



(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/CN2019/086718

(22) International Filing Date:
13 May 2019 (13.05.2019)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants (*for CN only*): **NOKIA SHANGHAI BELL CO., LTD.** [CN/CN]; No. 388, Ningqiao Road, Pudong Jin-qiao, Shanghai 201206 (CN). **NOKIA SOLUTIONS AND NETWORKS OY** [FI/FI]; Karaportti 3, 02610 Espoo (FI).

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

(72) Inventors: **METSÄLÄ, Esa**; Parolantie 3 E 10, 02200 Espoo (FI). **KANDALA, Anantha**; Hirsalantie 6A 1, 02600 Espoo (FI). **MALKAMÄKI, Esa**; Riippakaivuntie 17 B, 02130 Espoo (FI). **XU, Xiang**; Room 1-1505, No. 218 Hanzhong Road, Nanjing, Jiangsu 210000 (CN). **KOZIOL, Dawid**; Mechaniczna 8, 67-200 Glogow (PL).

(74) Agent: **KING & WOOD MALLESONS**; 20th Floor, East Tower, World Financial Centre, No. 1 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020 (CN).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: MAPPING OF BEARER IDENTIFICATION INTO IPV6 ARCHITECTURE

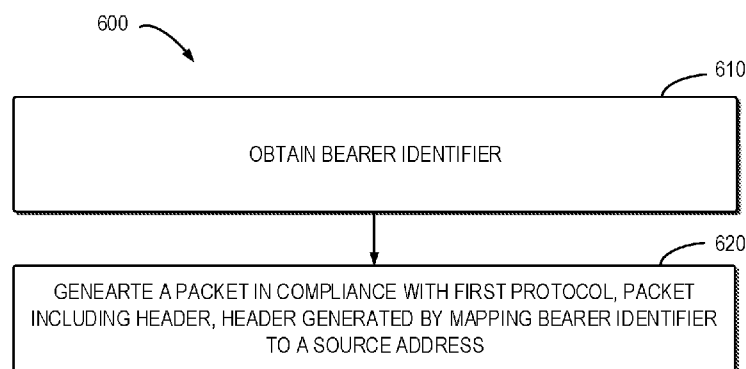


FIG. 6

(57) **Abstract:** Embodiments of the present disclosure relate to apparatuses, methods and computer readable storage media for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture. The first device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the device at least to obtain, from a second device, a bearer identifier indicating a tunnel; and generate a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.. In this way, the intermediate node can access the individual bearer since the TE ID is now visible in the source address of the IPv6 SA even the IPsec is applied.



MAPPING OF BEARER IDENTIFICATION INTO IPV6 ARCHITECTURE

FIELD

[0001] Embodiments of the present disclosure generally relate to the field of telecommunication, and in particular, to methods, devices and computer readable media for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture.

BACKGROUND

[0002] The 3rd Generation Partnership Project (3GPP) determines standards and specifications for new radio (NR) Integrated Access and Backhaul (IAB). In IAB, it is proposed to map general packet radio service (GPRS) tunneling protocol (GTP-U) Tunnel Endpoint Identifier (TE ID) into the flow label in the Internet Protocol Version 6 (IPv6) header.

[0003] 5G RAN requires IPsec for protection of logical interfaces like a front-haul (F1) interface and NG interface. IPsec can be used to create VPN Tunnels to end-to-end IP Traffic (also called as IPsec Transport mode) or site-to-site IPsec Tunnels (between two VPN Gateways, also known as IPsec Tunnel mode). In IPsec Tunnel mode, the original IP packet (IP header and the Data payload) is encapsulated within another packet. In IPsec Transport mode, only the Data Payload is secured by IPsec.

SUMMARY

[0004] In general, example embodiments of the present disclosure provide a solution for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture.

[0005] In a first aspect, there is a first device. The first device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device at least to obtain, from a second device, a bearer identifier indicating a tunnel; and generate a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

[0006] In a second aspect, there is a third device. The third device comprises at least one

processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the third device at least to receive a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer identifier to a first source address; encapsulate the first packet based on a second protocol; map the bearer identifier of the first source address in the first header to a second source address in a second header; and generate a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

[0007] In a third aspect, there is a fourth device. The fourth device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the fourth device at least to receive a first packet in compliance with a first protocol from a first device, the first packet including a first header; determine a bearer identifier in a first source address of the first header; and generate a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

[0008] In a fourth aspect, there is provided a method. The method comprising obtaining, from a second device, a bearer identifier indicating a tunnel; and generating a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

[0009] In a fifth aspect, there is provided a method. The method comprising receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer identifier to a first source address; encapsulating the first packet based on a second protocol; mapping the bearer identifier of the first source address in the first header to a second source address in a second header; and generating a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

[0010] In a sixth aspect, there is provided a method. The method comprising receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header; determining a bearer identifier in a first source address of the first header; and generating a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

[0011] In a seventh aspect, there is provided an apparatus comprises means for means for obtaining, from a second device, a bearer identifier indicating a tunnel; and means for generating a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

[0012] In an eighth aspect, there is provided an apparatus comprises means for means for receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer identifier to a first source address; means for encapsulating the first packet based on a second protocol; means for mapping the bearer identifier of the first source address in the first header to a second source address in a second header; and means for generating a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

[0013] In a ninth aspect, there is provided an apparatus comprises means for means for receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header; means for determining a bearer identifier in a first source address of the first header; and means for generating a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

[0014] In a tenth aspect, there is provided a computer readable medium having a computer program stored thereon which, when executed by at least one processor of a device, causes the device to carry out the method according to the fourth aspect.

[0015] In an eleventh aspect, there is provided a computer readable medium having a computer program stored thereon which, when executed by at least one processor of a device, causes the device to carry out the method according to the fifth aspect.

[0016] In a twelfth aspect, there is provided a computer readable medium having a computer program stored thereon which, when executed by at least one processor of a device, causes the device to carry out the method according to the sixth aspect.

[0017] Other features and advantages of the embodiments of the present disclosure will also be apparent from the following description of specific embodiments when read in conjunction with the accompanying drawings, which illustrate, by way of example, the principles of embodiments of the disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Embodiments of the disclosure are presented in the sense of examples and their advantages are explained in greater detail below, with reference to the accompanying drawings, where

[0019] FIG. 1 shows an example communication network in which example embodiments of the present disclosure may be implemented;

[0020] FIG. 2 shows a schematic diagram of example protocol stack for an IAB architecture;

[0021] FIG. 3 shows a schematic diagram illustrating a process for mapping of a bearer identification into Internet Protocol Version 6 (IPv6) architecture according to example embodiments of the present disclosure;

[0022] FIG. 4 shows a diagram of an example of IPv6 header according to some example embodiments of the present disclosure;

[0023] FIG 5 shows a diagram of example of IPsec modes according to some example embodiments of the present disclosure;

[0024] FIG. 6 shows a flowchart of an example method 600 for mapping of a bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure;

[0025] FIG. 7 shows a flowchart of an example method 700 for mapping of a bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure;

[0026] FIG. 8 shows a flowchart of an example method 800 for mapping of a bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure;

[0027] FIG. 9 shows a simplified block diagram of a device that is suitable for implementing example embodiments of the present disclosure; and

[0028] Fig. 10 shows a block diagram of an example computer readable medium in accordance with some embodiments of the present disclosure.

[0029] Throughout the drawings, the same or similar reference numerals represent the

same or similar element.

DETAILED DESCRIPTION

[0030] Principle of the present disclosure will now be described with reference to some example embodiments. It is to be understood that these embodiments are described only for the purpose of illustration and help those skilled in the art to understand and implement the present disclosure, without suggesting any limitation as to the scope of the disclosure. The disclosure described herein can be implemented in various manners other than the ones described below.

[0031] In the following description and claims, unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skills in the art to which this disclosure belongs.

[0032] As used herein, the term “communication network” refers to a network that follows any suitable communication standards or protocols such as long term evolution (LTE), LTE-Advanced (LTE-A) and 5G NR, and employs any suitable communication technologies, including, for example, MIMO, OFDM, time division multiplexing (TDM), frequency division multiplexing (FDM), code division multiplexing (CDM), Bluetooth, ZigBee, machine type communication (MTC), enhanced mobile broadband (eMBB), massive machine type communications (mMTC) and ultra-reliable low-latency communications (uRLLC) technologies. For the purpose of discussion, in some example embodiments, the LTE network, the LTE-A network, the 5G NR network or any combination thereof is taken as an example of the communication network.

[0033] As used herein, the term “network device” refers to any suitable device at a network side of a communication network. The network device may include any suitable device in an access network of the communication network, for example, including a base station (BS), a relay, an access point (AP), a node B (NodeB or NB), an evolved NodeB (eNodeB or eNB), an NG-RAN node (gNB or ng-eNB), a remote radio module (RRU), a radio header (RH), a remote radio head (RRH), a low power node such as a femto, a pico, a gNB Distributed Unit (DU), an Integrated Access and Backhaul (IAB) node and a gNB Central Unit (CU) and the like. For the purpose of discussion, in some example embodiments, the gNB is taken as an example of the network device.

[0034] The network device may also include any suitable device in a core network, for

example, including multi-standard radio (MSR) radio equipment such as MSR BSs, network controllers such as radio network controllers (RNCs) or base station controllers (BSCs), multi-cell/multicast coordination entities (MCEs), mobile switching centers (MSCs) and MMEs, operation and management (O&M) nodes, Operation Support System (OSS) nodes, self-organization network (SON) nodes, positioning nodes, such as enhanced serving mobile location centers (E-SMLCs), and/or mobile data terminals (MDTs), and 5G Core network nodes such as the access management function (AMF), session management function (SMF).

[0035] As used herein, the term “terminal device” refers to a device capable of, configured for, arranged for, and/or operable for communications with a network device or a further terminal device in a communication network. The communications may involve transmitting and/or receiving wireless signals using electromagnetic signals, radio waves, infrared signals, and/or other types of signals suitable for conveying information over air. In some example embodiments, the terminal device may be configured to transmit and/or receive information without direct human interaction. For example, the terminal device may transmit information to the network device on predetermined schedules, when triggered by an internal or external event, or in response to requests from the network side.

[0036] Examples of the terminal device include, but are not limited to, user equipment (UE) such as smart phones, wireless-enabled tablet computers, laptop-embedded equipment (LEE), laptop-mounted equipment (LME), Mobile Terminals (MT), such as those embedded in IAB nodes and/or wireless customer-premises equipment (CPE). For the purpose of discussion, in the following, some example embodiments will be described with reference to UEs as examples of the terminal devices, and the terms “terminal device” and “user equipment” (UE) may be used interchangeably in the context of the present disclosure.

[0037] As used herein, the term “cell” refers to an area covered by radio signals transmitted by a network device. The terminal device within the cell may be served by the network device and access the communication network via the network device.

[0038] As used herein, the term “circuitry” may refer to one or more or all of the following: (a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry); and (b) combinations of hardware circuits and software, such as (as applicable): (i) a combination of analog and/or digital hardware circuit(s) with

software/firmware and (ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions); and (c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0039] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other computing or network device.

[0040] As used herein, the singular forms “a”, “an”, and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. The term “includes” and its variants are to be read as open terms that mean “includes, but is not limited to”. The term “based on” is to be read as “based at least in part on”. The term “one embodiment” and “an embodiment” are to be read as “at least one embodiment”. The term “another embodiment” is to be read as “at least one other embodiment”. Other definitions, explicit and implicit, may be included below.

[0041] FIG. 1 shows an example communication network 100 in which example embodiments of the present disclosure can be implemented. The communication network 100 includes network devices 110-1, 110-2 and 110-3, which may be collectively referred to as the network device 110. If the communication network 100 is an IAB system, for example, the network devices 110-1 may be referred to as a central unit (CU) of IAB donor and the network devices 110-3 may be referred to a Distributed Unit (DU) of IAB donor. The network devices 110-2 may be referred to a Distributed Unit (DU) of IAB node. The network device 110-1 and network device 110-3 are connected via wired connection, for example, a fiber connection. The network device 110-2 wirelessly connected to the network device 110-3. The wireless connection is also referred as wireless backhaul. The network device 110-2 indirectly connect to network device 110-1 via network device 110-3. The network device 110-3 is also referred as intermediate node.

[0042] The communication network may also comprises a terminal device 120 connected to the network device 110-3. The network device 110-1 may be connected to a gateway 130 which may perform the corresponding security operation for the data transmitted from the network device 110-1. However, the gateway 130 may also be integrated in the network device 110-1. After performing the corresponding security operation, the data may be transmitted to the network device 110-3 either from the network device 110-1 or the gateway 130.

[0043] Further, the network devices 110 may also refer to any of gNB base station, a gNB-DU and a gNB-CU.

[0044] As an example of the communication network 100, the IAB system comprises an IAB donor and one or more IAB nodes. The IAB donor may be implemented as a gNB that terminates wireless backhaul radio interface from one or more IAB nodes. The IAB donor has wired/fiber connectivity with a core network. The IAB donor may include a central unit (CU) and one or more DUs.

[0045] In case where the IAB system is implemented by using the L2-based solutions, the IAB node may include a DU, but does not include CU. In case where the IAB system is implemented by using the L3-based solutions, the IAB node may include a DU or include a DU and a CU.

[0046] In example embodiments, each IAB node logically includes a mobile terminal (MT) that maintains connectivity with one or more upstream nodes (using for example, dual connectivity). Similar to a conventional user equipment which includes an MT, the MT of an IAB node may use radio resource control (RRC) signaling to supply radio link measurements of alternative upstream nodes to its current serving gNB CU. Based on signal strength, signal quality and other factors, a handover of an IAB node to a different upstream node may be triggered by RRC. The Donor-CU may also add or remove dual/Multi-Connectivity (DC/MC) legs by sending RRC Connection Reconfiguration messages. The IAB topology may change over time as radio conditions fluctuate, and as IAB nodes move, are added or removed. Handover and addition or removal of DC legs may be designed to work on a time scale of seconds to minutes, corresponding to macroscopic movement of MTs through a cellular network.

[0047] A CU (such as Donor-CU or CU of an IAB node) may be a logical node which may include the functions (for example, gNB functions) such as transfer of user data,

mobility control, radio access network sharing, positioning, session management etc., except those functions allocated exclusively to DUs. The CU may control the operation of the DUs over a front-haul (F1) interface. A DU is a logical node which may include a subset of the functions (for example, gNB functions), depending on the functional split option. The operations of the DUs may be controlled by the CU.

[0048] The IAB donor may serve directly connected IAB nodes such as the network device 110-2 and IAB node. The IAB donor may also serve directly connected terminal devices (not shown). The IAB node may serve one or more terminal devices directly connected to the IAB node. For example, the IAB node may serve a terminal device 120 directly connected to the IAB node.

[0049] It is to be understood that the number of IAB nodes, the intermediate nodes, and terminal devices connected to the IAB nodes is only for the purpose of illustration without suggesting any limitations. The communication network may include any suitable number of IAB nodes and terminal devices adapted for implementing example embodiments of the present disclosure.

[0050] Currently, 3GPP is working on NR Integrated Access and Backhaul. In an example of IAB architecture, backhauling of F1-U uses an adaptation layer or general packet radio service (GPRS) tunneling protocol (GTP-U) combined with an adaptation layer. FIG. 2 shows an example protocol stack of IAB architecture.

[0051] As shown in FIG. 2, the IP layer carried by adapt is connected to the fronthaul's IP-plane through a routing function at the IAB Donor-DU. On this IP layer, all IAB nodes hold IP addresses, which are routable from the IAB donor CU-CP.

[0052] The IP address assignment to the IAB node could be based on IPv6 Neighbour Discovery Protocol where the DU acts as an IPv6 router sending out ICMPv6 Router Advertisement (RA) over one or more backhaul bearer towards the IAB node. Other methods are not excluded. The extended IP-plane allows native F1-C to be used between an IAB-node DU and IAB-donor CU-CP. Signaling traffic can be prioritized on this IP routing plane using differentiated services code point (DSCP) markings in compliance with TS 38.474. The UE's and the MT's RRC use signaling radio bearer (SRB), which is carried over F1-C.

[0053] Currently, it is required that an IAB node's IPv6 address shall be related to a Donor-DU. This is because when the Donor-CU sends an IP packet (for example,

carrying the F1 application protocol (F1AP) message, or SCTP packet) with destination IP address set to the IAB node's IPv6 address, the IP packet shall be routed to the Donor-DU. That is, Donor-DU is acting as an anchor and the message is routed via the Donor-DU to the IAB node. For the user plane of the IAB Architecture, when the Donor-CU sends a GTP-U packet with destination IP address set to IAB node's address, the GTP-U packet must be routed to the Donor-DU. Then the Donor-DU will route the GTP-U packet to the IAB node. This does not preclude any other IP packet sent to the IAB node, when the destination IP address of the IP packet is set to the IAB node's IPv6 address. These IP packets shall be routed to the Donor-DU.

[0054] 5G RAN requires IPsec for protection of logical interfaces like a front-haul (F1) interface and NG interface. IPsec can be used to create VPN Tunnels to end-to-end IP Traffic (also called as IPsec Transport mode) or site-to-site IPsec Tunnels (between two VPN Gateways, also known as IPsec Tunnel mode). In IPsec Tunnel mode, the original IP packet (IP header and the Data payload) is encapsulated within another packet.

[0055] In IAB, it is proposed to map general packet radio service (GPRS) tunneling protocol (GTP-U) Tunnel Endpoint Identifier (TE ID) into the flow label in the Internet Protocol Version 6 (IPv6) header. This is problematic since the flow label field is 20 bits while GTP-U TE ID is 32 bits.

[0056] If applying the IPsec operation for an IP packet, some information may be hided in the protected field of the IP packet. That is, the intermediate nodes may not read anything except the unprotected fields of the IP packet.

[0057] Moreover, another problem with IPsec is that load balancing/Equal Cost Multipath (ECMP) routing is not possible, since the IPsec hides the upper layer port numbers and there is no entropy in the header fields that are available clear-text.

[0058] Furthermore, active-active load sharing is important since it allows load balancing traffic over multiple links/paths, increasing the utilization of links, and provides resiliency against link failure. With both ECMP multi-path routing and L2 Ethernet link aggregation distribution, it is typically wished to keep conversation together on the same link/path and not deploy packet-based load balancing. This requires identifying the conversation or flow, which is identified typically by source and destination MAC/IP addresses, and source/destination L4 ports. When traffic is protected by IPsec, only the source and destination MAC/IP addresses are visible. Due to this, load balancing does not work since

there is no entropy in these fields.

[0059] Therefore, the present disclosure proposes a solution for routing based on a bearer identifier for IPv6. With the proposed solution, IAB can use IPv6 IPsec while the intermediate node can access the individual bearer since the TE ID is now visible in the source address of the IPv6 SA. Intermediate IAB node reads the TE ID from the IPsec source IPv6 address field which is clear text. Meanwhile, ECMP with IPv6 IPsec is possible, as again now the source IPv6 address field varies and creates necessary entropy. Traffic can be load shared over two or more links in active-active mode on flow (conversation) basis.

[0060] FIG. 3 shows a schematic diagram of a process 300 for mapping of bearer identification into IPv6 architecture according to example embodiments of the present disclosure will be described with reference to FIG. 1. In this example, the process 300 may involve the network device 110 and the gateway 130 as illustrated in FIG. 1.

[0061] In the case shown in FIG.3, the network device 110-2 may allocate radio resources for a terminal device 120 connected with it (for example the terminal device shown in FIG. 3) and allocate 310 a bearer identifier for a Data Radio Bearer (DRB). The network device 110-2 may transmit 320 a message including the bearer identifier to the network device 110-1. This message may be transmitted to the network device 110-1 via one or more intermediate network nodes, for example, the network device 110-3. The bearer identifier may indicate tunnel for a downlink data transmission from the network device 110-1 to the network device 110-2. For example, the tunnel may be a GTP-U tunnel identified by a GTP-U TE ID.

[0062] When the network device 110-1 receives a data packet from, for example, the core network, and then the data packet is to be transmitted from the network device 110-1 to the network device 110-2, the network device 110-1 encapsulate the data packet in a GTP-U packet. The GTP-U packet includes the bearer identifier from the message received from the network device 110-2. The network device 110-1 maps the bearer identifier to a source address in an IPv6 header associated with network device 110-1. The network device 110-1 further generates 330 an IPv6 packet having the IPv6 header, and the GTP-U packet.

[0063] FIG. 4 shows a diagram of an example of IPv6 header 400 according to some example embodiments of the present disclosure. In the IPv6 header 400 as shown in FIG. 4, the bearer identifier obtained from the network device 110-2 may be mapped into the

source address in the source address field 401 of the IPv6 header 400.

[0064] In some example embodiments, the bearer identifier may be mapped into the interface identifier in the source address. The interface identifier may have a length of 64 bit while the bearer identifier may have a length of 32 bit. Thus, the bearer identifier may be mapped into a certain range of the interface identifier, for example, the last 32 bit in the interface identifier.

[0065] Referring back to FIG. 3, the network device 110-1 may transmit the IPv6 packet having the IPv6 header including a bearer identifier to the network device 110-3. The network device 110-3 may extract the bearer identity from the source address of the IP packet and generates 380, based on the bearer identity, a downlink packet including the data packet in compliance with a Backhaul Adaptation Protocol (BAP), to be transmitted to the network device 110-2 over the wireless backhaul.

[0066] In some example embodiments, for the sake of data security, the network device 110-1 may encapsulate the IPv6 packet based on the IPsec. As mentioned above, the IPsec may include two encapsulating mode, i.e. the transport mode and the tunnel mode.

[0067] FIG 5 shows a diagram of example of IPsec modes according to some example embodiments of the present disclosure. The encapsulating process in both modes may be described in detail with reference to FIG. 5 as below.

[0068] FIG. 5 shows an IPv6 packet 510 which may be the IPv6 packet generated by the network device 110-1. As shown in FIG.5, an IPv6 packet 510 may have an original IP header 511. After performing an encapsulating operation based on the IPsec in a transport mode for the IPv6 packet 510, an encapsulated packet 520 is generated which have encapsulated field 522 associated with the IPv6 packet 510. In the transport mode, the field associated with the source address in the original IP header 511 is not changed. That is, the header 521 in the encapsulated packet 520 may be same as the original IP header 511 in the IPv6 packet 510.

[0069] On the contrast, if an encapsulating operation based on the IPsec in a tunnel mode is performed for the IPv6 packet 510, an encapsulated packet 530 is generated which have encapsulated field 532 associated with the IPv6 packet 510. In the tunnel mode, the original IP header 511 may also be encapsulated. Thus, a new IPv6 header 531 is required for the encapsulated packet 530. In this case, the bearer identifier in the source address of the original IP header 511 may be copied to a source address of the new IPv6 header 531 to

ensure the bearer identifier to be seen by the subsequent node for an uplink transmission or a downlink transmission.

[0070] The encapsulating operation based on the IPsec in a tunnel mode may be performed by the network device 110-1. In some example embodiments, for example, the network device 110-1 implement the security gateway function, the network device 110-1 may encapsulate the IPv6 packet and add the new IPv6 header for the encapsulated packet. Similarly, the bearer identifier in the source address of the original IP header may be copied to a source address of the new IPv6 header. The network device 110-1 further transmit 360 the IPv6 packet generated by the network device 110-1 to the network device 110-3. It should be understood that the packet transmitted from the network device 110-1 may be a packet without encapsulating based on the IPsec or an encapsulated packet generated based on one of the encapsulating mode of the encapsulating operation above.

[0071] In some example embodiments, the encapsulating operation based on the IPsec in a tunnel mode may also be performed by an external device, for example, the gateway 130. Referring back to FIG. 3, in some example embodiments, the network device 110-1 may transmit 340 the IPv6 packet to a security gateway 130. The security gateway may encapsulate 350 the IPv6 packet in an IPsec packet, and add the new IPv6 header for the encapsulated packet. Similarly, the bearer identifier in the source address of the original IP header may be copied to a source address of the new IPv6 header. The security gateway may transmit 370 the encapsulated packet to the network device 110-3.

[0072] Upon the network device 110-3 received the IPsec packet from the network device 110-1, or from the gateway 130, the network device 110-3 may also extract the bearer identity from the source address of the IPsec packet. The network device 110-3 may generate 380, based on the bearer identity, a downlink packet including the data packet in compliance with a Backhaul Adaptation Protocol (BAP), to be transmitted to the network device 110-2 over the wireless backhaul. The bearer identity may be mapped to another bearer identity in the Backhaul Adaptation Protocol header or the bearer identity may be used to select the backhaul (BH) Radio Link Control (RLC) channel/bearer. The latter implies that the bearer identity is mapped to a logical channel identity identifying the BH RLC channel/bearer.

[0073] In this way, IAB can use IPv6 IPsec while the intermediate node can access the individual bearer since the TE ID is now visible in the source address of the IPv6 header.

The intermediate node(s) reads the TE ID from the IPsec source IPv6 address field which is clear text.

[0074] Furthermore, as described above, with both ECMP multi-path routing and L2 Ethernet link aggregation distribution, it is typically wished to keep conversation together on the same link/path and not deploy packet-based load balancing.

[0075] With IPsec tunnel mode, the IPv6 source address of the Outer IP header includes TE ID. This means that for each new bearer (e.g. conversation), a separate IPsec tunnel source address exists.

[0076] With IPsec transport mode, there is no separate IPsec tunnel source address, but the original IPv6 source address is visible. Thus, with IPsec transport mode, similarly each new conversation can be identified by the IPv6 source address (with TE ID included to the interface ID portion).

[0077] It should be noted that the load balancing with ECMP and/or Link aggregation is possible on any network node on the path from a gNB to the core network, also in general between any two mobile network elements that have GTP-U tunnel.

[0078] For example, in case of a path from a gNB to a User Plane Function (UPF), the gNB maps the TE ID allocated by UPF, to its IPv6 source address field, for the uplink direction. For the downlink direction, the UPF maps the TE ID allocated by the gNB, to its IPv6 source address field. In case of a path from a gNB-CU and a gNB-DU, the TE ID allocated by CU is mapped by DU to its' source IPv6 address. The TE ID allocated by DU is mapped by CU to its' source IPv6 address.

[0079] For load sharing with ECMP, common fields as below are used as an example:

source MAC address (source MAC visible)

destination MAC address (destination MAC visible)

source IP address (outer source IP visible with IPsec)

destination IP address (outer destination IP visible with IPsec)

L4 source port (source port not visible with IPsec)

L4 destination port (source port not visible with IPsec)

protocol (outer visible with IPsec)

[0080] With IPsec tunnel mode, the IPsec tunnel source address varies, when TE ID is

included into IPv6 source address as proposed. This means that it is possible to have ECMP load sharing hash algorithm divide traffic into a link and a further link on TEID basis. It should be understood that there can be any number of equal cost paths. With IPsec transport mode, there is only single IP source address, which varies due to TEID.

5 Any intermediate router/switch element may now load share traffic using ECMP or Link aggregation.

[0081] Same issue exists with Ethernet layer. Distribution algorithm is not standardized by IEEE802.1ax.

[0082] Ethernet Link aggregation (802.1ax) can divide traffic into two (or more) links, once again typically based on the same input and additionally Ethernet Source and destination MAC addresses, and the Ethertype:

10

source IP address (outer source IP visible with IPsec)

destination IP address (outer destination IP visible with IPsec)

source MAC address (source MAC visible)

15 destination MAC address (destination MAC visible)

L4 source port (source port not visible with IPsec)

L4 destination port (source port not visible with IPsec)

[0083] With the solution, the source IPv6 address varies on conversation basis as it includes TE ID, even if all other fields are identical. When the Link Aggregation distribution algorithm utilizes also source IP, the IPsec tunnel traffic can be distributed.

20 Any intermediate router/switch element may now load share traffic using ECMP or Link aggregation.

[0084] More details of the example embodiments in accordance with the present disclosure will be described with reference to FIGs. 6-8.

[0085] FIG. 6 shows a flowchart of an example method 600 for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure. The method 600 can be implemented at the network device 110-1 as shown in FIG. 1. For the purpose of discussion, the method 600 will be described with reference to FIG. 1.

25

[0086] At 610, the network device 110-1 obtains a bearer identifier indicating a tunnel

30

from the network device 110-2.

[0087] In some example embodiments, the network device 110-1 may map the bearer identifier into an interface identifier of the first source address, generate the first header based on the mapped interface identifier and generate the first packet based on the first header.

[0088] At 620, the network device 110-1 generates a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

[0089] In some example embodiments, the network device 110-1 may further encapsulate the first packet based on a second protocol without changing a field associated with the first source address in the first header.

[0090] In some example embodiments, the network device 110-1 may further encapsulate the first packet based on a second protocol, map the first source address in the first header to a second source address in a second header and generate a second packet in compliance with the first protocol based on the encapsulated packet and the second header.

[0091] In some example embodiments, the network device 110-1 may further transmit the first packet to a gateway 130 for encapsulating the first packet based on a second protocol.

[0092] In some example embodiments, the second protocol is an Internet Protocol Security suite of protocols in transport mode.

[0093] In some example embodiments, the second protocol is an Internet Protocol Security suite of protocols in tunnel mode.

[0094] In some example embodiments, the network device 110-1 may further transmit the first packet to a fourth device to enable the fourth device to obtain the bearer identifier.

[0095] In some example embodiments, the first protocol is an Internet Protocol Version 6.

[0096] FIG. 7 shows a flowchart of an example method 700 for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure. The method 700 can be implemented at the gateway 130 as shown in FIG. 1. For the purpose of discussion, the method 700 will be described with reference to FIG. 1.

[0097] At 710, the gateway 130 receives a first packet in compliance with a first protocol from a network device 110-1, the first packet including a first header, the first header

generated by mapping a bearer identifier to a first source address.

[0098] At 720, the gateway 130 encapsulates the first packet based on a second protocol.

[0099] At 730, the gateway 130 maps the bearer identifier of the first source address in the first header to a second source address in a second header.

5 [00100] At 740, the gateway 130 generates a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

[00101] In some example embodiments, the second protocol is an Internet Protocol Security suite of protocols in tunnel mode.

[00102] In some example embodiments, the first protocol is an Internet Protocol Version 6.

10 [00103] FIG. 8 shows a flowchart of an example method 800 for mapping of bearer identification into Internet Protocol Version 6 (IPv6) architecture according to some example embodiments of the present disclosure. The method 800 can be implemented at the network device 110-3 as shown in FIG. 1. For the purpose of discussion, the method 800 will be described with reference to FIG. 1.

15 [00104] At 810, the network device 110-3 receives a first packet in compliance with a first protocol from a network device 110-1, the first packet including a first header.

[00105] At 820, the network device 110-3 determines a bearer identifier in a first source address of the first header.

20 [00106] At 830, the network device 110-3 generates a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel. The third packet may include a third header generated by mapping the bearer identifier to a further bearer identifier in the third header. Alternatively, the bearer identifier is used for mapping of the third packet to a backhaul radio link control (RLC) channel and the corresponding logical channel identity (LCID).

25 [00107] In some example embodiments, the first protocol is an Internet Protocol Version 6 and the third protocol is Backhaul Adaptation Protocol.

[00108] In some example embodiments, an apparatus capable of performing the method 600 (for example, implemented at network device 110-1) may comprise means for performing the respective steps of the method 600. The means may be implemented in
30 any suitable form. For example, the means may be implemented in a circuitry or software module.

[00109] In some example embodiments, the apparatus comprises means for obtaining, from a second device, a bearer identifier indicating a tunnel; and means for generating a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

[00110] In some example embodiments, an apparatus capable of performing the method 700 (for example, implemented at the gateway 130) may comprise means for performing the respective steps of the method 700. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[00111] In some example embodiments, the apparatus comprises means for receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer identifier to a first source address; means for encapsulating the first packet based on a second protocol; means for mapping the bearer identifier of the first source address in the first header to a second source address in a second header; and means for generating a second packet in compliance with the first protocol based on the encapsulated packet and the second header.

[00112] In some example embodiments, an apparatus capable of performing the method 800 (for example, implemented at the network device 110-3) may comprise means for performing the respective steps of the method 800. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[00113] In some example embodiments, the apparatus comprises means for receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header; means for determining a bearer identifier in a first source address of the first header; and means for generating a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

[00114] FIG. 9 is a simplified block diagram of a device 900 that is suitable for implementing embodiments of the present disclosure. The device 900 may be provided to implement the communication device, for example the network device 110 as shown in Fig. 1. As shown, the device 900 includes one or more processors 910, one or more memories 940 coupled to the processor 910, and one or more transmitters and/or receivers (TX/RX) 940 coupled to the processor 910.

[00115] The TX/RX 940 is for bidirectional communications. The TX/RX 940 has at least one antenna to facilitate communication. The communication interface may represent any interface that is necessary for communication with other network elements.

[00116] The processor 910 may be of any type suitable to the local technical network and may include one or more of the following: general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The device 900 may have multiple processors, such as an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[00117] The memory 920 may include one or more non-volatile memories and one or more volatile memories. Examples of the non-volatile memories include, but are not limited to, a Read Only Memory (ROM) 924, an electrically programmable read only memory (EPROM), a flash memory, a hard disk, a compact disc (CD), a digital video disk (DVD), and other magnetic storage and/or optical storage. Examples of the volatile memories include, but are not limited to, a random access memory (RAM) 922 and other volatile memories that will not last in the power-down duration.

[00118] A computer program 930 includes computer executable instructions that are executed by the associated processor 910. The program 930 may be stored in the ROM 930. The processor 910 may perform any suitable actions and processing by loading the program 930 into the RAM 920.

[00119] The embodiments of the present disclosure may be implemented by means of the program 930 so that the device 900 may perform any process of the disclosure as discussed with reference to FIGs. 3 to 8. The embodiments of the present disclosure may also be implemented by hardware or by a combination of software and hardware.

[00120] In some embodiments, the program 930 may be tangibly contained in a computer readable medium which may be included in the device 900 (such as in the memory 920) or other storage devices that are accessible by the device 900. The device 900 may load the program 930 from the computer readable medium to the RAM 922 for execution. The computer readable medium may include any types of tangible non-volatile storage, such as ROM, EPROM, a flash memory, a hard disk, CD, DVD, and the like. Fig. 10 shows an example of the computer readable medium 1000 in form of CD or DVD. The computer readable medium has the program 930 stored thereon.

[00121] Generally, various embodiments of the present disclosure may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. Some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device. While various aspects of embodiments of the present disclosure are illustrated and described as block diagrams, flowcharts, or using some other pictorial representations, it is to be understood that the block, apparatus, system, technique or method described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

[00122] The present disclosure also provides at least one computer program product tangibly stored on a non-transitory computer readable storage medium. The computer program product includes computer-executable instructions, such as those included in program modules, being executed in a device on a target real or virtual processor, to carry out the methods 500 and 600 as described above with reference to FIGs. 2-6. Generally, program modules include routines, programs, libraries, objects, classes, components, data structures, or the like that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or split between program modules as desired in various embodiments. Machine-executable instructions for program modules may be executed within a local or distributed device. In a distributed device, program modules may be located in both local and remote storage media.

[00123] Program code for carrying out methods of the present disclosure may be written in any combination of one or more programming languages. These program codes may be provided to a processor or controller of a general purpose computer, special purpose computer, or other programmable data processing apparatus, such that the program codes, when executed by the processor or controller, cause the functions/operations specified in the flowcharts and/or block diagrams to be implemented. The program code may execute entirely on a machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or server.

[00124] In the context of the present disclosure, the computer program codes or related data may be carried by any suitable carrier to enable the device, apparatus or processor to perform various processes and operations as described above. Examples of the carrier include a signal, computer readable medium, and the like.

[00125] The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable medium may include but not limited to an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific
5 examples of the computer readable storage medium would include an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable
10 combination of the foregoing.

[00126] Further, while operations are depicted in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be
15 advantageous. Likewise, while several specific implementation details are contained in the above discussions, these should not be construed as limitations on the scope of the present disclosure, but rather as descriptions of features that may be specific to particular embodiments. Certain features that are described in the context of separate embodiments may also be implemented in combination in a single embodiment. Conversely, various
20 features that are described in the context of a single embodiment may also be implemented in multiple embodiments separately or in any suitable sub-combination.

[00127] Although the present disclosure has been described in languages specific to structural features and/or methodological acts, it is to be understood that the present disclosure defined in the appended claims is not necessarily limited to the specific features
25 or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

WHAT IS CLAIMED IS:

1. A first device comprising:

at least one processor; and

at least one memory including computer program codes;

5 the at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device at least to:

obtain, from a second device, a bearer identifier indicating a tunnel; and

generate a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first
10 source address in the first header.

2. The first device of claim 1, wherein the first device is caused to generate the first packet by:

mapping the bearer identifier into an interface identifier of the first source address;

15 generating the first header based on the mapped interface identifier; and

generating the first packet based on the first header.

3. The first device of claim 1, wherein the first device is further caused to:

encapsulate the first packet based on a second protocol without changing a field

20 associated with the first source address in the first header.

4. The first device of claim 3, wherein the second protocol is an Internet Protocol Security suite of protocols in transport mode.

5. The first device of claim 1, wherein the first device is further caused to:

encapsulate the first packet based on a second protocol;

map the first source address in the first header to a second source address in a second header; and

generate a second packet in compliance with the second protocol based on the
30 encapsulated packet and the second header.

6. The first device of claim 1, wherein the first device is further caused to:

transmit the first packet to a third device for encapsulating the first packet based on

a second protocol.

7. The first device of Claim 5 or 6, wherein the second protocol is an Internet Protocol Security suite of protocols in tunnel mode.

5

8. The first device of Claim 6, wherein the third device is a security gateway.

9. The first device of Claim 1, wherein the first device is a network device and the second device is a network device.

10

10. The first device of claim 1, wherein the first device is further caused to:
transmit the first packet to a fourth device to enable the fourth device to obtain the bearer identifier.

15

11. The first device of claim 1 or 5, wherein the first protocol is an Internet Protocol Version 6.

12. A third device comprising:

at least one processor; and

20

at least one memory including computer program codes;

the at least one memory and the computer program codes are configured to, with the at least one processor, cause the third device at least to:

receive a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer identifier to a first source address;

25

encapsulate the first packet based on a second protocol;

map the bearer identifier of the first source address in the first header to a second source address in a second header; and

generate a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

30

13. The third device of Claim 12, wherein the third device comprises security gateway.

14. The third device of Claim 12, wherein the second protocol is an Internet Protocol Security suite of protocols in tunnel mode.

15. The third device of claim 12, wherein the first device is a network device.

16. The third device of claim 12, wherein the first protocol is an Internet Protocol Version 6.

17. A fourth device comprising:
at least one processor; and
at least one memory including computer program codes;
the at least one memory and the computer program codes are configured to, with the at least one processor, cause the fourth device at least to:
receive a first packet in compliance with a first protocol from a first device,
the first packet including a first header;
determine a bearer identifier in a first source address of the first header; and
generate a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

18. The fourth device of Claim 17, wherein the first device is a network device and the fourth device is a network device.

19. The third device of claim 17, wherein the first protocol is an Internet Protocol Version 6 and the third protocol is Backhaul Adaptation Protocol.

20. A method comprising:
obtaining, from a second device, a bearer identifier indicating a tunnel; and
generating a first packet in compliance with a first protocol, the first packet including a first header, the first header generated by mapping the bearer identifier to a first source address in the first header.

21. The method of Claim 20, wherein generating the first packet comprises:
mapping the bearer identifier into an interface identifier of the first source address;
generating the first header based on the mapped interface identifier; and

generating the first packet based on the first header.

22. The method of Claim 20, further comprising:

encapsulating the first packet based on a second protocol without changing a field
5 associated with the first source address in the first header.

23. The method of Claim 22, wherein the second protocol is an Internet Protocol
Security suite of protocols in transport mode.

10 24. The method of Claim 20, further comprising:

encapsulating the first packet based on a second protocol;
mapping the first source address in the first header to a second source address in a
second header; and

generating a second packet in compliance with the first protocol based on the
15 encapsulated packet and the second header.

25. The method of Claim 20, further comprising:

transmitting the first packet to a third device for encapsulating the first packet
based on a second protocol.

20 26. The method of Claim 24 or 25, wherein the second protocol is an Internet
Protocol Security suite of protocols in tunnel mode.

27. The method of Claim 25, wherein the third device is a security gateway.

25 28. The method of Claim 20, wherein the first device is a network device and the
second device is a network device.

29. The method of Claim 20, further comprising:

30 transmitting the first packet to a fourth device to enable the fourth device to obtain
the bearer identifier.

30. The method of Claim 20 or 24, wherein the first protocol is an Internet
Protocol Version 6.

31. A method comprising:

receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header, the first header generated by mapping a bearer

5 identifier to a first source address;

encapsulating the first packet based on a second protocol;

mapping the bearer identifier of the first source address in the first header to a second source address in a second header; and

10 generating a second packet in compliance with the second protocol based on the encapsulated packet and the second header.

32. The method of Claim 31, wherein the third device comprises security gateway.

33. The method of Claim 31, wherein the second protocol is an Internet Protocol
15 Security suite of protocols in tunnel mode.

34. The method of Claim 31, wherein the first device is a network device.

35. The method of Claim 31, wherein the first protocol is an Internet Protocol
20 Version 6.

36. A method comprising:

receiving a first packet in compliance with a first protocol from a first device, the first packet including a first header;

25 determining a bearer identifier in a first source address of the first header; and

generating a third packet in compliance with a third protocol based on the bearer identifier to enable the third packet to be mapped to a backhaul channel.

37. The method of Claim 36, wherein the first device is a network device and the
30 fourth device is a network device.

38. The method of Claim 36, wherein the first protocol is an Internet Protocol Version 6 and the third protocol is Backhaul Adaptation Protocol.

39. An apparatus, comprising:

means for obtaining, from a second device, a bearer identifier indicating a tunnel;

and

means for generating a first packet in compliance with a first protocol, the first
5 packet including a first header, the first header generated by mapping the bearer identifier
to a first source address in the first header.

40. An apparatus, comprising:

means for receiving a first packet in compliance with a first protocol from a first
10 device, the first packet including a first header, the first header generated by mapping a
bearer identifier to a first source address;

means for encapsulating the first packet based on a second protocol;

means for mapping the bearer identifier of the first source address in the first
header to a second source address in a second header; and

15 means for generating a second packet in compliance with the second protocol
based on the encapsulated packet and the second header.

41. An apparatus, comprising:

means for receiving a first packet in compliance with a first protocol from a first
20 device, the first packet including a first header;

means for determining a bearer identifier in a first source address of the first
header; and

means for generating a third packet in compliance with a third protocol based on
the bearer identifier to enable the third packet to be mapped to a backhaul channel.

25 42. A non-transitory computer readable medium comprising program instructions
for causing an apparatus to perform at least the method of any of claims 20-30.

43. A non-transitory computer readable medium comprising program instructions
30 for causing an apparatus to perform at least the method of any of claims 31-35.

44. A non-transitory computer readable medium comprising program instructions
for causing an apparatus to perform at least the method of any of claims 36-38.

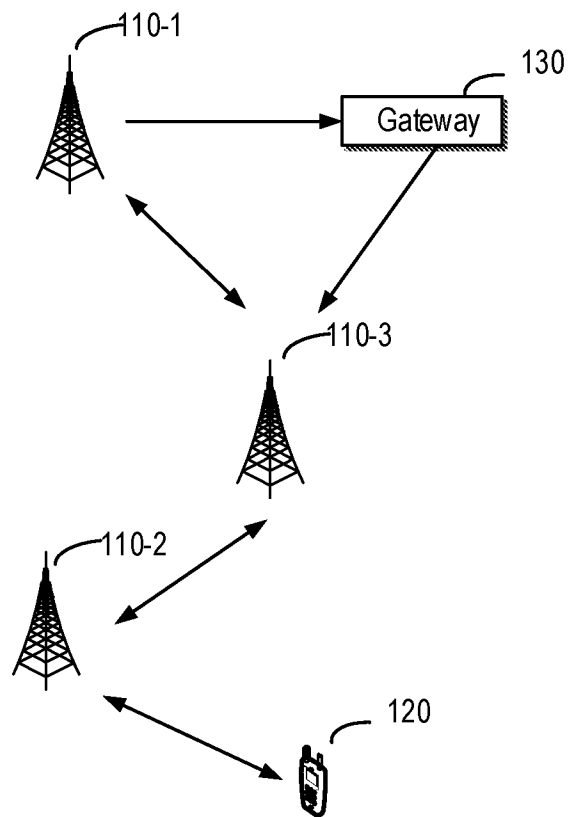


FIG. 1

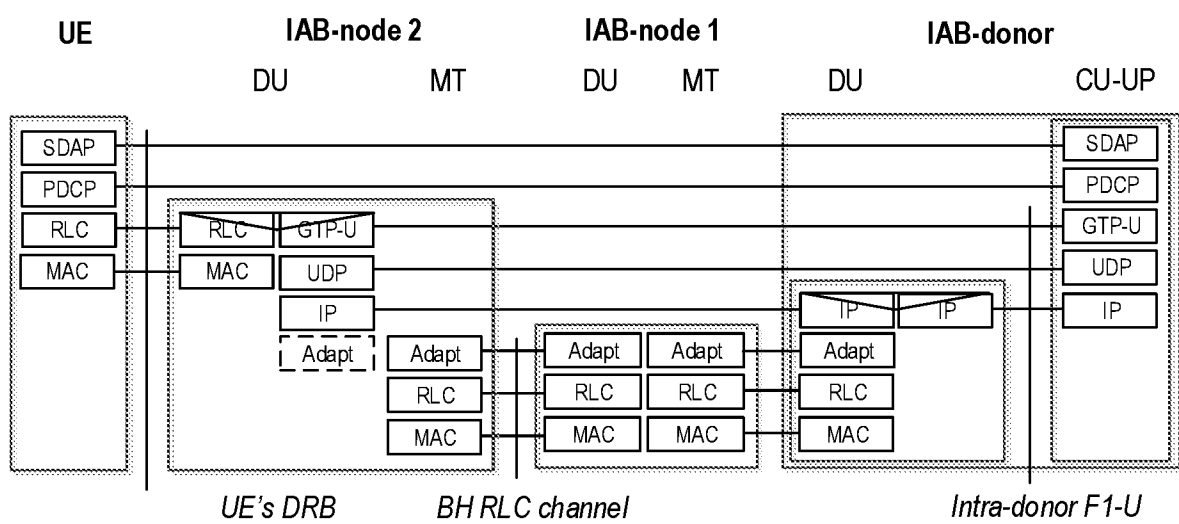


FIG. 2

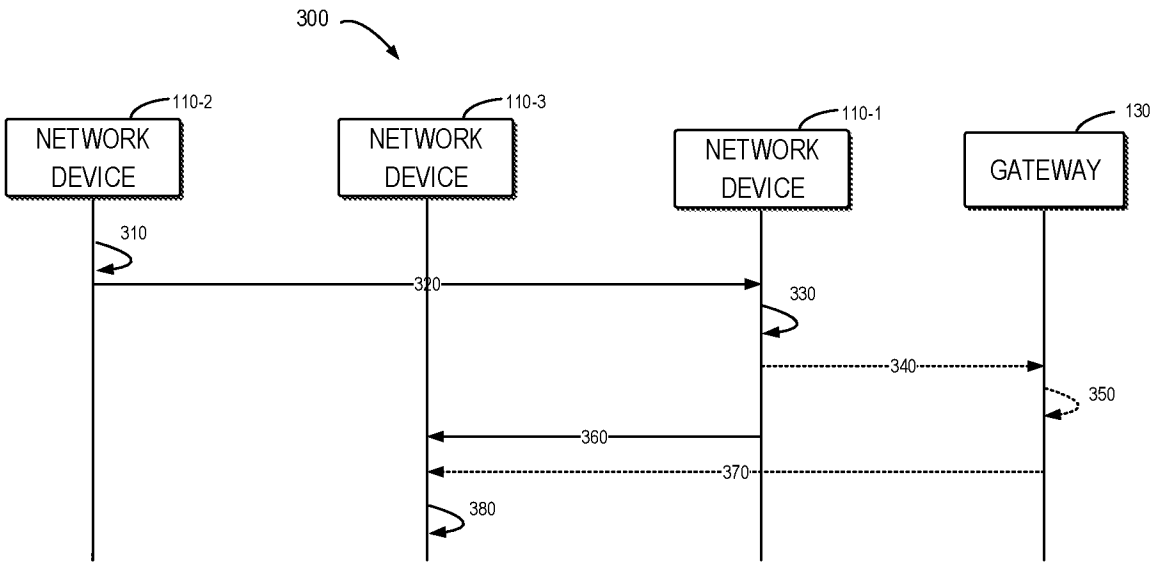


FIG. 3

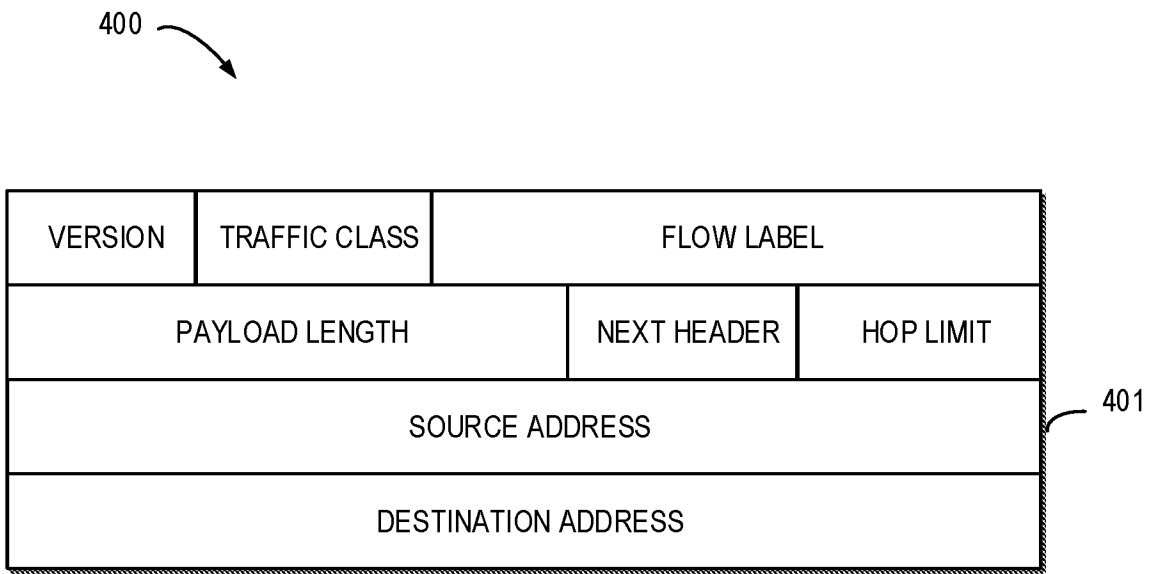


FIG. 4

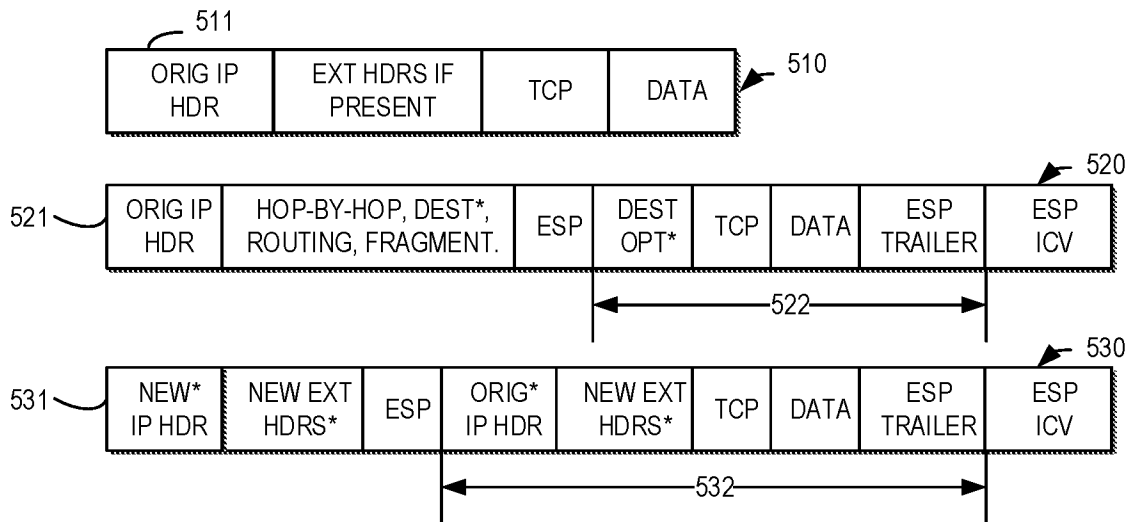


FIG. 5

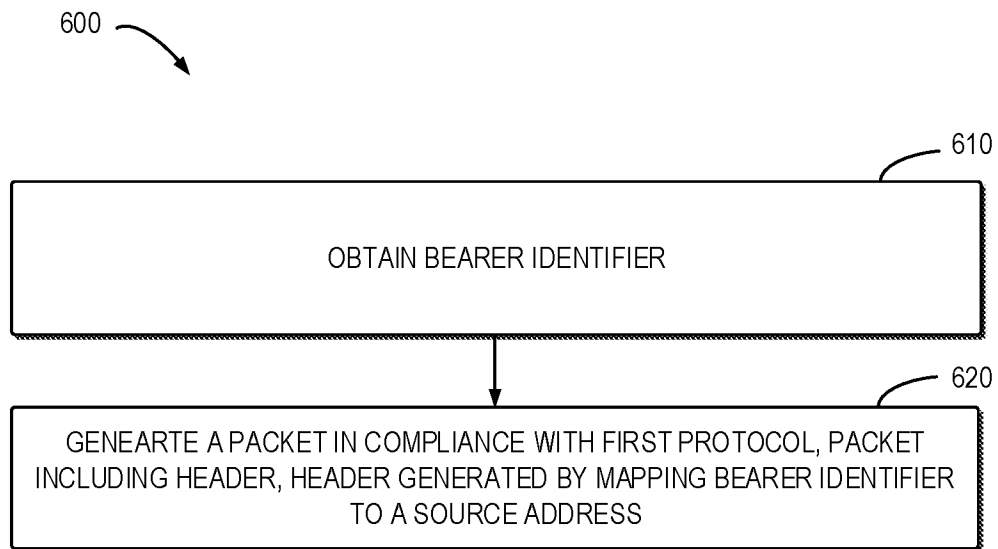
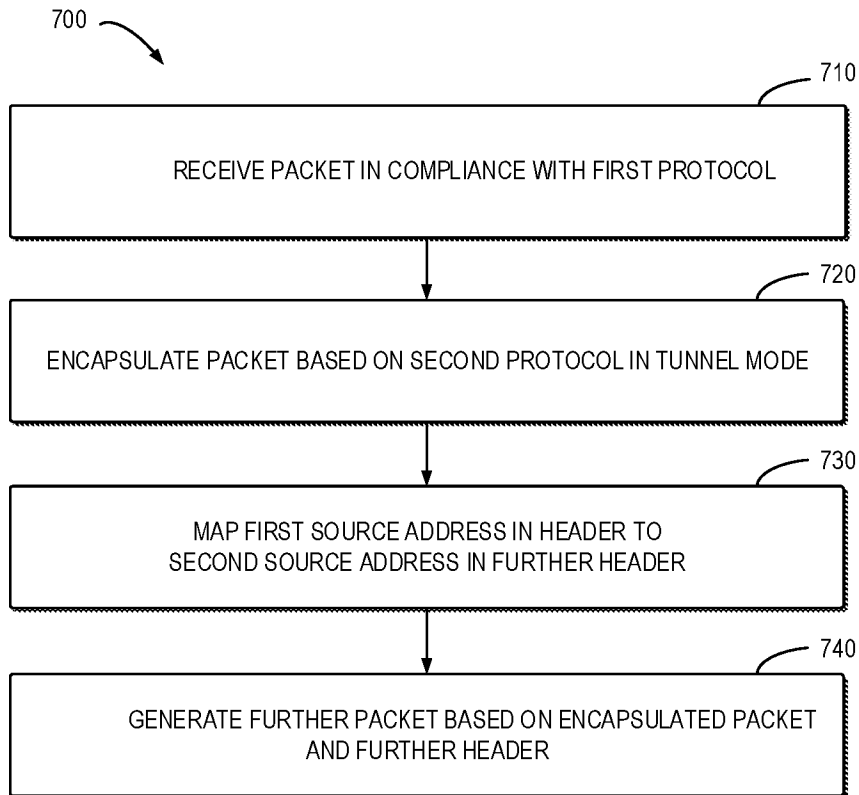
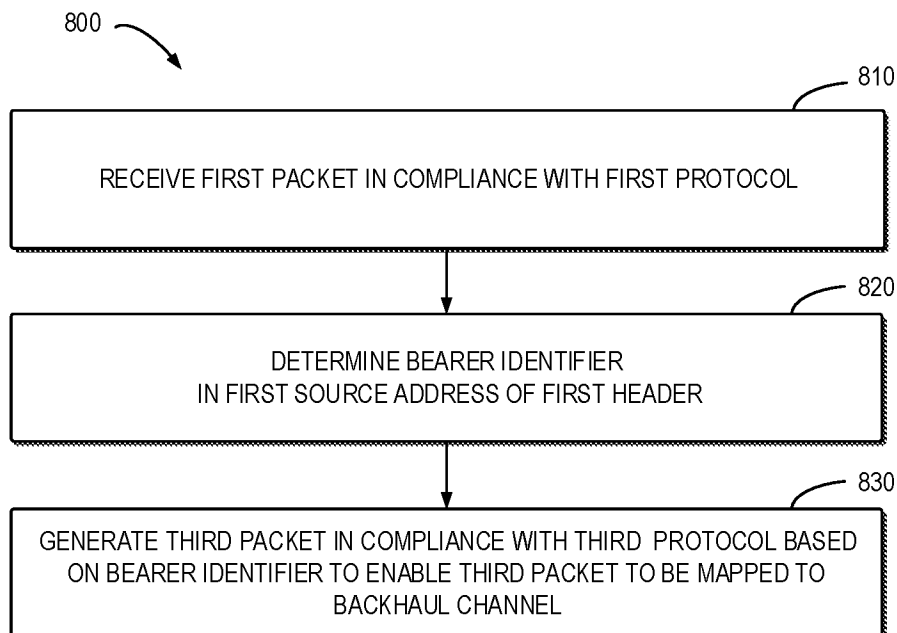
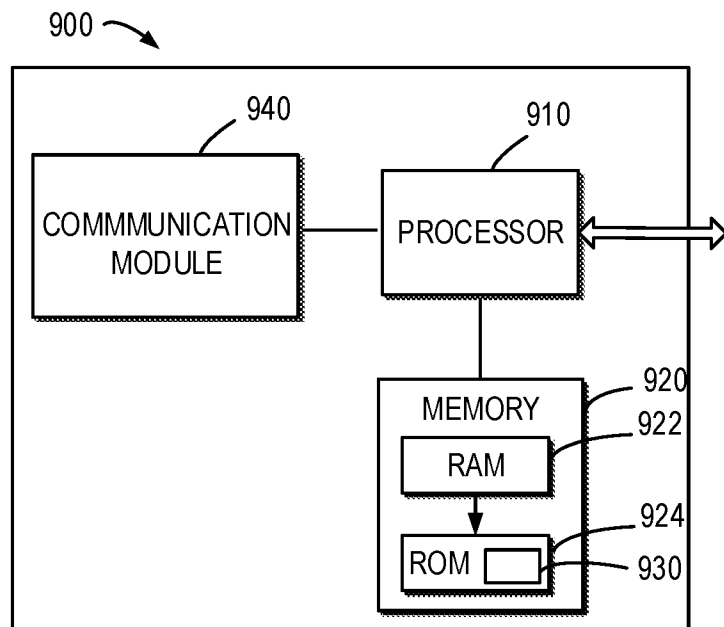
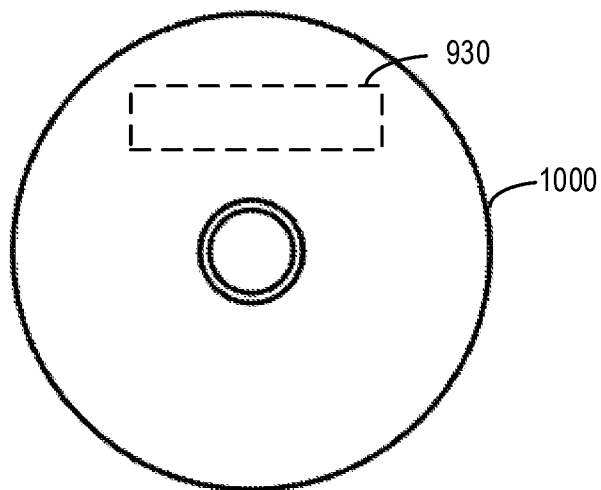


FIG. 6

**FIG. 7****FIG. 8**

**FIG. 9****FIG. 10**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/086718

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

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

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

CNPAT,CNKI,WPI,EPODOC,3GPP,IEEE, GOOGLE:bearer, flow, id, identification, identifier, IPV6, source, address, header, IAB, map, tunnel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016078570 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 26 May 2016 (2016-05-26) description, paragraphs [0031]-[0034], Figures 2, 3	1, 2, 9-11, 20, 21, 28-30, 39, 42
A	WO 2016078570 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 26 May 2016 (2016-05-26) description, paragraphs [0031]-[0034], Figures 2, 3	3-8, 12-19, 22-27, 31-38, 40-41, 43-44
A	WO 2014068524 A2 (RENESAS MOBILE CORPORATION) 08 May 2014 (2014-05-08) the whole document	1-44
A	CN 109218158 A (CHINA TELECOM CORP. LTD.) 15 January 2019 (2019-01-15) the whole document	1-44
A	CN 108306843 A (CHINA TELECOM CORP. LTD.) 20 July 2018 (2018-07-20) the whole document	1-44
A	FUJITSU. "Architecture and protocol details for LWA" 3GPP TSG-RAN WG2 Meeting #91 R2-153104, 28 August 2015 (2015-08-28), the whole document	1-44



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

14 January 2020

Date of mailing of the international search report

03 February 2020

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

YAO, Yaqian

Telephone No. 86-(10)-53961604

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/086718

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2016078570	A1	26 May 2016	KR	20170084201	A	19 July 2017
				CN	107079015	A	18 August 2017
				EP	3210432	A1	30 August 2017
				EP	3210365	A1	30 August 2017
				CN	107006045	A	01 August 2017
				US	2016142321	A1	19 May 2016
				JP	2017536765	A	07 December 2017
				WO	2016078589	A1	26 May 2016
				US	2016142308	A1	19 May 2016
WO	2014068524	A2	08 May 2014	WO	2014068524	A3	30 October 2014
				GB	2507546	A	07 May 2014
				US	2015319595	A1	05 November 2015
CN	109218158	A	15 January 2019	None			
CN	108306843	A	20 July 2018	None			