows may have the same traffic class 50 and that multiple UL packet classification rules 115 may be used for assigning outgoing UL data packets to one traffic class 50.

[0047] In addition to the reflective mode of generating the UL packet classification rules 115, the traffic classificator 110 may also be provided with other traffic classification modes, e.g. operating on the basis of UL packet classification rules signaled from the network, operating on the basis of statically configured UL packet classification rules, or operating on the basis of port mapping. The reflective mode may be activated in response to receiving a control signal from the network, e.g. when initializing the connection between the communication device 100 and the network gateway node 220 or in an update procedure.

[0048] The communication device 100 may also be provided with a functionality to indicate to the communication network that it supports the above-described reflective mode of generating the UL classification rules 115. For example, this could be included into connection initialization between the communication device 100 and the network gateway node 220. By way of example, an information element could be added to the signaling used during connection initialization. By means of this information element, the communication device 100 can indicate that it supports the reflective mode. And the network can signal to the communication device 100 whether the reflective mode should be used.

[0049] In some embodiments, the information that the communication device 100 supports the reflective mode of generating the UL classification rules 115 may also be distributed between network nodes, e.g. to the control node 300.

[0050] According to some embodiments, the reflective mode of generating the UL classification rules 115 may be selectively activated for a subgroup of the traffic classes 50, e.g. for only one traffic class. For example, the reflective mode could be activated only for voice traffic and/or multimedia traffic. This may be useful if not all applications or services require the reflective mode to be activated. For example, in some cases the IP 5-tuple in data packets of a service may be statically defined and a corresponding static UL packet classification rule 115 may be used in the communication device 100. Also, port mapping could be used for some of the traffic classes 50, while traffic classification to one or more other traffic classes is accomplished in the reflective mode.

[0051] In some embodiments, the network can signal to the communication device 100 whether the reflective mode of generating the UL classification rules 115 should be applied or not, e.g. using corresponding signaling on the link between the network gateway node 220 and the communication device 100. In such cases, the signaling from the communication device 100 to the communication network that the reflective mode is supported could

be implemented on a per traffic class basis as well. That is to say, the corresponding signaling could specify support of the reflective mode for a certain traffic class or group of traffic classes, e.g. voice traffic and multimedia traffic.

[0052] Fig. 8 further illustrates an exemplary implementation of the communication device 100. As explained above, the communication device may be a mobile terminal, e.g. the UE 40 explained in connection with Fig. 1, or a residential gateway, e.g. the RG 35 as explained in connection with Fig. 1.

[0053] According to the illustrated implementation, the communication device 100 includes at least a first interface 130 for coupling to the network gateway node 220 via the fixed access node 250. The interface 130 is implemented as a bidirectional interface, i.e. includes a receive (RX) interface for receiving DL data packets and a transmit (TX) interface for transmitting UL data packets. In some embodiments, e.g. if the communication device is implemented as a residential gateway, it may also include at least one second interface 140 for coupling to other devices, e.g. to the subscriber premises devices as illustrated in Fig. 1. The second interface 140 may be implemented as a bidirectional interface as well, i.e. include a receive (RX) interface and a transmit (TX) interface. Further, the communication device 100 includes a processor 150 coupled to the interface(s) 130, 140 and a memory 160 coupled to the processor 150. The memory 160 may include a read-only memory (ROM), e.g. a flash ROM, a random-access memory (RAM), e.g. a Dynamic RAM (DRAM) or static RAM (SRAM), a mass storage, e.g. a hard disk or solid state disk, or the like. The memory 160 includes suitably configured program code to be executed by the processor 150 so as to implement the above-described functionalities of the communication device 100. More specifically, the memory 160 may include a rule generator module 170 configured to implement the reflective mode of generating the UL packet classification rules and a traffic classification module 180 configured to classify the outgoing UL data packets in the above-described manner by applying the UL packet classification rules, and to mark the outgoing UL data packets accordingly. Accordingly, the traffic classificator 110 may be implemented by having the processor 150 execute the rule generator module 170 and the traffic classification module 180.

[0054] It is to be understood that the structure as illustrated in Fig. 8 is merely schematic and that the communication device 100 may actually include further components which, for the sake of clarity, have not been illustrated. Also, it is to be understood that the memory 160 may include further types of program code modules, which have not been illustrated, e.g. program code modules for implementing known functionalities of a mobile terminal or of a residential gateway.

[0055] Fig. 9 shows a flowchart illustrating a method 900 for handling UL data traffic, which may be used to implement the above-mentioned concepts. The method may be implemented in a communication device having access to a communication network via a fixed access, e.g. in the UE 40 or the RG 35 of Fig. 1.

[0056] In step 910, incoming data packets with a first identifier are received in the communication device. The data packets are received via the fixed access. For this purpose, the communication device may be coupled to the fixed access via an intermediate fixed access node. The data packets are identified by a first identifier, e.g. an IP 5-tuple or other identifier including a destination address identifier and a source address identifier. Further, the incoming data packets are associated with a traffic class, e.g. by a marking provided in the data packets.

[0057] In step 920, outgoing data packets with a complementary second identifier are detected.

[0058] In step 930, outgoing data packets with the second identifier are assigned to the same traffic class as the incoming data packets with the first identifier.

[0059] The detecting of outgoing data packets in step 920 and assigning to the same traffic class in step 930 may be accomplished on the basis of a packet classification rule. The packet classification rule may be generated in the communication device by monitoring the received incoming data packets.

[0060] Then, in optional step 940, the outgoing data packets may be provided with a marking which indicates the traffic class the outgoing data packets have been assigned to. This marking may be accomplished by setting a DSCP of the outgoing data packets, by setting priority bits of the outgoing data packets, and/or by including a VLAN tag or a tunnel identification into the outgoing data packets. The priority bits may be part of the VLAN tag.

[0061] According to the concepts as explained above, dynamic assignment of outgoing data traffic from a communication device to a desired traffic class is possible without requiring complex signaling to the communication device. The assignment may be adapted according to operating conditions or on the basis of policy data, e.g. on the basis of user-specific policies data and/or, if the outgoing data traffic relates to a specific service, on the basis of service-specific policies. Further, the assignment could be dependent on the time of day, the day of week or other parameters. A variety of different policies may thus be defined for controlling the assignment of the data traffic to a traffic class. One such policy may even be to block data traffic relating to a specific service.

[0062] It is to be understood that the concepts as explained above are merely exemplary and susceptible to various modifications. For example, the network nodes as illustrated in Figs. 1 and 2 need not be implemented as separate nodes, but two or more nodes may be integrated into a single component. The concepts may be applied in various types of communication networks and in various types of communication devices. In addition or as an alternative to IP 5-tuples, other identifiers and complementary identifiers may be used as well to imple-

ment the concepts. The concepts may be implemented by dedicated hardware and/or by software to be executed by a multipurpose processor in one of the involved nodes.

Claims

1. A method of handling network traffic in a communication device (100), comprising:

   - receiving incoming downlink data packets via a fixed access in the communication device (100), the downlink data packets including a first identifier and being assigned to a traffic class (50);
   - detecting outgoing uplink data packets to be transmitted via the fixed access from the communication device (100), said outgoing uplink data packets including a second identifier which is complementary with respect to said first identifier,

   characterized by
   said first identifier including a source address and said complementary second identifier including a destination address which is the same as the source address of said first identifier; the method comprising:

   - assigning the detected outgoing uplink data packets having said complementary second identifier to the same traffic class (50) as the incoming downlink data packets having said first identifier.

2. The method according to claim 1, comprising:

   - monitoring the received incoming downlink data packets; and
   - generating a packet classification rule for assigning the outgoing uplink data packets to the same traffic class (50) on the basis of the monitored incoming downlink data packets.

3. The method according to claim 1 or 2,
   wherein said assigning of the outgoing uplink data packets to the same traffic class (50) is activated on the basis of a control signal.

4. The method according to any one of the preceding claims,
   wherein said assigning of the outgoing uplink data packets is selectively activated for a subgroup of multiple traffic classes (50).

5. The method according to anyone of the preceding claims, comprising:

   - marking the outgoing uplink data packets, said marking indicating the traffic class (50) the outgoing uplink data packets are assigned to.

6. The method according to claim 5,
   wherein the incoming downlink data packets are provided with a marking indicating the traffic class (50) the incoming downlink data packets are assigned to; and
   wherein the outgoing uplink data packets are marked with the same marking as the incoming downlink data packets.

7. The method according to claim 5 or 6,
   wherein said marking of the outgoing uplink data packets comprises setting a Differentiated Services Code Point field of the data packets, setting priority bits of the data packets, providing the data packets with a virtual local area network tag, and/or providing the data packets with a tunnel identifier.

8. The method according to any one of the preceding claims, comprising:

   - indicating to a network component (220) that said communication device (100) is capable of said assigning the outgoing uplink data packets to the same traffic class (50).

9. The method according to any one of the preceding claims,
   wherein said communication device (100) is a residential gateway.

10. The method according to any one of claims 1 to 8,
    wherein said communication device (100) is a mobile terminal coupled to a residential gateway.

11. A communication device (100), comprising:

    - an interface (120) configured to receive incoming downlink data packets via a fixed access from a network;
    - an interface (120) configured to send outgoing uplink data packets via the fixed access to the network;
    - a traffic classificator (110) configured to detect incoming downlink data packets including a first identifier and outgoing uplink data packets including a second identifier which is complementary to said first identifier,

    characterized by
    said first identifier including a source address and said complementary second identifier including a destination address which is the same as the source address of said first identifier, and the traffic classificator (110) being configured to assign said outgoing

uplink data packets having said complementary second identifier to the same traffic class (50) as the incoming downlink data packets having the first identifier.

12. The communication device (100) according to claim 11,
wherein the communication device (100) is a residential gateway.

13. The communication device (100) according to claim 11,
wherein the communication device (100) is a mobile terminal configured to be coupled to a residential gateway.

14. The communication device (100) according to any one of claims 11 to 13,
wherein the communication device (100) is configured to be operated in accordance with the method according to any one of claims 2 to 10.

15. A computer program product, comprising program code which, when executed by a processor of a communication device (100), causes the communication device (100) to operate in accordance with a method according to any one of claims 1 to 10.

Patentansprüche

1. Verfahren zum Handhaben von Netzwerkverkehr in einem Kommunikationsgerät (100), aufweisend:

- Empfangen ankommender Downlink-Datenpakete über einen festen Zugang in dem Kommunikationsgerät (100), wobei die Downlink-Datenpakete einen ersten Identifizierer umfassen und einer Verkehrsklasse (50) zugewiesenen sind;
- Detektieren abgehender Uplink-Datenpakete, die über den festen Zugang von dem Kommunikationsgerät (100) gesendet werden sollen, wobei die abgehenden Uplink-Datenpakete einen zweiten Identifizierer umfassen, der zu dem ersten Identifizierer komplementär ist,

dadurch gekennzeichnet, dass
der erste Identifizierer eine Quellenadresse umfasst und der komplementäre zweite Identifizierer eine Zieladresse umfasst, die die gleiche wie die Quellenadresse des ersten Identifizierers ist; wobei das Verfahren aufweist:

- Zuweisen der detektierten abgehenden Uplink-Datenpakete, die den komplementären zweiten Identifizierer haben, zur selben Verkehrsklasse (50) wie die ankommenden Downlink-Datenpakete, die den ersten Identifizierer haben.

2. Verfahren nach Anspruch 1, aufweisend:

- Überwachen der empfangenen ankommenden Downlink-Datenpakete; und
- Generieren einer Paketklassifizierungsregel zum Zuweisen der abgehenden Uplink-Datenpakete zur selben Verkehrsklasse (50) anhand der überwachten ankommenden Downlink-Datenpakete.

3. Verfahren nach Anspruch 1 oder 2,
wobei das Zuweisen der abgehenden Uplink-Datenpakete zur selben Verkehrsklasse (50) basierend auf einem Steuerungssignal aktiviert wird.

4. Verfahren nach einem der vorangehenden Ansprüche,
wobei das Zuweisen der abgehenden Uplink-Datenpakete selektiv für eine Untergruppe mehrerer Verkehrsklassen (50) aktiviert wird.

5. Verfahren nach einem der vorangehenden Ansprüche, aufweisend:

- Markieren der abgehenden Uplink-Datenpakete, wobei das Markieren die Verkehrsklasse (50) anzeigt, der die abgehenden Uplink-Datenpakete zugewiesen sind.

6. Verfahren nach Anspruch 5,
wobei die ankommenden Downlink-Datenpakete mit einer Markierung versehen sind, die die Verkehrsklasse (50) anzeigt, der die ankommenden Downlink-Datenpakete zugewiesen sind; und
wobei die abgehenden Uplink-Datenpakete mit der gleichen Markierung markiert werden wie die ankommenden Downlink-Datenpakete.

7. Verfahren nach Anspruch 5 oder 6,
wobei das Markieren der abgehenden Uplink-Datenpakete Setzen eines Differentiated Services Code Point-Feldes der Datenpakete, Setzen von Prioritätsbits der Datenpakete, Versehen der Datenpakete mit einem Virtual Local Area Network-Tag und/oder Versehen der Datenpakete mit einem Tunnel-Identifizierer aufweist.

8. Verfahren nach einem der vorangehenden Ansprüche, aufweisend:

- Anzeigen gegenüber einer Netzwerkkomponente (220), dass das Kommunikationsgerät (100) in der Lage ist, die abgehenden Uplink-Datenpakete zur selben Verkehrsklasse (50) zuzuweisen.

9. Verfahren nach einem der vorangehenden Ansprüche,
wobei das Kommunikationsgerät (100) ein Residential Gateway ist.

10. Verfahren nach einem der Ansprüche 1 zu 8,
wobei das Kommunikationsgerät (100) ein Mobil-Endgerät ist, das an einen Residential Gateway gekoppelt ist.

11. Kommunikationsgerät (100), aufweisend:

- eine Schnittstelle (120), die dafür konfiguriert ist, ankommende Downlink-Datenpakete über einen festen Zugang von einem Netzwerk zu empfangen;
- eine Schnittstelle (120), die dafür konfiguriert ist, abgehende Uplink-Datenpakete über den festen Zugang zu dem Netzwerk zu senden;
- einen Verkehrsklassifizierer (110), der dafür konfiguriert ist, ankommende Downlink-Datenpakete, die einen ersten Identifizierer umfassen, und abgehende Uplink-Datenpakete zu detektieren, die einen zweiten Identifizierer umfassen, der zu dem ersten Identifizierer komplementär ist,

dadurch gekennzeichnet, dass
der erste Identifizierer eine Quellenadresse umfasst und der komplementäre zweite Identifizierer eine Zieladresse umfasst, die die gleiche wie die Quellenadresse des ersten Identifizierers ist, und der Verkehrsklassifizierer (110) dafür konfiguriert ist, die abgehenden Uplink-Datenpakete, die den komplementären zweiten Identifizierer haben, zur selben Verkehrsklasse (50) zuzuweisen wie die ankommenden Downlink-Datenpakete, die den ersten Identifizierer haben.

12. Kommunikationsgerät (100) nach Anspruch 11,
wobei das Kommunikationsgerät (100) ein Residential Gateway ist.

13. Kommunikationsgerät (100) nach Anspruch 11,
wobei das Kommunikationsgerät (100) ein Mobil-Endgerät ist, das dafür konfiguriert ist, an einen Residential Gateway gekoppelt zu werden.

14. Kommunikationsgerät (100) nach einem der Ansprüche 11 bis 13,
wobei das Kommunikationsgerät (100) dafür konfiguriert ist, gemäß dem Verfahren nach einem der Ansprüche 2 bis 10 betrieben zu werden.

15. Computerprogrammprodukt, das Programmcode umfasst, der, wenn er durch einen Prozessor eines Kommunikationsgerätes (100) ausgeführt wird, das Kommunikationsgerät (100) veranlasst, gemäß einem Verfahren nach einem der Ansprüche 1 bis 10 zu arbeiten.

Revendications

1. Procédé de gestion du trafic de réseau dans un dispositif de communication (100), comprenant de :

- recevoir des paquets de données entrants de liaison descendante via un accès fixe dans le dispositif de communication (100), les paquets de données de liaison descendante incluant un premier identifiant et étant attribués à une classe de trafic (50) ;
- détecter les paquets de données sortants de liaison montante à transmettre via l'accès fixe depuis le dispositif de communication (100), les paquets de données sortants de liaison montante incluant un second identifiant qui est complémentaire par rapport au premier identifiant,

caractérisée par
ledit premier identifiant incluant une adresse source et ledit second identifiant complémentaire incluant une adresse de destination qui est la même que l'adresse source du premier identifiant ; le procédé comprenant de :

- attribuer les paquets de données sortants de liaison montante détectée ayant ledit second identifiant complémentaire à la même classe de trafic (50) que les paquets de données entrants de liaison descendante ayant ledit premier identifiant.

2. Procédé selon la revendication 1, comprenant de :

- surveiller les paquets de données entrants de liaison descendante reçus ; et
- générer une règle de classification des paquets pour attribuer les paquets de données sortants de liaison montante à la même classe de trafic (50) sur la base des paquets de données entrants de liaison descendante surveillés.

3. Procédé selon la revendication 1 ou 2,
dans lequel ladite attribution des paquets de données sortants de liaison montante à la même classe trafic (50) est activée sur la base d'un signal de contrôle.

4. Procédé selon une quelconque des revendications précédentes,
dans lequel ladite attribution des paquets de données sortants de liaison montante est activée sélectivement pour un sous-groupe de classes de trafic multiples (50).

5. Procédé selon un quelconque des revendications précédentes, comprenant de :

- marquer les paquets de données sortants de liaison montante, ledit marquage indiquant la classe de trafic (50) à laquelle les paquets de données sortants de liaison montante sont attribués.

6. Procédé selon la revendication 5,
dans lequel les paquets de données entrants de liaison descendante sont pourvus d'un marquage indiquant la classe de trafic (50) à laquelle les paquets de données entrants de liaison descendante sont attribués ; et
dans lequel les paquets de données sortants de liaison montante sont marqués avec le même marquage que les paquets de données entrants de liaison descendante.

7. Procédé selon la revendication 5 ou 6,
dans lequel ledit marquage des paquets de données sortants de liaison montante comprend de régler un champ de code de service différencié des paquets de données, régler les bits de priorité des paquets de données, munir les paquets de données d'une étiquette de réseau local virtuel et/ou munir les paquets de données d'un identifiant de tunnel.

8. Procédé selon une quelconque des revendications précédentes, comprenant de :

- indiquer à un composant de réseau (220) que le dispositif de communication (100) est capable de ladite attribution des paquets de données sortants de liaison montante à la même classe de trafic (50).

9. Procédé selon une quelconque des revendications précédentes,
dans lequel le dispositif de communication (100) est une passerelle résidentielle.

10. Procédé selon une quelconque des revendications 1 à 8,
dans lequel ledit dispositif de communication (100) est un terminal mobile couplé à une passerelle résidentielle.

11. Dispositif de communication (100), comprenant :

- une interface (120) configuré pour recevoir des paquets de données entrants de liaison descendante via un accès fixe depuis un réseau ;
- une interface (120) configuré pour transmettre des paquets de données de liaison montante sortants via l'accès fixe au réseau ;
- un classificateur de trafic (110) configuré pour détecter les paquets de données entrants de liaison descendante incluant un premier identifiant et les paquets de données sortants de liaison montante incluant un second identifiant qui est complémentaire au premier identifiant,

caractérisé par
ledit premier identifiant inclut une adresse source et ledit second identifiant complémentaire inclut une adresse de destination qui est la même que l'adresse source dudit première identifiant, et le classificateur de trafic (110) est configuré pour attribuer lesdits paquets de données sortants de liaison montante ayant ledit second identifiant complémentaire à la même classe de trafic (50) que les paquets de données entrants de liaison descendante ayant le premier identifiant.

12. Dispositif de communication (100) selon la revendication 11,
dans lequel le dispositif de communication (100) est une passerelle résidentielle.

13. Dispositif de communication selon la revendication 11,
dans lequel le dispositif de communication (100) est un terminal mobile configuré pour être couplé à une passerelle résidentielle.

14. Dispositif de communication (100) selon une quelconque des revendications 11 à 13,
dans lequel le dispositif de communication (100) est configuré pour fonctionner conformément au procédé suivant une des revendications 2 à 10.

15. Produit de programmes informatiques, comprenant un code de programmes qui, quand il est exécuté par un processeur d'un dispositif de communication (100), amène le dispositif de communication (100) à fonctionner conformément à un procédé selon une quelconque des revendications 1 à 10.

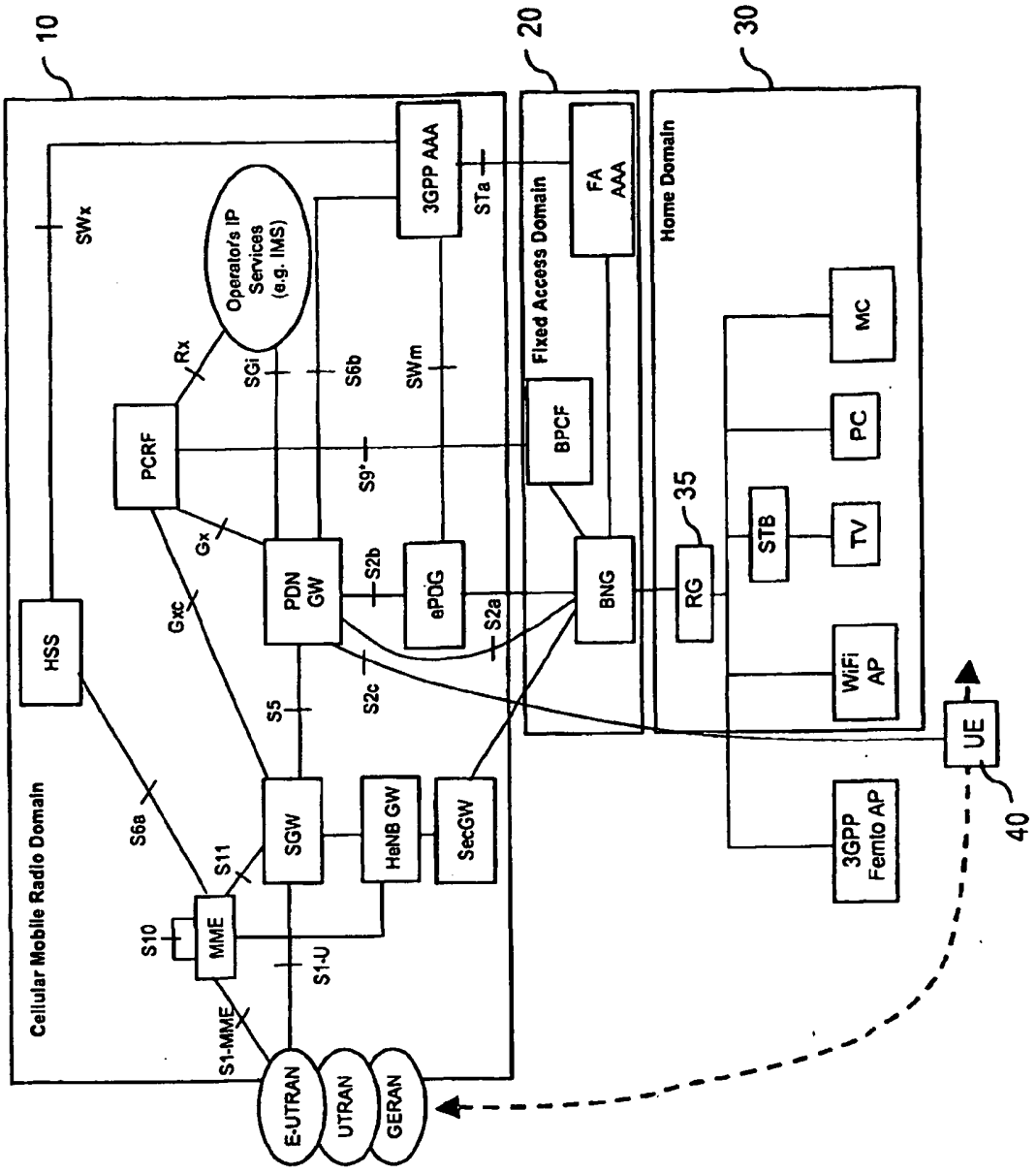
10
20
30
Cellular Mobile Radio Domain
Fixed Access Domain
Home Domain
HSS
SWx
3GPP AAA
STa
FA AAA
Operator's IP Services (e.g. IMS)
Rx
SGi
S6b
SWm
PCRF
BPCF
S9'
Gx
Gxc
PDN GW
S2b
ePDG
S2a
BNG
RG
35
STB
TV
PC
MC
S5
S2c
WiFi AP
UE
40
S6a
S11
SGW
HeNB GW
SecGW
3GPP Femto AP
S10
MME
S1-U
S1-MME
E-UTRAN
UTRAN
GERAN

FIG. 1

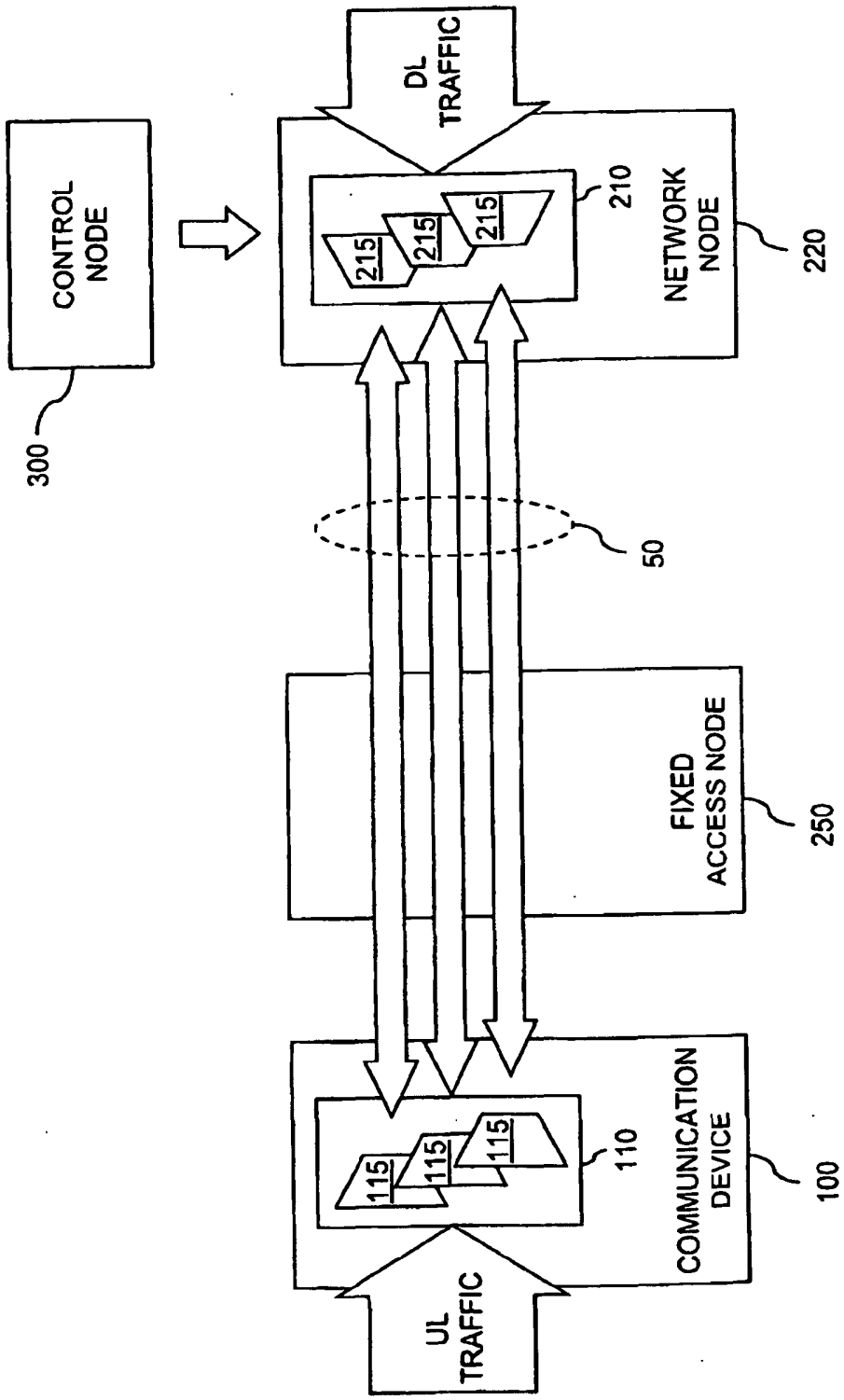
CONTROL NODE
300
DL TRAFFIC
210
215
215
215
NETWORK NODE
220
50
FIXED ACCESS NODE
250
COMMUNICATION DEVICE
100
110
115
115
115
UL TRAFFIC

FIG. 2

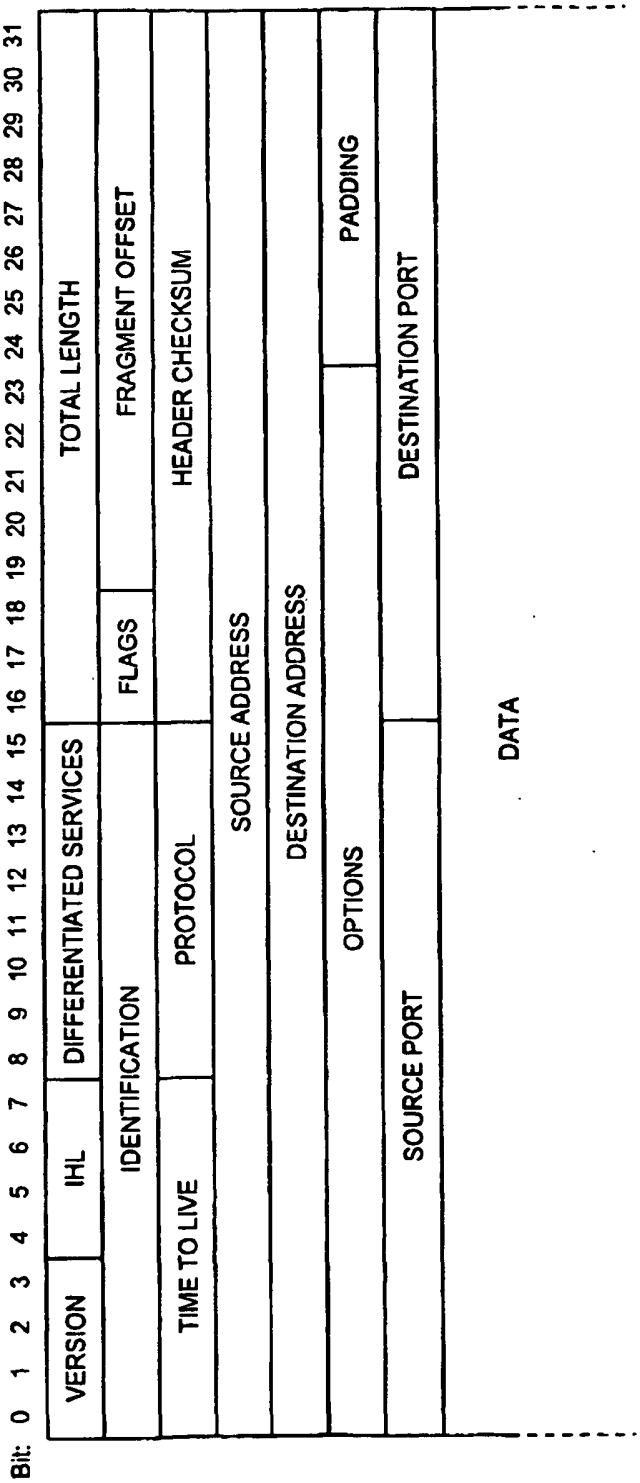
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSION
IHL
DIFFERENTIATED SERVICES
TOTAL LENGTH
IDENTIFICATION
FLAGS
FRAGMENT OFFSET
TIME TO LIVE
PROTOCOL
HEADER CHECKSUM
SOURCE ADDRESS
DESTINATION ADDRESS
OPTIONS
PADDING
SOURCE PORT
DESTINATION PORT
DATA

FIG. 3

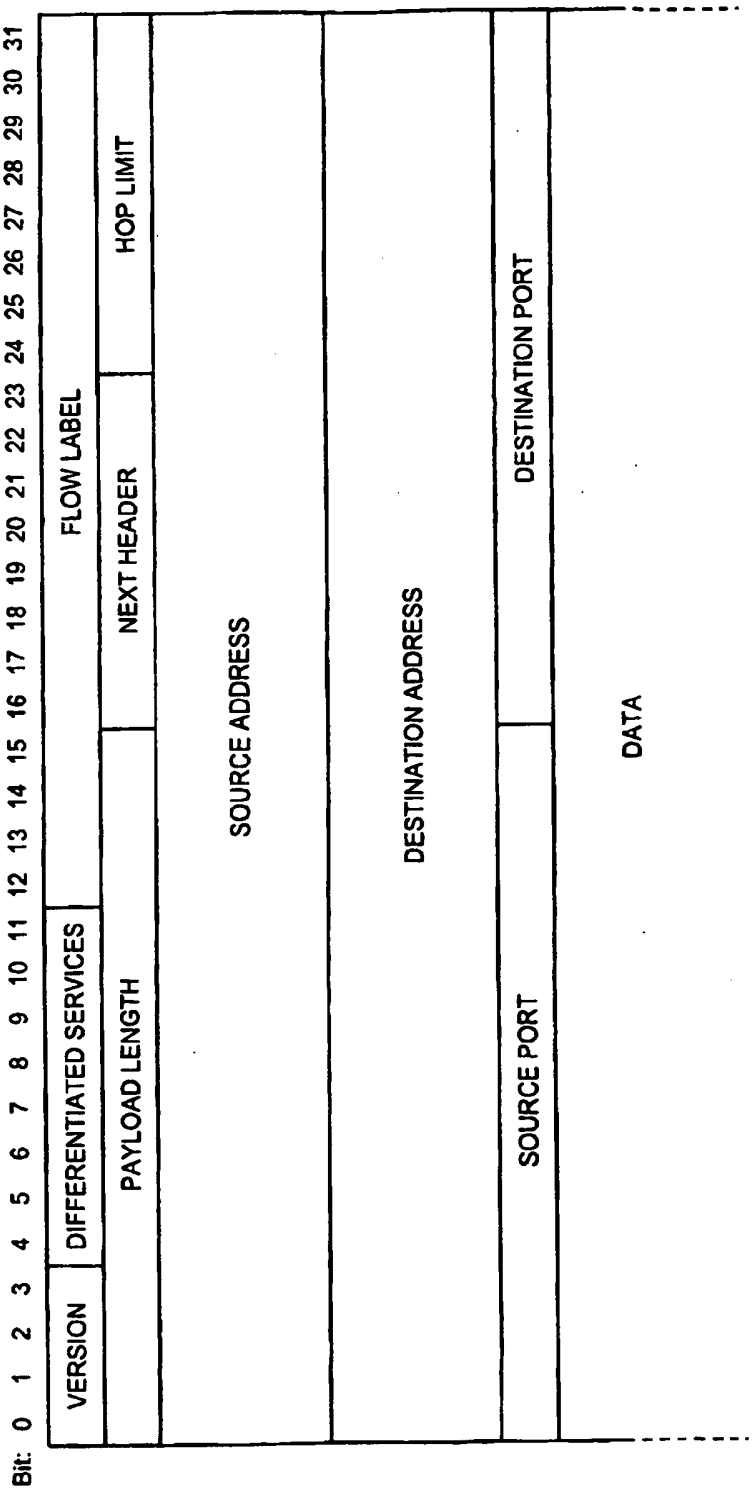
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSION
DIFFERENTIATED SERVICES
FLOW LABEL
PAYLOAD LENGTH
NEXT HEADER
HOP LIMIT
SOURCE ADDRESS
DESTINATION ADDRESS
SOURCE PORT
DESTINATION PORT
DATA

FIG. 4

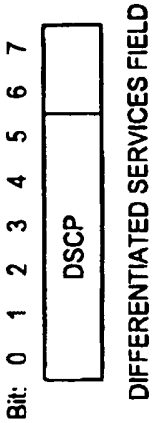

FIG. 5

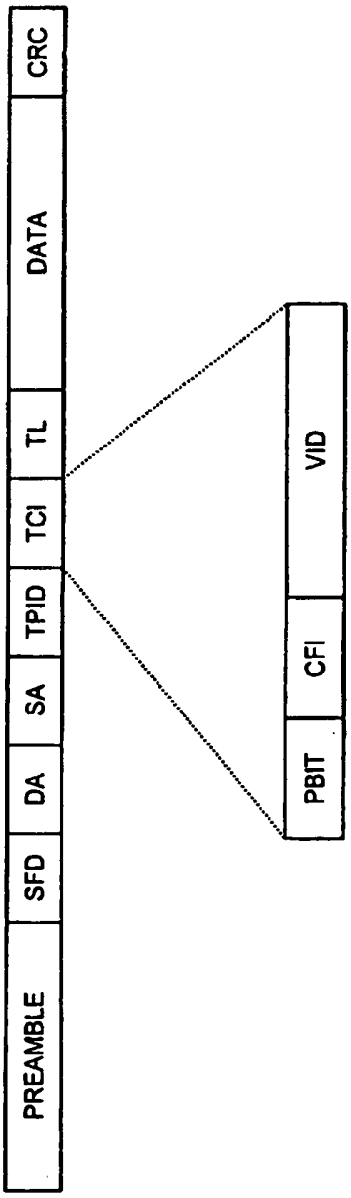

FIG. 6

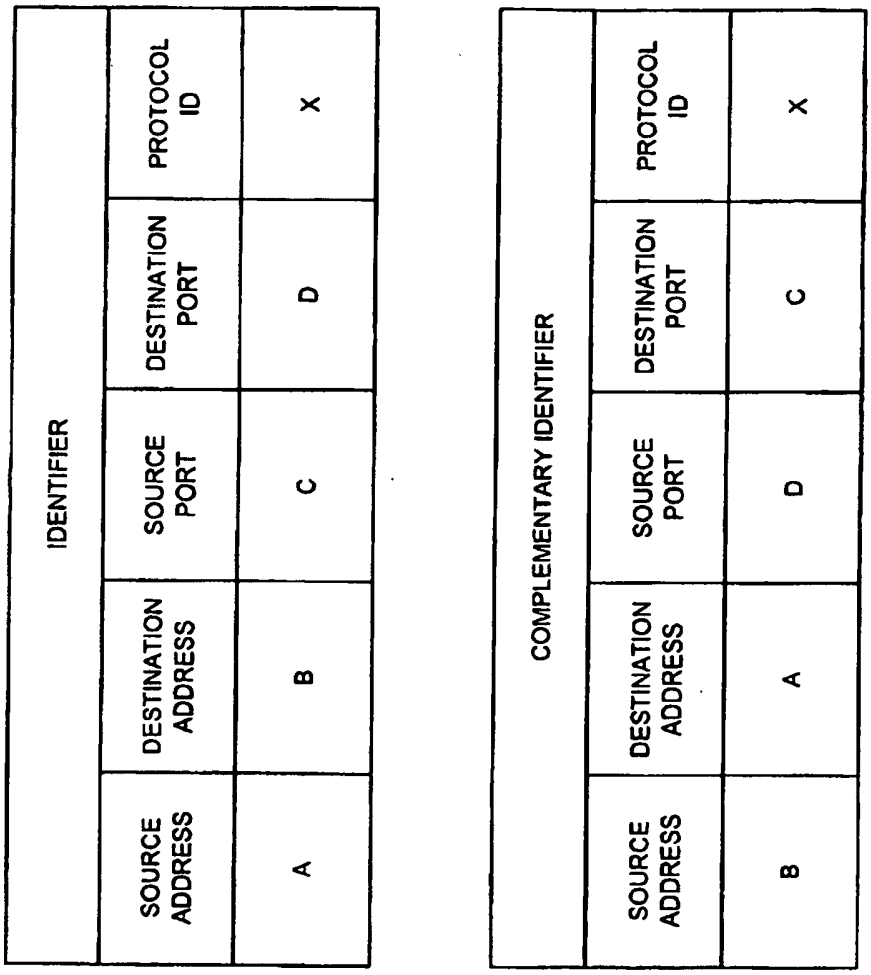
IDENTIFIER
SOURCE ADDRESS
DESTINATION ADDRESS
SOURCE PORT
DESTINATION PORT
PROTOCOL ID
A
B
C
D
X
COMPLEMENTARY IDENTIFIER
SOURCE ADDRESS
DESTINATION ADDRESS
SOURCE PORT
DESTINATION PORT
PROTOCOL ID
B
A
D
C
X

FIG. 7

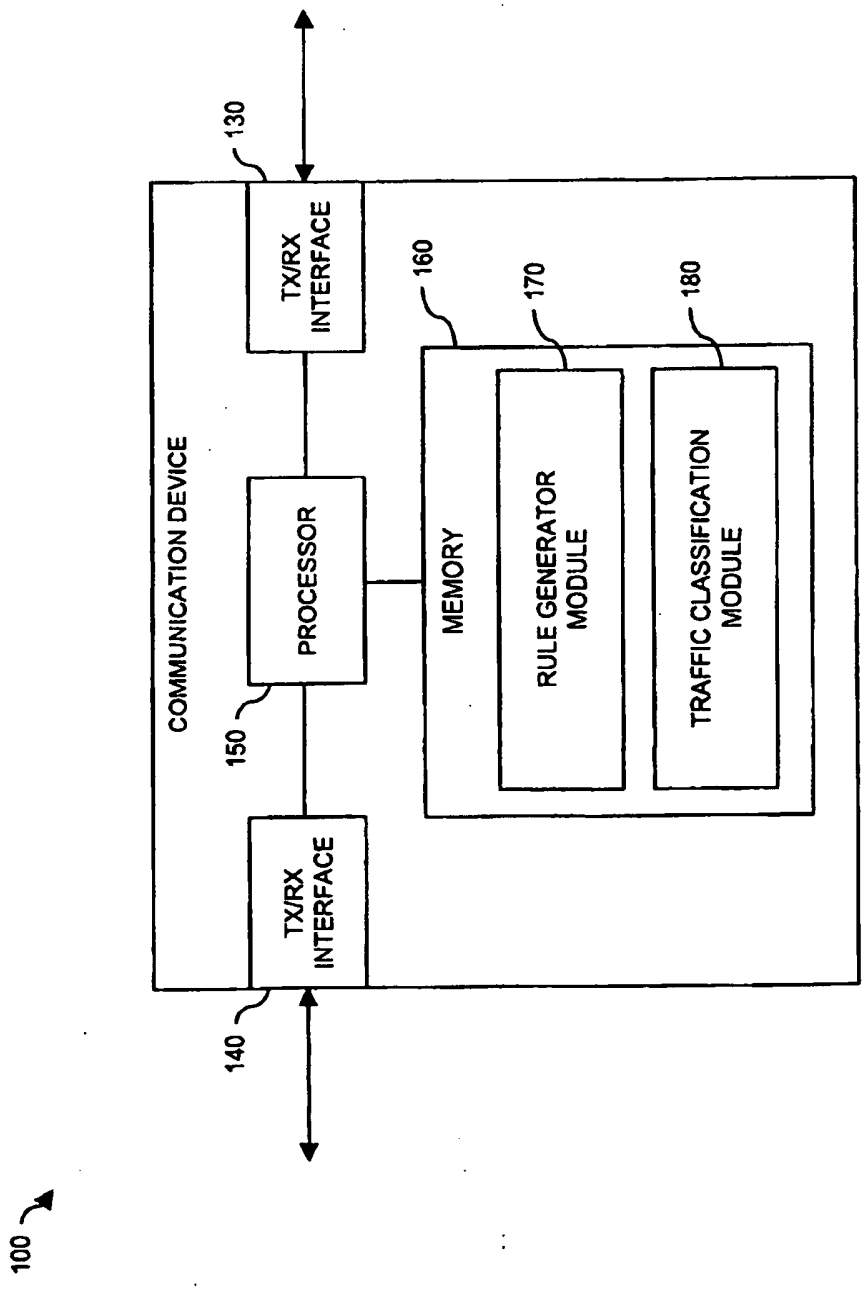
100
COMMUNICATION DEVICE
130
TX/RX INTERFACE
160
170
180
MEMORY
RULE GENERATOR MODULE
TRAFFIC CLASSIFICATION MODULE
PROCESSOR
150
TX/RX INTERFACE
140

FIG. 8

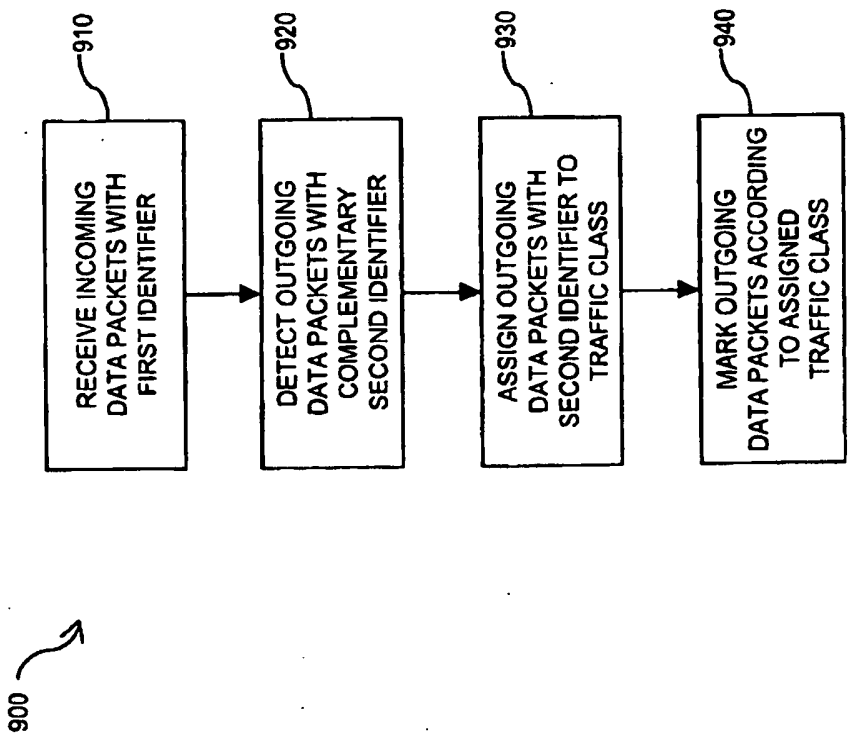
900
910
RECEIVE INCOMING DATA PACKETS WITH FIRST IDENTIFIER
920
DETECT OUTGOING DATA PACKETS WITH COMPLEMENTARY SECOND IDENTIFIER
930
ASSIGN OUTGOING DATA PACKETS WITH SECOND IDENTIFIER TO TRAFFIC CLASS
940
MARK OUTGOING DATA PACKETS ACCORDING TO ASSIGNED TRAFFIC CLASS

FIG. 9

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20070127487 A1 **[0006]**

714244/KOT

HÁLÓZATI FORGALOM KEZELÉSE RÖGZÍTETT CÍMEN KERESZTÜL

Szabadalmi igénypontok

1. Eljárás hálózati forgalomnak kommunikációs eszközben (100) való kezelésére, amely a következőket tartalmazza:

   - bejövő lefelé irányú kapcsolati adatcsomagok vétele rögzített hozzáférésen keresztül a kommunikációs eszközben (100), a lefelé irányú kapcsolati adatcsomagok tartalmaznak egy első azonosítót és hozzá vannak rendelve egy forgalmi osztályhoz (50);
   - a kommunikációs eszköztől (100) a rögzített hozzáférésen keresztül átviendő kimenő felfelé irányú kapcsolati adatcsomagok érzékelése, a kimenő felfelé irányú kapcsolati adatcsomagok tartalmaznak egy második azonosítót, amely kiegészítő az első azonosító vonatkozásában,

   a következőkkel jellemezve:

   az első azonosító tartalmaz egy forráscímet, a kiegészítő második azonosító pedig tartalmaz egy célcímet, amely ugyanaz, mint az első azonosító forráscíme;

   az eljárás a következőket tartalmazza:

   - a második azonosítóval rendelkező érzékelt kimenő felfelé irányú kapcsolati adatcsomagok hozzárendelése ugyanahhoz a forgalmi osztályhoz (50), mint az első azonosítóval rendelkező bejövő lefelé irányú kapcsolati adatcsomagoké.

2. Az 1. igénypont szerinti eljárás, amely a következőket tartalmazza:

   - a vett bejövő lefelé irányú kapcsolati adatcsomagok figyelése; és
   - csomagosztályozási szabály létrehozása a kimenő felfelé irányú kapcsolati adatcsomagoknak a figyelt bejövő lefelé irányú kapcsolati adatcsomagok alapján ugyanahhoz a forgalmi osztályhoz (50) való hozzárendelésére.

3. Az 1. vagy 2. igénypont szerinti eljárás,
   ahol a kimenő felfelé irányú kapcsolati adatcsomagoknak ugyanahhoz a forgalmi osztályhoz (50) való hozzárendelése egy vezérlő jel alapján aktiválódik.

4. Az előző igénypontok egyike szerinti eljárás,
ahol a kimenő felfelé irányú kapcsolati adatcsomagok hozzárendelése szelektíven aktiválódik több forgalmi osztály (50) alcsoportjára.

5. Az előző igénypontok egyike szerinti eljárás, amely a következőket tartalmazza:

- a kimenő felfelé irányú kapcsolati adatcsomagok megjelölése, a jelölés jelzi azt a forgalmi osztályt (50), amelyhez a kimenő felfelé irányú kapcsolati adatcsomagok hozzá vannak rendelve.

6. Az 5. igénypont szerinti eljárás,
ahol a bejövő lefelé irányú kapcsolati adatcsomagok jelzéssel vannak biztosítva, amely jelzi azt a forgalmi osztályt (50), amelyhez a bejövő lefelé irányú kapcsolati adatcsomagok hozzá vannak rendelve; és
ahol a kimenő felfelé irányú kapcsolati adatcsomagok ugyanazzal a jelzéssel vannak megjelölve, mint a bejövő lefelé irányú kapcsolati adatcsomagok.

7. Az 5. vagy 6. igénypont szerinti eljárás,
ahol a kimenő felfelé irányú kapcsolati adatcsomagok jelölése tartalmazza az adatcsomagoknak egy DSCP differenciált szolgáltatások kódpont mezőt, az adatcsomagok elsőbbségi bitjeinek beállítását, az adatcsomagoknak virtuális helyi hálózati címkével való ellátását és/vagy az adatcsomagoknak alagútazonosítóval való ellátását.

8. Az előző igénypontok egyike szerinti eljárás, amely a következőket tartalmazza:

- annak jelzése egy hálózati elemnek (220), hogy a kommunikációs eszköz (100) képes a kimenő felfelé irányú kapcsolati adatcsomagoknak ugyanahhoz a forgalmi osztályhoz (50) való hozzárendelésére.

9. Az előző igénypontok egyike szerinti eljárás,
ahol a kommunikációs eszköz (100) egy lakossági átjáró.

10. Az 1 – 8. igénypontok egyike szerinti eljárás, ahol a kommunikációs eszköz (100) lakossági átjáróhoz csatlakozó mobil végberendezés.

11. Kommunikációs eszköz (100), amely a következőket tartalmazza:

- felület (120), amely arra van kialakítva, hogy bejövő lefelé irányú kapcsolati adatcsomagokat fogadjon rögzített hozzáférésen keresztül egy hálózatból;
- felület (120), amely arra van kialakítva, hogy bejövő lefelé irányú kapcsolati adatcsomagokat fogadjon rögzített hozzáférésen keresztül egy hálózatból;
- forgalom-osztályozó (110), amely arra van kialakítva, hogy érzékelje a bejövő lefelé irányú kapcsolati adatcsomagokat, beleértve egy első azonosítót és kimenő felfelé irányú kapcsolati adatcsomagokat, beleértve egy második azonosítót, amely kiegészíti az első azonosítót,

a következőkkel jellemezve:

az első azonosító tartalmaz egy forráscímet, a kiegészítő második azonosító pedig tartalmaz egy célcímet, amely ugyanaz, mint az első azonosító forráscíme, és a forgalomosztályozó (110) arra van kialakítva, hogy a kiegészítő második azonosítóval rendelkező kimenő felfelé irányú kapcsolati adatcsomagokat hozzárendelje ugyanahhoz a forgalomosztályhoz (50), mint az első azonosítóval rendelkező bejövő lefelé irányú kapcsolati adatcsomagokat.

12. A 11. igénypont szerinti kommunikációs eszköz (100),
ahol a kommunikációs eszköz (100) egy lakossági átjáró.

13. A 11. igénypont szerinti kommunikációs eszköz (100),
ahol a kommunikációs eszköz (100) egy mobil végberendezés, amely arra van kialakítva, hogy csatlakozzon egy lakossági átjáróhoz.

14. A 11 – 13. igénypontok egyike szerinti kommunikációs eszköz (100),
ahol a kommunikációs eszköz (100) arra van kialakítva, hogy a 2 – 10. igénypontok egyike szerinti eljárással összhangban legyen működtetve.

15. Számítógépes programtermék, amely programkódot tartalmaz, amely kommunikációs eszköz (100) processzora általi végrehajtáskor azt eredményezi, hogy a kommunikációs eszköz (100) az 1 – 10. igénypontok egyike szerinti eljárással összhangban működik.