United States Patent Application Publication 20250267023
Kind Code A1
Publication Date August 21, 2025
Inventor(s) Talebi Fard; Peyman et al.

Deterministic Networks

Abstract

A PCF receives, from a SMF of a deterministic network (DetNet) node, a request message comprising one or more parameters, the one or more parameters comprising interface information indicating a status associated with an interface of the DetNet node. The PCF sends, to the SMF and in response to receiving the request message, policy information for a PDU session associated with the DetNet node.

Inventors: **Talebi Fard; Peyman (Vienna, VA), Park; Kyungmin (Vienna, VA), Dinan; Esmael Hejazi (McLean, VA), Chun; SungDuck (Fairfax, VA), Xu; Jian (McLean, VA), Qiao; Weihua (Herndon, VA), Filin; Stanislav (Chantilly, VA)**

Applicant: **Ofinno, LLC** (Reston, VA)

Family ID: **1000008602140**

Assignee: **Ofinno, LLC (Reston, VA)**

Appl. No.: **18/925824**

Filed: **October 24, 2024**

Related U.S. Application Data

parent US continuation PCT/US2023/020169 20230427 PENDING child US 18925824
us-provisional-application US 63335530 20220427
us-provisional-application US 63335531 20220427

Publication Classification

Int. Cl.: **H04L12/14** (20240101); **H04M15/00** (20240101); **H04W4/24** (20240101)

U.S. Cl.:

CPC **H04L12/1407** (20130101); **H04M15/66** (20130101); **H04W4/24** (20130101);

Background/Summary

CROSS-REFERENCE TO RELATED APPLICATIONS [0001] This application is a continuation of International Application No. PCT/US2023/020169, filed Apr. 27, 2023, which claims the benefit of U.S. Provisional Applications: No. 63/335,530 and No. 63/335,531, both filed Apr. 27, 2022, all of which are hereby incorporated by reference in their entireties.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Examples of several of the various embodiments of the present disclosure are described herein with reference to the drawings.

[0003] FIG. **1**A and FIG. **1**B illustrate example communication networks including an access network and a core network.

[0004] FIG. **2**A, FIG. **2**B, FIG. **2**C, and FIG. **2**D illustrate various examples of a framework for a service-based architecture within a core network.

[0005] FIG. **3** illustrates an example communication network including core network functions.

[0006] FIG. **4**A and FIG. **4**B illustrate example of core network architecture with multiple user plane functions and untrusted access.

[0007] FIG. **5** illustrates an example of a core network architecture for a roaming scenario.

[0008] FIG. **6** illustrates an example of network slicing.

[0009] FIG. **7**A, FIG. **7**B, and FIG. **7**C illustrate a user plane protocol stack, a control plane protocol stack, and services provided between protocol layers of the user plane protocol stack.

[0010] FIG. **8** illustrates an example of a quality of service model for data exchange.

[0011] FIG. **9**A, FIG. **9**B, FIG. **9**C, and FIG. **9**D illustrate example states and state transitions of a wireless device.

[0012] FIG. **10** illustrates an example of a registration procedure for a wireless device.

[0013] FIG. **11** illustrates an example of a service request procedure for a wireless device.

[0014] FIG. **12** illustrates an example of a protocol data unit session establishment procedure for a wireless device.

[0015] FIG. **13** illustrates examples of components of the elements in a communications network.

[0016] FIG. **14**A, FIG. **14**B, FIG. **14**C, and FIG. **14**D illustrate various examples of physical core network deployments, each having one or more network functions or portions thereof.

[0017] FIG. **15** illustrates an example embodiment of a present disclosure.

[0018] FIG. **16** illustrates an example embodiment of a present disclosure.

[0019] FIG. **17** illustrates an example embodiment of a present disclosure.

[0020] FIG. **18** illustrates an example embodiment of a present disclosure.

[0021] FIG. **19** illustrates an example embodiment of a present disclosure.

[0022] FIG. **20** illustrates an example embodiment of a present disclosure.

[0023] FIG. **21** illustrates an example embodiment of a present disclosure.

[0024] FIG. **22** illustrates an example embodiment of a present disclosure.

[0025] FIG. **23** illustrates an example embodiment of a present disclosure.

[0026] FIG. **24** illustrates an example embodiment of a present disclosure.

[0027] FIG. **25** illustrates an example embodiment of a present disclosure.

[0028] FIG. **26** illustrates an example embodiment of a present disclosure.

[0029] FIG. **27** illustrates an example embodiment of a present disclosure.

[0030] FIG. **28** illustrates an example embodiment of a present disclosure.

Description

DETAILED DESCRIPTION

[0031] In the present disclosure, various embodiments are presented as examples of how the disclosed techniques may be implemented and/or how the disclosed techniques may be practiced in environments and scenarios. It will be apparent to persons skilled in the relevant art that various changes in form and detail can be made therein without departing from the scope. In fact, after reading the description, it will be apparent to one skilled in the relevant art how to implement alternative embodiments. The present embodiments should not be limited by any of the described exemplary embodiments. The embodiments of the present disclosure will be described with reference to the accompanying drawings. Limitations, features, and/or elements from the disclosed example embodiments may be combined to create further embodiments within the scope of the disclosure. Any figures which highlight the functionality and advantages, are presented for example purposes only. The disclosed architecture is sufficiently flexible and configurable, such that it may be utilized in ways other than that shown. For example, the actions listed in any flowchart may be re-ordered or only optionally used in some embodiments.

[0032] Embodiments may be configured to operate as needed. The disclosed mechanism may be performed when certain criteria are met, for example, in a wireless device, a base station, a radio environment, a network, a combination of the above, and/or the like. Example criteria may be based, at least in part, on for example, wireless device or network node configurations, traffic load, initial system set up, packet sizes, traffic characteristics, a combination of the above, and/or the like. When the one or more criteria are met, various example embodiments may be applied. Therefore, it may be possible to implement example embodiments that selectively implement disclosed protocols.

[0033] A base station may communicate with a mix of wireless devices. Wireless devices and/or base stations may support multiple technologies, and/or multiple releases of the same technology. Wireless devices may have one or more specific capabilities. When this disclosure refers to a base station communicating with a plurality of wireless devices, this disclosure may refer to a subset of the total wireless devices in a coverage area. This disclosure may refer to, for example, a plurality of wireless devices of a given LTE or 5G release with a given capability and in a given sector of the base station. The plurality of wireless devices in this disclosure may refer to a selected plurality of wireless devices, and/or a subset of total wireless devices in a coverage area which perform according to disclosed methods, and/or the like. There may be a plurality of base stations or a plurality of wireless devices in a coverage area that may not comply with the disclosed methods, for example, those wireless devices or base stations may perform based on older releases of LTE or 5G technology.

[0034] In this disclosure, “a” and “an” and similar phrases refer to a single instance of a particular element, but should not be interpreted to exclude other instances of that element. For example, a bicycle with two wheels may be described as having “a wheel”. Any term that ends with the suffix “(s)” is to be interpreted as “at least one” and/or “one or more.” In this disclosure, the term “may” is to be interpreted as “may, for example.” In other words, the term “may” is indicative that the phrase following the term “may” is an example of one of a multitude of suitable possibilities that may, or may not, be employed by one or more of the various embodiments. The terms “comprises” and “consists of”, as used herein, enumerate one or more components of the element being described. The term “comprises” is interchangeable with “includes” and does not exclude unenumerated components from being included in the element being described. By contrast, “consists of” provides a complete enumeration of the one or more components of the element being described.

[0035] The phrases “based on”, “in response to”, “depending on”, “employing”, “using”, and similar phrases indicate the presence and/or influence of a particular factor and/or condition on an event and/or action, but do not exclude unenumerated factors and/or conditions from also being present and/or influencing the event and/or action. For example, if action X is performed “based on” condition Y, this is to be interpreted as the action being performed “based at least on” condition Y. For example, if the performance of action X is performed when conditions Y and Z are both satisfied, then the performing of action X may be described as being “based on Y”.

[0036] The term “configured” may relate to the capacity of a device whether the device is in an operational or non-operational state. Configured may refer to specific settings in a device that effect the operational characteristics of the device whether the device is in an operational or non-operational state. In other words, the hardware, software, firmware, registers, memory values, and/or the like may be “configured” within a device, whether the device is in an operational or nonoperational state, to provide the device with specific characteristics. Terms such as “a control message to cause in a device” may mean that a control message has parameters that may be used to configure specific characteristics or may be used to implement certain actions in the device, whether the device is in an operational or non-operational state.

[0037] In this disclosure, a parameter may comprise one or more information objects, and an information object m ay comprise one or more other objects. For example, if parameter J comprises parameter K, and parameter K comprises parameter L, and parameter L comprises parameter M, then J comprises L, and J comprises M. A parameter may be referred to as a field or information element. In an example embodiment, when one or more messages comprise a plurality of parameters, it implies that a parameter in the plurality of parameters is in at least one of the one or more messages, but does not have to be in each of the one or more messages.

[0038] This disclosure may refer to possible combinations of enumerated elements. For the sake of brevity and legibility, the present disclosure does not explicitly recite each and every permutation that may be obtained by choosing from a set of optional features. The present disclosure is to be interpreted as explicitly disclosing all such permutations. For example, the seven possible combinations of enumerated elements A, B, C consist of: (1) “A”; (2) “B”; (3) “C”; (4) “A and B”; (5) “A and C”; (6) “B and C”; and (7) “A, B, and C”. For the sake of brevity and legibility, these seven possible combinations may be described using any of the following interchangeable formulations: “at least one of A, B, and C”; “at least one of A, B, or C”; “one or more of A, B, and C”; “one or more of A, B, or C”; “A, B, and/or C”. It will be understood that impossible combinations are excluded. For example, “X and/or not-X” should be interpreted as “X or not-X”. It will be further understood that these formulations may describe alternative phrasings of overlapping and/or synonymous concepts, for example, “identifier, identification, and/or ID number”.

[0039] This disclosure may refer to sets and/or subsets. As an example, set X may be a set of elements comprising one or more elements. If every element of X is also an element of Y, then X may be referred to as a subset of Y. In this disclosure, only non-empty sets and subsets are considered. For example, if Y consists of the elements Y1, Y2, and Y3, then the possible subsets of Y are {Y1, Y2, Y3}, {Y1, Y2}, {Y1, Y3}, {Y2, Y3}, {Y1}, {Y2}, and {Y3}.

[0040] FIG. **1**A illustrates an example of a communication network **100** in which embodiments of the present disclosure may be implemented. The communication network **100** may comprise, for example, a public land mobile network (PLMN) run by a network operator. As illustrated in FIG. **1**A, the communication network **100** includes a wireless device **101**, an access network (AN) **102**, a core network (CN) **105**, and one or more data network (DNs) **108**.

[0041] The wireless device **101** may communicate with DNs **108** via AN **102** and CN **105**. In the present disclosure, the term wireless device may refer to and encompass any mobile device or fixed (non-mobile) device for which wireless communication is needed or usable. For example, a wireless device may be a telephone, smart phone, tablet, computer, laptop, sensor, meter, wearable device, Internet of Things (IoT) device, vehicle road side unit (RSU), relay node, automobile, unmanned aerial vehicle, urban air mobility, and/or any combination thereof. The term wireless device encompasses other terminology, including user equipment (UE), user terminal (UT), access terminal (AT), mobile station, handset, wireless transmit and receive unit (WTRU), and/or wireless communication device.

[0042] The AN **102** may connect wireless device **101** to CN **105** in any suitable manner. The communication direction from the AN **102** to the wireless device **101** is known as the downlink and the communication direction from the wireless device **101** to AN **102** is known as the uplink. Downlink transmissions may be separated from uplink transmissions using frequency division duplexing (FDD), time-division duplexing (TDD), and/or some combination of the two duplexing techniques. The AN **102** may connect to wireless device **101** through radio communications over an air interface. An access network that at least partially operates over the air interface may be referred to as a radio access network (RAN). The CN **105** may set up one or more end-to-end connection between wireless device **101** and the one or more DNs **108**. The CN **105** may authenticate wireless device **101** and provide charging functionality.

[0043] In the present disclosure, the term base station may refer to and encompass any element of AN **102** that facilitates communication between wireless device **101** and AN **102**. Access networks and base stations have many different names and implementations. The base station may be a terrestrial base station fixed to the earth. The base station may be a mobile base station with a moving coverage area. The base station may be in space, for example, on board a satellite. For example, WiFi and other standards may use the term access point. As another example, the Third-Generation Partnership Project (3GPP) has produced specifications for three generations of mobile networks, each of which uses different terminology. Third Generation (3G) and/or Universal Mobile Telecommunications System (UMTS) standards may use the term Node B. 4G, Long Term Evolution (LTE), and/or Evolved Universal Terrestrial Radio Access (E-UTRA) standards may use the term Evolved Node B (eNB). 5G and/or New Radio (NR) standards may describe AN **102** as a next-generation radio access network (NG-RAN) and may refer to base stations as Next Generation eNB (ng-eNB) and/or Generation Node B (gNB). Future standards (for example, 6G, 7G, 8G) may use new terminology to refer to the elements which implement the methods described in the present disclosure (e.g., wireless devices, base stations, ANs, CNs, and/or components thereof). A base station may be implemented as a repeater or relay node used to extend the coverage area of a donor node. A repeater node may amplify and rebroadcast a radio signal received from a donor node. A relay node may perform the same/similar functions as a repeater node but may decode the radio signal received from the donor node to remove noise before amplifying and rebroadcasting the radio signal.

[0044] The AN **102** may include one or more base stations, each having one or more coverage areas. The geographical size and/or extent of a coverage area may be defined in terms of a range at which a receiver of AN **102** can successfully receive transmissions from a transmitter (e.g., wireless device **101**) operating within the coverage area (and/or vice-versa). The coverage areas may be referred to as sectors or cells (although in some contexts, the term cell refers to the carrier frequency used in a particular coverage area, rather than the coverage area itself). Base stations with large coverage areas may be referred to as macrocell base stations. Other base stations cover smaller areas, for example, to provide coverage in areas with weak macrocell coverage, or to provide additional coverage in areas with high traffic (sometimes referred to as hotspots). Examples of small cell base stations include, in order of decreasing coverage area, microcell base stations, picocell base stations, and femtocell base stations or home base stations. Together, the coverage areas of the base stations may provide radio coverage to wireless device **101** over a wide geographic area to support wireless device mobility.

[0045] A base station may include one or more sets of antennas for communicating with the wireless device **101** over the air interface. Each set of antennas may be separately controlled by the base station. Each set of antennas may have a corresponding coverage area. As an example, a base station may include three sets of antennas to respectively control three coverage areas on three different sides of the base station. The entirety of the base station (and its corresponding antennas) may be deployed at a single location. Alternatively, a controller at a central location may control one or more sets of antennas at one or more distributed locations. The controller may be, for example, a baseband processing unit that is part of a centralized or cloud RAN architecture. The baseband processing unit may be either centralized in a pool of baseband processing units or virtualized. A set of antennas at a distributed location may be referred to as a remote radio head (RRH).

[0046] FIG. **1**B illustrates another example communication network **150** in which embodiments of the present disclosure may be implemented. The communication network **150** may comprise, for example, a PLMN run by a network operator. As illustrated in FIG. **1**B, communication network **150** includes UEs **151**, a next generation radio access network (NG-RAN) **152**, a 5G core network (5G-CN) **155**, and one or more DNs **158**. The NG-RAN **152** includes one or more base stations, illustrated as generation node Bs (gNBs) **152**A and next generation evolved Node Bs (ng eNBs) **152**B. The 5G-CN **155** includes one or more network functions (NFs), including control plane functions **155**A and user plane functions **155**B. The one or more DNs **158** may comprise public DNs (e.g., the Internet), private DNs, and/or intra-operator DNs. Relative to corresponding components illustrated in FIG. **1**A, these components may represent specific implementations and/or terminology.

[0047] The base stations of the NG-RAN **152** may be connected to the UEs **151** via Uu interfaces. The base stations of the NG-RAN **152** may be connected to each other via Xn interfaces. The base stations of the NG-RAN **152** may be connected to 5G CN **155** via NG interfaces. The Uu interface may include an air interface. The NG and Xn interfaces may include an air interface, or may consist of direct physical connections and/or indirect connections over an underlying transport network (e.g., an internet protocol (IP) transport network).

[0048] Each of the Uu, Xn, and NG interfaces may be associated with a protocol stack. The protocol stacks may include a user plane (UP) and a control plane (CP). Generally, user plane data may include data pertaining to users of the UEs **151**, for example, internet content downloaded via a web browser application, sensor data uploaded via a tracking application, or email data communicated to or from an email server. Control plane data, by contrast, may comprise signaling and messages that facilitate packaging and routing of user plane data so that it can be exchanged with the DN(s). The NG interface, for example, may be divided into an NG user plane interface (NG-U) and an NG control plane interface (NG-C). The NG-U interface may provide delivery of user plane data between the base stations and the one or more user plane network functions **155**B. The NG-C interface may be used for control signaling between the base stations and the one or more control plane network functions **155**A. The NG-C interface may provide, for example, NG interface management, UE context management, UE mobility management, transport of NAS messages, paging, PDU session management, and configuration transfer and/or warning message transmission. In some cases, the NGC interface may support transmission of user data (for example, a small data transmission for an IoT device).

[0049] One or more of the base stations of the NG-RAN **152** may be split into a central unit (CU) and one or more distributed units (DUs). A CU may be coupled to one or more DUs via an F1 interface. The CU may handle one or more upper layers in the protocol stack and the DU may handle one or more lower layers in the protocol stack. For example, the CU may handle RRC, PDCP, and SDAP, and the DU may handle RLC, MAC, and PHY. The one or more DUs may be in geographically diverse locations relative to the CU and/or each other. Accordingly, the CU/DU split architecture may permit increased coverage and/or better coordination.

[0050] The gNBs **152**A and ng-eNBs **152**B may provide different user plane and control plane protocol termination towards the UEs **151**. For example, the gNB **154**A may provide new radio (NR) protocol terminations over a Uu interface associated with a first protocol stack. The ng-eNBs

152B may provide Evolved UMTS Terrestrial Radio Access (E-UTRA) protocol terminations over a Uu interface associated with a second protocol stack.

[0051] The 5G-CN **155** may authenticate UEs **151**, set up end-to-end connections between UEs **151** and the one or more DNs **158**, and provide charging functionality. The 5G-CN **155** may be based on a service-based architecture, in which the NFs making up the 5G-CN **155** offer services to each other and to other elements of the communication network **150** via interfaces. The 5G-CN **155** may include any number of other NFs and any number of instances of each NF.

[0052] FIG. **2**A, FIG. **2**B, FIG. **2**C, and FIG. **2**D illustrate various examples of a framework for a service-based architecture within a core network. In a service-based architecture, a service may be sought by a service consumer and provided by a service producer. Prior to obtaining a particular service, an NF may determine where such as service can be obtained. To discover a service, the NF may communicate with a network repository function (NRF). As an example, an NF that provides one or more services may register with a network repository function (NRF). The NRF may store data relating to the one or more services that the NF is prepared to provide to other NFs in the service-based architecture. A consumer NF may query the NRF to discover a producer NF (for example, by obtaining from the NRF a list of NF instances that provide a particular service).

[0053] In the example of FIG. **2**A, an NF **211** (a consumer NF in this example) may send a request **221** to an NF **212** (a producer NF). The request **221** may be a request for a particular service and may be sent based on a discovery that NF **212** is a producer of that service. The request **221** may comprise data relating to NF **211** and/or the requested service. The NF **212** may receive request **221**, perform one or more actions associated with the requested service (e.g., retrieving data), and provide a response **221**. The one or more actions performed by the NF **212** may be based on request data included in the request **221**, data stored by NF **212**, and/or data retrieved by NF **212**. The response **222** may notify NF **211** that the one or more actions have been completed. The response **222** may comprise response data relating to NF **212**, the one or more actions, and/or the requested service.

[0054] In the example of FIG. **2**B, an NF **231** sends a request **241** to an NF **232**. In this example, part of the service produced by NF **232** is to send a request **242** to an NF **233**. The NF **233** may perform one or more actions and provide a response **243** to NF **232**. Based on response **243**, NF **232** may send a response **244** to NF **231**. It will be understood from FIG. **2**B that a single NF may perform the role of producer of services, consumer of services, or both. A particular NF service may include any number of nested NF services produced by one or more other NFs.

[0055] FIG. **2**C illustrates examples of subscribe-notify interactions between a consumer NF and a producer NF. In FIG. **2**C, an NF **251** sends a subscription **261** to an NF **252**. An NF **253** sends a subscription **262** to the NF **252**. Two NFs are shown in FIG. **2**C for illustrative purposes (to demonstrate that the NF **252** may provide multiple subscription services to different NFs), but it will be understood that a subscribe-notify interaction only requires one subscriber. The NFs **251**, **253** may be independent from one another. For example, the NFs **251**, **253** may independently discover NF **252** and/or independently determine to subscribe to the service offered by NF **252**. In response to receipt of a subscription, the NF **252** may provide a notification to the subscribing NF. For example, NF **252** may send a notification **263** to NF **251** based on subscription **261** and may send a notification **264** to NF **253** based on subscription **262**.

[0056] As shown in the example illustration of FIG. **2**C, the sending of the notifications **263**, **264** may be based on a determination that a condition has occurred. For example, the notifications **263**, **264** may be based on a determination that a particular event has occurred, a determination that a particular condition is outstanding, and/or a determination that a duration of time associated with the subscription has elapsed (for example, a period associated with a subscription for periodic notifications). As shown in the example illustration of FIG. **2**C, NF **252** may send notifications **263**, **264** to NFs **251**, **253** simultaneously and/or in response to the same condition. However, it will be understood that the NF **252** may provide notifications at different times and/or in response to different notification conditions. In an example, the NF **251** may request a notification when a certain parameter, as measured by the NF **252**, exceeds a first threshold, and the NF **252** may request a notification when the parameter exceeds a second threshold different from the first threshold. In an example, a parameter of interest and/or a corresponding threshold may be indicated in the subscriptions **261**, **262**.

[0057] FIG. **2**D illustrates another example of a subscribe-notify interaction. In FIG. **2**D, an NF **271** sends a subscription **281** to an NF **272**. In response to receipt of subscription **281** and/or a determination that a notification condition has occurred, NF **272** may send a notification **284**. The notification **284** may be sent to an NF **273**. Unlike the example in FIG. **2**C (in which a notification is sent to the subscribing NF), FIG. **2**D demonstrates that a subscription and its corresponding notification may be associated with different NFs. For example, NF **271** may subscribe to the service provided by NF **272** on behalf of NF **273**.

[0058] FIG. **3** illustrates another example communication network **300** in which embodiments of the present disclosure may be implemented. Communication network **300** includes a user equipment (UE) **301**, an access network (AN) **302**, and a data network (DN) **308**. The remaining elements depicted in FIG. **3** may be included in and/or associated with a core network. Each element of the core network may be referred to as a network function (NF).

[0059] The NFs depicted in FIG. **3** include a user plane function (UPF) **305**, an access and mobility management function (AMF) **312**, a session management function (SMF) **314**, a policy control function (PCF) **320**, a network repository function (NRF) **330**, a network exposure function (NEF) **340**, a unified data management (UDM) **350**, an authentication server function (AUSF) **360**, a network slice selection function (NSSF) **370**, a charging function (CHF) **380**, a network data analytics function (NWDAF) **390**, and an application function (AF) **399**. The UPF **305** may be a user-plane core network function, whereas the NFs **312**, **314**, and **320-390** may be control-plane core network functions. Although not shown in the example of FIG. **3**, the core network may include additional instances of any of the NFs depicted and/or one or more different NF types that provide different services. Other examples of NF type include a gateway mobile location center (GMLC), a location management function (LMF), an operations, administration, and maintenance function (OAM), a public warning system (PWS), a short message service function (SMSF), a unified data repository (UDR), and an unstructured data storage function (UDSF).

[0060] Each element depicted in FIG. **3** has an interface with at least one other element. The interface may be a logical connection rather than, for example, a direct physical connection. Any interface may be identified using a reference point representation and/or a service-based representation. In a reference point representation, the letter ‘N’ is followed by a numeral, indicating an interface between two specific elements. For example, as shown in FIG. **3**, AN **302** and UPF **305** interface via ‘N3’, whereas UPF **305** and DN **308** interface via ‘N6’. By contrast, in a service-based representation, the letter ‘N’ is followed by letters. The letters identify an NF that provides services to the core network. For example, PCF **320** may provide services via interface ‘Npcf’. The PCF **320** may provide services to any NF in the core network via ‘Npcf’. Accordingly, a service-based representation may correspond to a bundle of reference point representations. For example, the Npcf interface between PCF **320** and the core network generally may correspond to an N7 interface between PCF **320** and SMF **314**, an N30 interface between PCF **320** and NEF **340**, etc.

[0061] The UPF **305** may serve as a gateway for user plane traffic between AN **302** and DN **308**. The UE **301** may connect to UPF **305** via a Uu interface and an N3 interface (also described as NGU interface). The UPF **305** may connect to DN **308** via an N6 interface. The UPF **305** may connect to one or more other UPFs (not shown) via an N9 interface. The UE **301** may be configured to receive services through a protocol data unit (PDU) session, which is a logical connection between UE **301** and DN **308**. The UPF **305** (or a plurality of UPFs if desired) may be selected by SMF **314** to handle a particular PDU session between UE **301** and DN **308**. The SMF

314 may control the functions of UPF **305** with respect to the PDU session. The SMF **314** may connect to UPF **305** via an N4 interface. The UPF **305** may handle any number of PDU sessions associated with any number of UEs (via any number of ANs). For purposes of handling the one or more PDU sessions, UPF **305** may be controlled by any number of SMFs via any number of corresponding N4 interfaces.

[0062] The AMF **312** depicted in FIG. **3** may control UE access to the core network. The UE **301** may register with the network via AMF **312**. It may be necessary for UE **301** to register prior to establishing a PDU session. The AMF **312** may manage a registration area of UE **301**, enabling the network to track the physical location of UE **301** within the network. For a UE in connected mode, AMF **312** may manage UE mobility, for example, handovers from one AN or portion thereof to another. For a UE in idle mode, AMF **312** may perform registration updates and/or page the UE to transition the UE to connected mode.

[0063] The AMF **312** may receive, from UE **301**, non-access stratum (NAS) messages transmitted in accordance with NAS protocol. NAS messages relate to communications between UE **301** and the core network. Although NAS messages may be relayed to AMF **312** via AN **302**, they may be described as communications via the N1 interface. NAS messages may facilitate UE registration and mobility management, for example, by authenticating, identifying, configuring, and/or managing a connection of UE **301**. NAS messages may support session management procedures for maintaining user plane connectivity and quality of service (QoS) of a session between UE **301** and DN **309**. If the NAS message involves session management, AMF **312** may send the NAS message to SMF **314**. NAS messages may be used to transport messages between UE **301** and other components of the core network (e.g., core network components other than AMF **312** and SMF **314**). The AMF **312** may act on a particular NAS message itself, or alternatively, forward the NAS message to an appropriate core network function (e.g., SMF **314**, etc.)

[0064] The SMF **314** depicted in FIG. **3** may establish, modify, and/or release a PDU session based on messaging received UE **301**. The SMF **314** may allocate, manage, and/or assign an IP address to UE **301**, for example, upon establishment of a PDU session. There may be multiple SMFs in the network, each of which may be associated with a respective group of wireless devices, base stations, and/or UPFs. A UE with multiple PDU sessions may be associated with a different SMF for each PDU session. As noted above, SMF **314** may select one or more UPFs to handle a PDU session and may control the handling of the PDU session by the selected UPF by providing rules for packet handling (PDR, FAR, QER, etc.). Rules relating to QoS and/or charging for a particular PDU session may be obtained from PCF **320** and provided to UPF **305**.

[0065] The PCF **320** may provide, to other NFs, services relating to policy rules. The PCF **320** may use subscription data and information about network conditions to determine policy rules and then provide the policy rules to a particular NF which may be responsible for enforcement of those rules. Policy rules may relate to policy control for access and mobility, and may be enforced by the AMF. Policy rules may relate to session management, and may be enforced by the SMF **314**. Policy rules may be, for example, network-specific, wireless device-specific, session-specific, or data flow-specific.

[0066] The NRF **330** may provide service discovery. The NRF **330** may belong to a particular PLMN. The NRF **330** may maintain NF profiles relating to other NFs in the communication network **300**. The NF profile may include, for example, an address, PLMN, and/or type of the NF, a slice identifier, a list of the one or more services provided by the NF, and the authorization required to access the services.

[0067] The NEF **340** depicted in FIG. **3** may provide an interface to external domains, permitting external domains to selectively access the control plane of the communication network **300**. The external domain may comprise, for example, third-party network functions, application functions, etc. The NEF **340** may act as a proxy between external elements and network functions such as AMF **312**, SMF **314**, PCF **320**, UDM **350**, etc. As an example, NEF **340** may determine a location or reachability status of UE **301** based on reports from AMF **312**, and provide status information to an external element. As an example, an external element may provide, via NEF **340**, information that facilitates the setting of parameters for establishment of a PDU session. The NEF **340** may determine which data and capabilities of the control plane are exposed to the external domain. The NEF **340** may provide secure exposure that authenticates and/or authorizes an external entity to which data or capabilities of the communication network **300** are exposed. The NEF **340** may selectively control the exposure such that the internal architecture of the core network is hidden from the external domain.

[0068] The UDM **350** may provide data storage for other NFs. The UDM **350** may permit a consolidated view of network information that may be used to ensure that the most relevant information can be made available to different NFs from a single resource. The UDM **350** may store and/or retrieve information from a unified data repository (UDR). For example, UDM **350** may obtain user subscription data relating to UE **301** from the UDR.

[0069] The AUSF **360** may support mutual authentication of UE **301** by the core network and authentication of the core network by UE **301**. The AUSF **360** may perform key agreement procedures and provide keying material that can be used to improve security.

[0070] The NSSF **370** may select one or more network slices to be used by the UE **301**. The NSSF **370** may select a slice based on slice selection information. For example, the NSSF **370** may receive Single Network Slice Selection Assistance Information (S-NSSAI) and map the S-NSSAI to a network slice instance identifier (NSI).

[0071] The CHF **380** may control billing-related tasks associated with UE **301**. For example, UPF **305** may report traffic usage associated with UE **301** to SMF **314**. The SMF **314** may collect usage data from UPF **305** and one or more other UPFs. The usage data may indicate how much data is exchanged, what DN the data is exchanged with, a network slice associated with the data, or any other information that may influence billing. The SMF **314** may share the collected usage data with the CHF. The CHF may use the collected usage data to perform billing-related tasks associated with UE **301**. The CHF may, depending on the billing status of UE **301**, instruct SMF **314** to limit or influence access of UE **301** and/or to provide billing-related notifications to UE **301**.

[0072] The NWDAF **390** may collect and analyze data from other network functions and offer data analysis services to other network functions. As an example, NWDAF **390** may collect data relating to a load level for a particular network slice instance from UPF **305**, AMF **312**, and/or SMF **314**. Based on the collected data, NWDAF **390** may provide load level data to the PCF **320** and/or NSSF **370**, and/or notify the PC **220** and/or NSSF **370** if load level for a slice reaches and/or exceeds a load level threshold.

[0073] The AF **399** may be outside the core network, but may interact with the core network to provide information relating to the QoS requirements or traffic routing preferences associated with a particular application. The AF **399** may access the core network based on the exposure constraints imposed by the NEF **340**. However, an operator of the core network may consider the AF **399** to be a trusted domain that can access the network directly.

[0074] FIGS. **4**A, **4**B, and **5** illustrate other examples of core network architectures that are analogous in some respects to the core network architecture **300** depicted in FIG. **3**. For conciseness, some of the core network elements depicted in FIG. **3** are omitted. Many of the elements depicted in FIGS. **4**A, **4**B, and **5** are analogous in some respects to elements depicted in FIG. **3**. For conciseness, some of the details relating to their functions or operation are omitted.

[0075] FIG. **4**A illustrates an example of a core network architecture **400**A comprising an arrangement of multiple UPFs. Core network architecture **400**A includes a UE **401**, an AN **402**, an AMF **412**, and an SMF **414**. Unlike previous examples of core network architectures described above, FIG. **4**A depicts multiple UPFs, including a UPF **405**, a UPF **406**, and a UPF **407**, and multiple DNs, including a DN **408** and a DN **409**. Each of the multiple UPFs **405**, **406**, **407** may communicate with the SMF **414** via an N4 interface. The DNs **408**, **409** communicate with the

UPFs **405**, **406**, respectively, via N6 interfaces. As shown in FIG. **4**A, the multiple UPFs **405**, **406**, **407** may communicate with one another via N9 interfaces.

[0076] The UPFs **405**, **406**, **407** may perform traffic detection, in which the UPFs identify and/or classify packets. Packet identification may be performed based on packet detection rules (PDR) provided by the SMF **414**. A PDR may include packet detection information comprising one or more of: a source interface, a UE IP address, core network (CN) tunnel information (e.g., a CN address of an N3/N9 tunnel corresponding to a PDU session), a network instance identifier, a quality of service flow identifier (QFI), a filter set (for example, an IP packet filter set or an ethernet packet filter set), and/or an application identifier.

[0077] In addition to indicating how a particular packet is to be detected, a PDR may further indicate rules for handling the packet upon detection thereof. The rules may include, for example, forwarding action rules (FARs), multi-access rules (MARs), usage reporting rules (URRs), QoS enforcement rules (QERs), etc. For example, the PDR may comprise one or more FAR identifiers, MAR identifiers, URR identifiers, and/or QER identifiers. These identifiers may indicate the rules that are prescribed for the handling of a particular detected packet.

[0078] The UPF **405** may perform traffic forwarding in accordance with a FAR. For example, the FAR may indicate that a packet associated with a particular PDR is to be forwarded, duplicated, dropped, and/or buffered. The FAR may indicate a destination interface, for example, “access” for downlink or “core” for uplink. If a packet is to be buffered, the FAR may indicate a buffering action rule (BAR). As an example, UPF **405** may perform data buffering of a certain number downlink packets if a PDU session is deactivated.

[0079] The UPF **405** may perform QoS enforcement in accordance with a QER. For example, the QER may indicate a guaranteed bitrate that is authorized and/or a maximum bitrate to be enforced for a packet associated with a particular PDR. The QER may indicate that a particular guaranteed and/or maximum bitrate may be for uplink packets and/or downlink packets. The UPF **405** may mark packets belonging to a particular QoS flow with a corresponding QFI. The marking may enable a recipient of the packet to determine a QoS of the packet.

[0080] The UPF **405** may provide usage reports to the SMF **414** in accordance with a URR. The URR may indicate one or more triggering conditions for generation and reporting of the usage report, for example, immediate reporting, periodic reporting, a threshold for incoming uplink traffic, or any other suitable triggering condition. The URR may indicate a method for measuring usage of network resources, for example, data volume, duration, and/or event.

[0081] As noted above, the DNs **408**, **409** may comprise public DNs (e.g., the Internet), private DNs (e.g., private, internal corporate-owned DNs), and/or intra-operator DNs. Each DN may provide an operator service and/or a third-party service. The service provided by a DN may be the Internet, an IP multimedia subsystem (IMS), an augmented or virtual reality network, an edge computing or mobile edge computing (MEC) network, etc. Each DN may be identified using a data network name (DNN). The UE **401** may be configured to establish a first logical connection with DN **408** (a first PDU session), a second logical connection with DN **409** (a second PDU session), or both simultaneously (first and second PDU sessions).

[0082] Each PDU session may be associated with at least one UPF configured to operate as a PDU session anchor (PSA, or “anchor”). The anchor may be a UPF that provides an N6 interface with a DN.

[0083] In the example of FIG. **4**A, UPF **405** may be the anchor for the first PDU session between UE **401** and DN **408**, whereas the UPF **406** may be the anchor for the second PDU session between UE **401** and DN **409**. The core network may use the anchor to provide service continuity of a particular PDU session (for example, IP address continuity) as UE **401** moves from one access network to another. For example, suppose that UE **401** establishes a PDU session using a data path to the DN **408** using an access network other than AN **402**. The data path may include UPF **405** acting as anchor. Suppose further that the UE **401** later moves into the coverage area of the AN

402. In such a scenario, SMF **414** may select a new UPF (UPF **407**) to bridge the gap between the newly-entered access network (AN **402**) and the anchor UPF (UPF **405**). The continuity of the PDU session may be preserved as any number of UPFs are added or removed from the data path. When a UPF is added to a data path, as shown in FIG. **4**A, it may be described as an intermediate UPF and/or a cascaded UPF.

[0084] As noted above, UPF **406** may be the anchor for the second PDU session between UE **401** and DN **409**. Although the anchor for the first and second PDU sessions are associated with different UPFs in FIG. **4**A, it will be understood that this is merely an example. It will also be understood that multiple PDU sessions with a single DN may correspond to any number of anchors. When there are multiple UPFs, a UPF at the branching point (UPF **407** in FIG. **4**) may operate as an uplink classifier (UL-CL). The UL-CL may divert uplink user plane traffic to different UPFs.

[0085] The SMF **414** may allocate, manage, and/or assign an IP address to UE **401**, for example, upon establishment of a PDU session. The SMF **414** may maintain an internal pool of IP addresses to be assigned. The SMF **414** may, if necessary, assign an IP address provided by a dynamic host configuration protocol (DHCP) server or an authentication, authorization, and accounting (AAA) server. IP address management may be performed in accordance with a session and service continuity (SSC) mode. In SSC mode 1, an IP address of UE **401** may be maintained (and the same anchor UPF may be used) as the wireless device moves within the network. In SSC mode 2, the IP address of UE **401** changes as UE **401** moves within the network (e.g., the old IP address and UPF may be abandoned and a new IP address and anchor UPF may be established). In SSC mode 3, it may be possible to maintain an old IP address (similar to SSC mode 1) temporarily while establishing a new IP address (similar to SSC mode 2), thus combining features of SSC modes 1 and 2. Applications that are sensitive to IP address changes may operate in accordance with SSC mode 1.

[0086] UPF selection may be controlled by SMF **414**. For example, upon establishment and/or modification of a PDU session between UE **401** and DN **408**, SMF **414** may select UPF **405** as the anchor for the PDU session and/or UPF **407** as an intermediate UPF. Criteria for UPF selection include path efficiency and/or speed between AN **402** and DN **408**. The reliability, load status, location, slice support and/or other capabilities of candidate UPFs may also be considered.

[0087] FIG. **4**B illustrates an example of a core network architecture **400**B that accommodates untrusted access. Similar to FIG. **4**A, UE **401** as depicted in FIG. **4**B connects to DN **408** via AN **402** and UPF **405**. The AN **402** and UPF **405** constitute trusted (e.g., 3GPP) access to the DN **408**. By contrast, UE **401** may also access DN **408** using an untrusted access network, AN **403**, and a non-3GPP interworking function (N3IWF) **404**.

[0088] The AN **403** may be, for example, a wireless land area network (WLAN) operating in accordance with the IEEE 802.11 standard. The UE **401** may connect to AN **403**, via an interface Y1, in whatever manner is prescribed for AN **403**. The connection to AN **403** may or may not involve authentication. The UE **401** may obtain an IP address from AN **403**. The UE **401** may determine to connect to core network **400**B and select untrusted access for that purpose. The AN **403** may communicate with N3IWF **404** via a Y2 interface. After selecting untrusted access, the UE **401** may provide N3IWF **404** with sufficient information to select an AMF. The selected AMF may be, for example, the same AMF that is used by UE **401** for 3GPP access (AMF **412** in the present example). The N3IWF **404** may communicate with AMF **412** via an N2 interface. The UPF **405** may be selected and N3IWF **404** may communicate with UPF **405** via an N3 interface. The UPF **405** may be a PDU session anchor (PSA) and may remain the anchor for the PDU session even as UE **401** shifts between trusted access and untrusted access.

[0089] FIG. **5** illustrates an example of a core network architecture **500** in which a UE **501** is in a roaming scenario. In a roaming scenario, UE **501** is a subscriber of a first PLMN (a home PLMN, or HPLMN) but attaches to a second PLMN (a visited PLMN, or VPLMN). Core network architecture **500** includes UE **501**, an AN **502**, a UPF **505**, and a D N **508**.

[0090] The AN **502** and UPF **505** may be associated with a VPLMN. The VPLMN may manage the AN **502** and UPF **505** using core network elements associated with the VPLMN, including an AMF **512**, an SMF **514**, a PCF **520**, an NRF **530**, an NEF **540**, and an NSSF **570**. An AF **599** may be adjacent the core network of the VPLMN.

[0091] The UE **501** may not be a subscriber of the VPLMN. The AMF **512** may authorize UE **501** to access the network based on, for example, roaming restrictions that apply to UE **501**. In order to obtain network services provided by the VPLMN, it may be necessary for the core network of the VPLMN to interact with core network elements of a HPLMN of UE **501**, in particular, a PCF **521**, an NRF **531**, an NEF **541**, a UDM **551**, and/or an AUSF **561**. The VPLMN and HPLMN may communicate using an N32 interface connecting respective security edge protection proxies (SEPPs). In FIG. **5**, the respective SEPPs are depicted as a VSEPP **590** and an HSEPP **591**.

[0092] The VSEPP **590** and the HSEPP **591** communicate via an N32 interface for defined purposes while concealing information about each PLMN from the other. The SEPPs may apply roaming policies based on communications via the N32 interface. The PCF **520** and PCF **521** may communicate via the SEPPs to exchange policy-related signaling. The NRF **530** and NRF **531** may communicate via the SEPPs to enable service discovery of NFs in the respective PLMNs. The VPLMN and HPLMN may independently maintain NEF **540** and NEF **541**. The NSSF **570** and NSSF **571** may communicate via the SEPPs to coordinate slice selection for UE **501**. The HPLMN may handle all authentication and subscription related signaling. For example, when the UE **501** registers or requests service via the VPLMN, the VPLMN may authenticate UE **501** and/or obtain subscription data of UE **501** by accessing, via the SEPPs, the UDM **551** and AUSF **561** of the HPLMN.

[0093] The core network architecture **500** depicted in FIG. **5** may be referred to as a local breakout configuration, in which UE **501** accesses DN **508** using one or more UPFs of the VPLMN (i.e., UPF **505**). However, other configurations are possible. For example, in a home-routed configuration (not shown in FIG. **5**), UE **501** may access a DN using one or more UPFs of the HPLMN. In the home-routed configuration, an N9 interface may run parallel to the N32 interface, crossing the frontier between the VPLMN and the HPLMN to carry user plane data. One or more SMFs of the respective PLMNs may communicate via the N32 interface to coordinate session management for UE **501**. The SMFs may control their respective UPFs on either side of the frontier.

[0094] FIG. **6** illustrates an example of network slicing. Network slicing may refer to division of shared infrastructure (e.g., physical infrastructure) into distinct logical networks. These distinct logical networks may be independently controlled, isolated from one another, and/or associated with dedicated resources.

[0095] Network architecture **600**A illustrates an un-sliced physical network corresponding to a single logical network. The network architecture **600**A comprises a user plane wherein UEs **601**A, **601**B, **601**C (collectively, UEs **601**) have a physical and logical connection to a DN **608** via an AN **602** and a UPF **605**. The network architecture **600**A comprises a control plane wherein an AMF **612** and a SMF **614** control various aspects of the user plane.

[0096] The network architecture **600**A may have a specific set of characteristics (e.g., relating to maximum bit rate, reliability, latency, bandwidth usage, power consumption, etc.). This set of characteristics may be affected by the nature of the network elements themselves (e.g., processing power, availability of free memory, proximity to other network elements, etc.) or the management thereof (e.g., optimized to maximize bit rate or reliability, reduce latency or power bandwidth usage, etc.). The characteristics of network architecture **600**A may change over time, for example, by upgrading equipment or by modifying procedures to target a particular characteristic. However, at any given time, network architecture **600**A will have a single set of characteristics that may or may not be optimized for a particular use case. For example, UEs **601**A, **601**B, **601**C may have different requirements, but network architecture **600**A can only be optimized for one of the three.

[0097] Network architecture **600**B is an example of a sliced physical network divided into multiple logical networks. In FIG. **6**, the physical network is divided into three logical networks, referred to as slice A, slice B, and slice C. For example, UE **601**A may be served by AN **602**A, UPF **605**A, AMF **612**, and SMF **614**A. UE **601**B may be served by AN **602**B, UPF **605**B, AMF **612**, and SMF **614**B. UE **601**C may be served by AN **602**C, UPF **605**C, AMF **612**, and SMF **614**C. Although the respective UEs **601** communicate with different network elements from a logical perspective, these network elements may be deployed by a network operator using the same physical network elements.

[0098] Each network slice may be tailored to network services having different sets of characteristics. For example, slice A may correspond to enhanced mobile broadband (eMBB) service. Mobile broadband may refer to internet access by mobile users, commonly associated with smartphones. Slice B may correspond to ultra-reliable low-latency communication (URLLC), which focuses on reliability and speed. Relative to eMBB, URLLC may improve the feasibility of use cases such as autonomous driving and telesurgery. Slice C may correspond to massive machine type communication (mMTC), which focuses on low-power services delivered to a large number of users. For example, slice C may be optimized for a dense network of battery-powered sensors that provide small amounts of data at regular intervals. Many mMTC use cases would be prohibitively expensive if they operated using an eMBB or URLLC network.

[0099] If the service requirements for one of the UEs **601** changes, then the network slice serving that UE can be updated to provide better service. Moreover, the set of network characteristics corresponding to eMBB, URLLC, and mMTC may be varied, such that differentiated species of eMBB, URLLC, and mMTC are provided. Alternatively, network operators may provide entirely new services in response to, for example, customer demand.

[0100] In FIG. **6**, each of the UEs **601** has its own network slice. However, it will be understood that a single slice may serve any number of UEs and a single UE may operate using any number of slices. Moreover, in the example network architecture **600**B, the AN **602**, UPF **605** and SMF **614** are separated into three separate slices, whereas the AMF **612** is unsliced. However, it will be understood that a network operator may deploy any architecture that selectively utilizes any mix of sliced and unsliced network elements, with different network elements divided into different numbers of slices. Although FIG. **6** only depicts three core network functions, it will be understood that other core network functions may be sliced as well. A PLMN that supports multiple network slices may maintain a separate network repository function (NFR) for each slice, enabling other NFs to discover network services associated with that slice.

[0101] Network slice selection may be controlled by an AMF, or alternatively, by a separate network slice selection function (NSSF). For example, a network operator may define and implement distinct network slice instances (NSIs). Each NSI may be associated with single network slice selection assistance information (SNSSAI). The SNSSAI may include a particular slice/service type (SST) indicator (indicating eMBB, URLLC, mMTC, etc.). as an example, a particular tracking area may be associated with one or more configured SNSSAIs. UEs may identify one or more requested and/or subscribed SNSSAIs (e.g., during registration). The network may indicate to the UE one or more allowed and/or rejected SNSSAIs.

[0102] The SNSSAI may further include a slice differentiator (SD) to distinguish between different tenants of a particular slice and/or service type. For example, a tenant may be a customer (e.g., vehicle manufacture, service provider, etc.) of a network operator that obtains (for example, purchases) guaranteed network resources and/or specific policies for handling its subscribers. The network operator may configure different slices and/or slice types, and use the SD to determine which tenant is associated with a particular slice.

[0103] FIG. **7**A, FIG. **7**B, and FIG. **7**C illustrate a user plane (UP) protocol stack, a control plane (CP) protocol stack, and services provided between protocol layers of the UP protocol stack.

[0104] The layers may be associated with an open system interconnection (OSI) model of computer networking functionality. In the OSI model, layer 1 may correspond to the bottom layer, with higher layers on top of the bottom layer. Layer 1 may correspond to a physical layer, which is concerned with the physical infrastructure used for transfer of signals (for example, cables, fiber optics, and/or radio frequency transceivers). In New Radio (NR), layer 1 may comprise a physical layer (PHY). Layer 2 may correspond to a data link layer. Layer 2 may be concerned with packaging of data (into, e.g., data frames) for transfer, between nodes of the network, using the physical infrastructure of layer 1. In NR, layer 2 may comprise a media access control layer (MAC), a radio link control layer (RLC), a packet data convergence layer (PDCP), and a service data application protocol layer (SDAP).

[0105] Layer 3 may correspond to a network layer. Layer 3 may be concerned with routing of the data which has been packaged in layer 2. Layer 3 may handle prioritization of data and traffic avoidance. In NR, layer 3 may comprise a radio resource control layer (RRC) and a non-access stratum layer (NAS). Layers 4 through 7 may correspond to a transport layer, a session layer, a presentation layer, and an application layer. The application layer interacts with an end user to provide data associated with an application. In an example, an end user implementing the application may generate data associated with the application and initiate sending of that information to a targeted data network (e.g., the Internet, an application server, etc.). Starting at the application layer, each layer in the OSI model may manipulate and/or repackage the information and deliver it to a lower layer. At the lowest layer, the manipulated and/or repackaged information may be exchanged via physical infrastructure (for example, electrically, optically, and/or electromagnetically). As it approaches the targeted data network, the information will be unpackaged and provided to higher and higher layers, until it once again reaches the application layer in a form that is usable by the targeted data network (e.g., the same form in which it was provided by the end user). To respond to the end user, the data network may perform this procedure in reverse.

[0106] FIG. **7**A illustrates a user plane protocol stack. The user plane protocol stack may be a new radio (NR) protocol stack for a Uu interface between a UE **701** and a gNB **702**. In layer 1 of the UP protocol stack, the UE **701** may implement PHY **731** and the gNB **702** may implement PHY **732**. In layer 2 of the UP protocol stack, the UE **701** may implement MAC **741**, RLC **751**, PDCP **761**, and SDAP **771**. The gNB **702** may implement MAC **742**, RLC **752**, PDCP **762**, and SDAP **772**.

[0107] FIG. **7**B illustrates a control plane protocol stack. The control plane protocol stack may be an NR protocol stack for the Uu interface between the UE **701** and the gNB **702** and/or an N1 interface between the UE **701** and an AMF **712**. In layer 1 of the CP protocol stack, the UE **701** may implement PHY **731** and the gNB **702** may implement PHY **732**. In layer 2 of the CP protocol stack, the UE **701** may implement MAC **741**, RLC **751**, PDCP **761**, RRC **781**, and NAS **791**. The gNB **702** may implement MAC **742**, RLC **752**, PDCP **762**, and RRC **782**. The AMF **712** may implement NAS **792**.

[0108] The NAS may be concerned with the non-access stratum, in particular, communication between the UE **701** and the core network (e.g., the AMF **712**). Lower layers may be concerned with the access stratum, for example, communication between the UE **701** and the gNB **702**. Messages sent between the UE **701** and the core network may be referred to as NAS messages. In an example, a NAS message may be relayed by the gNB **702**, but the content of the NAS message (e.g., information elements of the NAS message) may not be visible to the gNB **702**.

[0109] FIG. **7**C illustrates an example of services provided between protocol layers of the NR user plane protocol stack illustrated in FIG. **7**A. The UE **701** may receive services through a PDU session, which may be a logical connection between the UE **701** and a data network (DN). The UE **701** and the DN may exchange data packets associated with the PDU session. The PDU session may comprise one or more quality of service (QoS) flows. SDAP **771** and SDAP **772** may perform mapping and/or demapping between the one or more QoS flows of the PDU session and one or more radio bearers (e.g., data radio bearers). The mapping between the QoS flows and the data radio bearers may be determined in the SDAP **772** by the gNB **702**, and the UE **701** may be notified of the mapping (e.g., based on control signaling and/or reflective mapping). For reflective mapping, the SDAP **772** of the gNB **220** may mark downlink packets with a QoS flow indicator (QFI) and deliver the downlink packets to the UE **701**. The UE **701** may determine the mapping based on the QFI of the downlink packets.

[0110] PDCP **761** and PDCP **762** may perform header compression and/or decompression. Header compression may reduce the amount of data transmitted over the physical layer. The PDCP **761** and PDCP **762** may perform ciphering and/or deciphering. Ciphering may reduce unauthorized decoding of data transmitted over the physical layer (e.g., intercepted on an air interface), and protect data integrity (e.g., to ensure control messages originate from intended sources). The PDCP **761** and PDCP **762** may perform retransmissions of undelivered packets, in-sequence delivery and reordering of packets, duplication of packets, and/or identification and removal of duplicate packets. In a dual connectivity scenario, PDCP **761** and PDCP **762** may perform mapping between a split radio bearer and RLC channels.

[0111] RLC **751** and RLC **752** may perform segmentation, retransmission through Automatic Repeat Request (ARQ). The RLC **751** and RLC **752** may perform removal of duplicate data units received from MAC **741** and MAC **742**, respectively. The RLCs **213** and **223** may provide RLC channels as a service to PDCPs **214** and **224**, respectively.

[0112] MAC **741** and MAC **742** may perform multiplexing and/or demultiplexing of logical channels. MAC **741** and MAC **742** may map logical channels to transport channels. In an example, UE **701** may, in MAC **741**, multiplex data units of one or more logical channels into a transport block. The UE **701** may transmit the transport block to the gNB **702** using PHY **731**. The gNB **702** may receive the transport block using PHY **732** and demultiplex data units of the transport blocks back into logical channels. MAC **741** and MAC **742** may perform error correction through Hybrid Automatic Repeat Request (HARQ), logical channel prioritization, and/or padding.

[0113] PHY **731** and PHY **732** may perform mapping of transport channels to physical channels. PHY **731** and PHY **732** may perform digital and analog signal processing functions (e.g., coding/decoding and modulation/demodulation) for sending and receiving information (e.g., transmission via an air interface). PHY **731** and PHY **732** may perform multi-antenna mapping.

[0114] FIG. **8** illustrates an example of a quality of service (QoS) model for differentiated data exchange. In the QoS model of FIG. **8**, there are a UE **801**, a AN **802**, and a UPF **805**. The QoS model facilitates prioritization of certain packet or protocol data units (PDUs), also referred to as packets. For example, higher-priority packets may be exchanged faster and/or more reliably than lower-priority packets. The network may devote more resources to exchange of high-QoS packets.

[0115] In the example of FIG. **8**, a PDU session **810** is established between UE **801** and UPF **805**. The PDU session **810** may be a logical connection enabling the UE **801** to exchange data with a particular data network (for example, the Internet). The UE **801** may request establishment of the PDU session **810**. At the time that the PDU session **810** is established, the UE **801** may, for example, identify the targeted data network based on its data network name (DNN). The PDU session **810** may be managed, for example, by a session management function (SMF, not shown). In order to facilitate exchange of data associated with the PDU session **810**, between the UE **801** and the data network, the SMF may select the UPF **805** (and optionally, one or more other UPFs, not shown).

[0116] One or more applications associated with UE **801** may generate uplink packets **812**A-**812**E associated with the PDU session **810**. In order to work within the QoS model, UE **801** may apply QoS rules **814** to uplink packets **812**A-**812**E. The QoS rules **814** may be associated with PDU session **810** and may be determined and/or provided to the UE **801** when PDU session **810** is established and/or modified. Based on QoS rules **814**, UE **801** may classify uplink packets **812**A-**812**E, map each of the uplink packets **812**A-**812**E to a QoS flow, and/or mark uplink packets **812**A-

812E with a QoS flow indicator (QFI). As a packet travels through the network, and potentially mixes with other packets from other UEs having potentially different priorities, the QFI indicates how the packet should be handled in accordance with the QoS model. In the present illustration, uplink packets **812**A, **812**B are mapped to QoS flow **816**A, uplink packet **812**C is mapped to QoS flow **816**B, and the remaining packets are mapped to QoS flow **816**C.

[0117] The QoS flows may be the finest granularity of QoS differentiation in a PDU session. In the figure, three QoS flows **816**A-**816**C are illustrated. However, it will be understood that there may be any number of QoS flows. Some QoS flows may be associated with a guaranteed bit rate (GBR QoS flows) and others may have bit rates that are not guaranteed (non-GBR QoS flows). QoS flows may also be subject to per-UE and per-session aggregate bit rates. One of the QoS flows may be a default QoS flow. The QoS flows may have different priorities. For example, QoS flow **816**A may have a higher priority than QoS flow **816**B, which may have a higher priority than QoS flow **816**C. Different priorities may be reflected by different QoS flow characteristics. For example, QoS flows may be associated with flow bit rates. A particular QoS flow may be associated with a guaranteed flow bit rate (GFBR) and/or a maximum flow bit rate (MFBR). QoS flows may be associated with specific packet delay budgets (PDBs), packet error rates (PERs), and/or maximum packet loss rates. QoS flows may also be subject to per-UE and per-session aggregate bit rates.

[0118] In order to work within the QoS model, UE **801** may apply resource mapping rules **818** to the QoS flows **816**A-**816**C. The air interface between UE **801** and AN **802** may be associated with resources **820**. In the present illustration, QoS flow **816**A is mapped to resource **820**A, whereas QoS flows **816**B, **816**C are mapped to resource **820**B. The resource mapping rules **818** may be provided by the AN **802**. In order to meet QoS requirements, the resource mapping rules **818** may designate more resources for relatively high-priority QoS flows. With more resources, a high-priority QoS flow such as QoS flow **816**A may be more likely to obtain the high flow bit rate, low packet delay budget, or other characteristic associated with QoS rules **814**. The resources **820** may comprise, for example, radio bearers. The radio bearers (e.g., data radio bearers) may be established between the UE **801** and the AN **802**. The radio bearers in 5G, between the UE **801** and the AN **802**, may be distinct from bearers in LTE, for example, Evolved Packet System (EPS) bearers between a UE and a packet data network gateway (PGW), S1 bearers between an eNB and a serving gateway (SGW), and/or an S5/S8 bearer between an SGW and a PGW.

[0119] Once a packet associated with a particular QoS flow is received at AN **802** via resource **820**A or resource **820**B, AN **802** may separate packets into respective QoS flows **856**A-**856**C based on QoS profiles **828**. The QoS profiles **828** may be received from an SMF. Each QoS profile may correspond to a QFI, for example, the QFI marked on the uplink packets **812**A-**812**E. Each QoS profile may include QoS parameters such as 5G QoS identifier (5QI) and an allocation and retention priority (ARP). The QoS profile for non-GBR QoS flows may further include additional QoS parameters such as a reflective QoS attribute (RQA).The QoS profile for GBR QoS flows may further include additional QoS parameters such as a guaranteed flow bit rate (GFBR), a maximum flow bit rate (MFBR), and/or a maximum packet loss rate. The 5QI may be a standardized 5QI which have one-to-one mapping to a standardized combination of 5G QoS characteristics per well-known services. The 5QI may be a dynamically assigned 5QI which the standardized 5QI values are not defined. The 5QI may represent 5G QoS characteristics. The 5QI may comprise a resource type, a default priority level, a packet delay budget (PDB), a packet error rate (PER), a maximum data burst volume, and/or an averaging window. The resource type may indicate a non-GBR QoS flow, a GBR QoS flow or a delay-critical GBR QoS flow. The averaging window may represent a duration over which the GFBR and/or MFBR is calculated. ARP may be a priority level comprising pre-emption capability and a pre-emption vulnerability. Based on the ARP, the AN **802** may apply admission control for the QoS flows in a case of resource limitations.

[0120] The AN **802** may select one or more N3 tunnels **850** for transmission of the QoS flows **856**A-**856**C. After the packets are divided into QoS flows **856**A-**856**C, the packet may be sent to

UPF **805** (e.g., towards a DN) via the selected one or more N3 tunnels **850**. The UPF **805** may verify that the QFIs of the uplink packets **812**A-**812**E are aligned with the QoS rules **814** provided to the UE **801**. The UPF **805** may measure and/or count packets and/or provide packet metrics to, for example, a PCF.

[0121] The figure also illustrates a process for downlink. In particular, one or more applications may generate downlink packets **852**A-**852**E. The UPF **805** may receive downlink packets **852**A-**852**E from one or more DNs and/or one or more other UPFs. As per the QoS model, UPF **805** may apply packet detection rules (PDRs) **854** to downlink packets **852**A-**852**E. Based on PDRs **854**, UPF **805** may map packets **852**A-**852**E into QoS flows. In the present illustration, downlink packets **852**A, **852**B are mapped to QoS flow **856**A, downlink packet **852**C is mapped to QoS flow **856**B, and the remaining packets are mapped to QoS flow **856**C.

[0122] The QoS flows **856**A-**856**C may be sent to AN **802**. The AN **802** may apply resource mapping rules to the QoS flows **856**A-**856**C. In the present illustration, QoS flow **856**A is mapped to resource **820**A, whereas QoS flows **856**B, **856**C are mapped to resource **820**B. In order to meet QoS requirements, the resource mapping rules may designate more resources to high-priority QoS flows.

[0123] FIGS. **9**A-**9**D illustrate example states and state transitions of a wireless device (e.g., a UE). At any given time, the wireless device may have a radio resource control (RRC) state, a registration management (RM) state, and a connection management (CM) state.

[0124] FIG. **9**A is an example diagram showing RRC state transitions of a wireless device (e.g., a UE). The UE may be in one of three RRC states: RRC idle **910**, (e.g., RRC_IDLE), RRC inactive **920** (e.g., RRC_INACTIVE), or RRC connected **930** (e.g., RRC_CONNECTED). The UE may implement different RAN-related control-plane procedures depending on its RRC state. Other elements of the network, for example, a base station, may track the RRC state of one or more UEs and implement RAN-related control-plane procedures appropriate to the RRC state of each.

[0125] In RRC connected **930**, it may be possible for the UE to exchange data with the network (for example, the base station). The parameters necessary for exchange of data may be established and known to both the UE and the network. The parameters may be referred to and/or included in an RRC context of the UE (sometimes referred to as a UE context). These parameters may include, for example: one or more AS contexts; one or more radio link configuration parameters; bearer configuration information (e.g., relating to a data radio bearer, signaling radio bearer, logical channel, QoS flow, and/or PDU session); security information; and/or PHY, MAC, RLC, PDCP, and/or SDAP layer configuration information. The base station with which the UE is connected may store the RRC context of the UE.

[0126] While in RRC connected **930**, mobility of the UE may be managed by the access network, whereas the UE itself may manage mobility while in RRC idle **910** and/or RRC inactive **920**. While in RRC connected **930**, the UE may manage mobility by measuring signal levels (e.g., reference signal levels) from a serving cell and neighboring cells and reporting these measurements to the base station currently serving the UE. The network may initiate handover based on the reported measurements. The RRC state may transition from RRC connected **930** to RRC idle **910** through a connection release procedure **930** or to RRC inactive **920** through a connection inactivation procedure **932**.

[0127] In RRC idle **910**, an RRC context may not be established for the UE. In RRC idle **910**, the UE may not have an RRC connection with a base station. While in RRC idle **910**, the UE may be in a sleep state for a majority of the time (e.g., to conserve battery power). The UE may wake up periodically (e.g., once in every discontinuous reception cycle) to monitor for paging messages from the access network. Mobility of the UE may be managed by the UE through a procedure known as cell reselection. The RRC state may transition from RRC idle **910** to RRC connected **930** through a connection establishment procedure **913**, which may involve a random access procedure, as discussed in greater detail below.

[0128] In RRC inactive **920**, the RRC context previously established is maintained in the UE and the base station. This may allow for a fast transition to RRC connected **930** with reduced signaling overhead as compared to the transition from RRC idle **910** to RRC connected **930**. The RRC state may transition to RRC connected **930** through a connection resume procedure **923**. The RRC state may transition to RRC idle **910** though a connection release procedure **921** that may be the same as or similar to connection release procedure **931**.

[0129] An RRC state may be associated with a mobility management mechanism. In RRC idle **910** and RRC inactive **920**, mobility may be managed by the UE through cell reselection. The purpose of mobility management in RRC idle **910** and/or RRC inactive **920** is to allow the network to be able to notify the UE of an event via a paging message without having to broadcast the paging message over the entire mobile communications network. The mobility management mechanism used in RRC idle **910** and/or RRC inactive **920** may allow the network to track the UE on a cell-group level so that the paging message may be broadcast over the cells of the cell group that the UE currently resides within instead of the entire communication network. Tracking may be based on different granularities of grouping. For example, there may be three levels of cell-grouping granularity: individual cells; cells within a RAN area identified by a RAN area identifier (RAI); and cells within a group of RAN areas, referred to as a tracking area and identified by a tracking area identifier (TAI).

[0130] Tracking areas may be used to track the UE at the CN level. The CN may provide the UE with a list of TAIs associated with a UE registration area. If the UE moves, through cell reselection, to a cell associated with a TAI not included in the list of TAIs associated with the UE registration area, the UE may perform a registration update with the CN to allow the CN to update the UE's location and provide the UE with a new the UE registration area.

[0131] RAN areas may be used to track the UE at the RAN level. For a UE in RRC inactive **920** state, the UE may be assigned a RAN notification area. A RAN notification area may comprise one or more cell identities, a list of RAIs, and/or a list of TAIs. In an example, a base station may belong to one or more RAN notification areas. In an example, a cell may belong to one or more RAN notification areas. If the UE moves, through cell reselection, to a cell not included in the RAN notification area assigned to the UE, the UE may perform a notification area update with the RAN to update the UE's RAN notification area.

[0132] A base station storing an RRC context for a UE or a last serving base station of the UE may be referred to as an anchor base station. An anchor base station may maintain an RRC context for the UE at least during a period of time that the UE stays in a RAN notification area of the anchor base station and/or during a period of time that the UE stays in RRC inactive **920**.

[0133] FIG. **9**B is an example diagram showing registration management (RM) state transitions of a wireless device (e.g., a UE). The states are RM deregistered **940**, (e.g., RM-DEREGISTERED) and RM registered **950** (e.g., RM-REGISTERED).

[0134] In RM deregistered **940**, the UE is not registered with the network, and the UE is not reachable by the network. In order to be reachable by the network, the UE must perform an initial registration. As an example, the UE may register with an AMF of the network. If registration is rejected (registration reject **944**), then the UE remains in RM deregistered **940**. If registration is accepted (registration accept **945**), then the UE transitions to RM registered **950**. While the UE is RM registered **950**, the network may store, keep, and/or maintain a UE context for the UE. The UE context may be referred to as wireless device context. The UE context corresponding to network registration (maintained by the core network) may be different from the RRC context corresponding to RRC state (maintained by an access network, e.g., a base station). The UE context may comprise a UE identifier and a record of various information relating to the UE, for example, UE capability information, policy information for access and mobility management of the UE, lists of allowed or established slices or PDU sessions, and/or a registration area of the UE (i.e., a list of tracking areas covering the geographical area where the wireless device is likely to be found).

[0135] While the UE is RM registered **950**, the network may store the UE context of the UE, and if necessary use the UE context to reach the UE. Moreover, some services may not be provided by the network unless the UE is registered. The UE may update its UE context while remaining in RM registered **950** (registration update accept **955**). For example, if the UE leaves one tracking area and enters another tracking area, the UE may provide a tracking area identifier to the network. The network may deregister the UE, or the UE may deregister itself (deregistration **954**). For example, the network may automatically deregister the wireless device if the wireless device is inactive for a certain amount of time. Upon deregistration, the UE may transition to RM deregistered **940**.

[0136] FIG. **9**C is an example diagram showing connection management (CM) state transitions of a wireless device (e.g., a UE), shown from a perspective of the wireless device. The UE may be in CM idle **960** (e.g., CM-IDLE) or CM connected **970** (e.g., CM-CONNECTED).

[0137] In CM idle **960**, the UE does not have a non access stratum (NAS) signaling connection with the network. As a result, the UE can not communicate with core network functions. The UE may transition to CM connected **970** by establishing an AN signaling connection (AN signaling connection establishment **967**). This transition may be initiated by sending an initial NAS message. The initial NAS message may be a registration request (e.g., if the UE is RM deregistered **940**) or a service request (e.g., if the UE is RM registered **950**). If the UE is RM registered **950**, then the UE may initiate the AN signaling connection establishment by sending a service request, or the network may send a page, thereby triggering the UE to send the service request.

[0138] In CM connected **970**, the UE can communicate with core network functions using NAS signaling. As an example, the UE may exchange NAS signaling with an AMF for registration management purposes, service request procedures, and/or authentication procedures. As another example, the UE may exchange NAS signaling, with an SMF, to establish and/or modify a PDU session. The network may disconnect the UE, or the UE may disconnect itself (AN signaling connection release **976**). For example, if the UE transitions to RM deregistered **940**, then the UE may also transition to CM idle **960**. When the UE transitions to CM idle **960**, the network may deactivate a user plane connection of a PDU session of the UE.

[0139] FIG. **9**D is an example diagram showing CM state transitions of the wireless device (e.g., a UE), shown from a network perspective (e.g., an AMF). The CM state of the UE, as tracked by the AMF, may be in CM idle **980** (e.g., CM-IDLE) or CM connected **990** (e.g., CM-CONNECTED). When the UE transitions from CM idle **980** to CM connected **990**, the AMF many establish an N2 context of the UE (N2 context establishment **989**). When the UE transitions from CM connected **990** to CM idle **980**, the AMF many release the N2 context of the UE (N2 context release **998**).

[0140] FIGS. **10-12** illustrate example procedures for registering, service request, and PDU session establishment of a UE.

[0141] FIG. **10** illustrates an example of a registration procedure for a wireless device (e.g., a UE). Based on the registration procedure, the UE may transition from, for example, RM deregistered **940** to RM registered **950**.

[0142] Registration may be initiated by a UE for the purposes of obtaining authorization to receive services, enabling mobility tracking, enabling reachability, or other purposes. The UE may perform an initial registration as a first step toward connection to the network (for example, if the UE is powered on, airplane mode is turned off, etc.). Registration may also be performed periodically to keep the network informed of the UE's presence (for example, while in CM-IDLE state), or in response to a change in UE capability or registration area. Deregistration (not shown in FIG. **10**) may be performed to stop network access.

[0143] At **1010**, the UE transmits a registration request to an AN. As an example, the UE may have moved from a coverage area of a previous AMF (illustrated as AMF #1) into a coverage area of a new AMF (illustrated as AMF #2). The registration request may be a NAS message. The registration request may include a UE identifier. The AN may select an AMF for registration of the UE. For example, the AN may select a default AMF. For example, the AN may select an AMF that is already mapped to the UE (e.g., a previous AMF). The NAS registration request may include a network slice identifier and the AN may select an AMF based on the requested slice. After the AMF is selected, the AN may send the registration request to the selected AMF.

[0144] At **1020**, the AMF that receives the registration request (AMF #2) performs a context transfer. The context may be a UE context, for example, an RRC context for the UE. As an example, AMF #2 may send AMF #1 a message requesting a context of the UE. The message may include the UE identifier. The message may be a Namf_Communication_UEContextTransfer message. AMF #1 may send to AMF #2 a message that includes the requested UE context. This message may be a Namf_Communication_UEContextTransfer message. After the UE context is received, the AMF #2 may coordinate authentication of the UE. After authentication is complete, AMF #2 may send to AMF #1 a message indicating that the UE context transfer is complete. This message may be a Namf_Communication_UEContextTransfer Response message.

[0145] Authentication may require participation of the UE, an AUSF, a UDM and/or a UDR (not shown). For example, the AMF may request that the AUSF authenticate the UE. For example, the AUSF may execute authentication of the UE. For example, the AUSF may get authentication data from UDM. For example, the AUSF may send a subscription permanent identifier (SUPI) to the AMF based on the authentication being successful. For example, the AUSF may provide an intermediate key to the AMF. The intermediate key may be used to derive an access-specific security key for the UE, enabling the AMF to perform security context management (SCM). The AUSF may obtain subscription data from the UDM. The subscription data may be based on information obtained from the UDM (and/or the UDR). The subscription data may include subscription identifiers, security credentials, access and mobility related subscription data and/or session related data.

[0146] At **1030**, the new AMF, AMF #2, registers and/or subscribes with the UDM. AMF #2 may perform registration using a UE context management service of the UDM (Nudm_UECM). AMF #2 may obtain subscription information of the UE using a subscriber data management service of the UDM (Nudm_SDM). AMF #2 may further request that the UDM notify AMF #2 if the subscription information of the UE changes. As the new AMF registers and subscribes, the old AMF, AMF #1, may deregister and unsubscribe. After deregistration, AMF #1 is free of responsibility for mobility management of the UE.

[0147] At **1040**, AMF #2 retrieves access and mobility (AM) policies from the PCF. As an example, the AMF #2 may provide subscription data of the UE to the PCF. The PCF may determine access and mobility policies for the UE based on the subscription data, network operator data, current network conditions, and/or other suitable information. For example, the owner of a first UE may purchase a higher level of service than the owner of a second UE. The PCF may provide the rules associated with the different levels of service. Based on the subscription data of the respective UEs, the network may apply different policies which facilitate different levels of service.

[0148] For example, access and mobility policies may relate to service area restrictions, RAT/frequency selection priority (RFSP, where RAT stands for radio access technology), authorization and prioritization of access type (e.g., LTE versus NR), and/or selection of non-3GPP access (e.g., Access Network Discovery and Selection Policy (ANDSP)). The service area restrictions may comprise a list of tracking areas where the UE is allowed to be served (or forbidden from being served). The access and mobility policies may include a UE route selection policy (URSP)) that influences routing to an established PDU session or a new PDU session. As noted above, different policies may be obtained and/or enforced based on subscription data of the UE, location of the UE (i.e., location of the AN and/or AMF), or other suitable factors.

[0149] At **1050**, AMF #2 may update a context of a PDU session. For example, if the UE has an existing PDU session, the AMF #2 may coordinate with an SMF to activate a user plane connection associated with the existing PDU session. The SMF may update and/or release a session management context of the PDU session (Nsmf_PDUSession_UpdateSMContext, Nsmf_PDUSession_ReleaseSMContext).

[0150] At **1060**, AMF #2 sends a registration accept message to the AN, which forwards the registration accept message to the UE. The registration accept message may include a new UE identifier and/or a new configured slice identifier. The UE may transmit a registration complete message to the AN, which forwards the registration complete message to the AMF #2. The registration complete message may acknowledge receipt of the new UE identifier and/or new configured slice identifier.

[0151] At **1070**, AMF #2 may obtain UE policy control information from the PCF. The PCF may provide an access network discovery and selection policy (ANDSP) to facilitate non-3GPP access. The PCF may provide a UE route selection policy (URSP) to facilitate mapping of particular data traffic to particular PDU session connectivity parameters. As an example, the URSP may indicate that data traffic associated with a particular application should be mapped to a particular SSC mode, network slice, PDU session type, or preferred access type (3GPP or non-3GPP).

[0152] FIG. **11** illustrates an example of a service request procedure for a wireless device (e.g., a UE). The service request procedure depicted in FIG. **11** is a network-triggered service request procedure for a UE in a CM-IDLE state. However, other service request procedures (e.g., a UE-triggered service request procedure) may also be understood by reference to FIG. **11**, as will be discussed in greater detail below.

[0153] At **1110**, a UPF receives data. The data may be downlink data for transmission to a UE. The data may be associated with an existing PDU session between the UE and a DN. The data may be received, for example, from a DN and/or another UPF. The UPF may buffer the received data. In response to the receiving of the data, the UPF may notify an SMF of the received data. The identity of the SMF to be notified may be determined based on the received data. The notification may be, for example, an N4 session report. The notification may indicate that the UPF has received data associated with the UE and/or a particular PDU session associated with the UE. In response to receiving the notification, the SMF may send PDU session information to an AMF. The PDU session information may be sent in an N1N2 message transfer for forwarding to an AN. The PDU session information may include, for example, UPF tunnel endpoint information and/or QoS information.

[0154] At **1120**, the AMF determines that the UE is in a CM-IDLE state. The determining at **1120** may be in response to the receiving of the PDU session information. Based on the determination that the UE is CM-IDLE, the service request procedure may proceed to **1130** and **1140**, as depicted in FIG. **11**. However, if the UE is not CM-IDLE (e.g., the UE is CM-CONNECTED), then **1130** and **1140** may be skipped, and the service request procedure may proceed directly to **1150**.

[0155] At **1130**, the AMF pages the UE. The paging at **1130** may be performed based on the UE being CM-IDLE. To perform the paging, the AMF may send a page to the AN. The page may be referred to as a paging or a paging message. The page may be an N2 request message. The AN may be one of a plurality of ANs in a RAN notification area of the UE. The AN may send a page to the UE. The UE may be in a coverage area of the AN and may receive the page.

[0156] At **1140**, the UE may request service. The UE may transmit a service request to the AMF via the AN. As depicted in FIG. **11**, the UE may request service at **1140** in response to receiving the paging at **1130**. However, as noted above, this is for the specific case of a network-triggered service request procedure. In some scenarios (for example, if uplink data becomes available at the UE), then the UE may commence a UE-triggered service request procedure. The UE-triggered service request procedure may commence starting at **1140**.

[0157] At **1150**, the network may authenticate the UE. Authentication may require participation of the UE, an AUSF, and/or a UDM, for example, similar to authentication described elsewhere in the present disclosure. In some cases (for example, if the UE has recently been authenticated), the authentication at **1150** may be skipped.

[0158] At **1160**, the AMF and SMF may perform a PDU session update. As part of the PDU session update, the SMF may provide the AMF with one or more UPF tunnel endpoint identifiers. In some cases (not shown in FIG. **11**), it may be necessary for the SMF to coordinate with one or more other SMFs and/or one or more other UPFs to set up a user plane.

[0159] At **1170**, the AMF may send PDU session information to the AN. The PDU session information may be included in an N2 request message. Based on the PDU session information, the AN may configure a user plane resource for the UE. To configure the user plane resource, the AN may, for example, perform an RRC reconfiguration of the UE. The AN may acknowledge to the AMF that the PDU session information has been received. The AN may notify the AMF that the user plane resource has been configured, and/or provide information relating to the user plane resource configuration.

[0160] In the case of a UE-triggered service request procedure, the UE may receive, at **1170**, a NAS service accept message from the AMF via the AN. After the user plane resource is configured, the UE may transmit uplink data (for example, the uplink data that caused the UE to trigger the service request procedure).

[0161] At **1180**, the AMF may update a session management (SM) context of the PDU session. For example, the AMF may notify the SMF (and/or one or more other associated SMFs) that the user plane resource has been configured, and/or provide information relating to the user plane resource configuration. The AMF may provide the SMF (and/or one or more other associated SMFs) with one or more AN tunnel endpoint identifiers of the AN. After the SM context update is complete, the SMF may send an update SM context response message to the AMF.

[0162] Based on the update of the session management context, the SMF may update a PCF for purposes of policy control. For example, if a location of the UE has changed, the SMF may notify the PCF of the UE's a new location.

[0163] Based on the update of the session management context, the SMF and UPF may perform a session modification. The session modification may be performed using N4 session modification messages. After the session modification is complete, the UPF may transmit downlink data (for example, the downlink data that caused the UPF to trigger the network-triggered service request procedure) to the UE. The transmitting of the downlink data may be based on the one or more AN tunnel endpoint identifiers of the AN.

[0164] FIG. **12** illustrates an example of a protocol data unit (PDU) session establishment procedure for a wireless device (e.g., a UE). The UE may determine to transmit the PDU session establishment request to create a new PDU session, to hand over an existing PDU session to a 3GPP network, or for any other suitable reason.

[0165] At **1210**, the UE initiates PDU session establishment. The UE may transmit a PDU session establishment request to an AMF via an AN. The PDU session establishment request may be a NAS message. The PDU session establishment request may indicate: a PDU session ID; a requested PDU session type (new or existing); a requested DN (DNN); a requested network slice (S-NSSAI); a requested SSC mode; and/or any other suitable information. The PDU session ID may be generated by the UE. The PDU session type may be, for example, an Internet Protocol (IP)-based type (e.g., IPv4, IPv6, or dual stack IPv4/IPv6), an Ethernet type, or an unstructured type.

[0166] The AMF may select an SMF based on the PDU session establishment request. In some scenarios, the requested PDU session may already be associated with a particular SMF. For example, the AMF may store a UE context of the UE, and the UE context may indicate that the PDU session ID of the requested PDU session is already associated with the particular SMF. In some scenarios, the AMF may select the SMF based on a determination that the SMF is prepared to handle the requested PDU session. For example, the requested PDU session may be associated with a particular DNN and/or S-NSSAI, and the SMF may be selected based on a determination that the SMF can manage a PDU session associated with the particular DNN and/or S-NSSAI.

[0167] At **1220**, the network manages a context of the PDU session. After selecting the SMF at **1210**, the AMF sends a PDU session context request to the SMF. The PDU session context request may include the PDU session establishment request received from the UE at **1210**. The PDU session context request may be a Nsmf_PDUSession_CreateSMContext Request and/or a Nsmf_PDUSession_UpdateSMContext Request. The PDU session context request may indicate identifiers of the UE; the requested DN; and/or the requested network slice. Based on the PDU session context request, the SMF may retrieve subscription data from a UDM. The subscription data may be session management subscription data of the UE. The SMF may subscribe for updates to the subscription data, so that the PCF will send new information if the subscription data of the UE changes. After the subscription data of the UE is obtained, the SMF may transmit a PDU session context response to the AMG. The PDU session context response may be a Nsmf_PDUSession_CreateSMContext Response and/or a Nsmf_PDUSession_UpdateSMContext Response. The PDU session context response may include a session management context ID.

[0168] At **1230**, secondary authorization/authentication may be performed, if necessary. The secondary authorization/authentication may involve the UE, the AMF, the SMF, and the DN. The SMF may access the DN via a Data Network Authentication, Authorization and Accounting (DN AAA) server.

[0169] At **1240**, the network sets up a data path for uplink data associated with the PDU session. The SMF may select a PCF and establish a session management policy association. Based on the association, the PCF may provide an initial set of policy control and charging rules (PCC rules) for the PDU session. When targeting a particular PDU session, the PCF may indicate, to the SMF, a method for allocating an IP address to the PDU Session, a default charging method for the PDU session, an address of the corresponding charging entity, triggers for requesting new policies, etc. The PCF may also target a service data flow (SDF) comprising one or more PDU sessions. When targeting an SDF, the PCF may indicate, to the SMF, policies for applying QoS requirements, monitoring traffic (e.g., for charging purposes), and/or steering traffic (e.g., by using one or more particular N6 interfaces).

[0170] The SMF may determine and/or allocate an IP address for the PDU session. The SMF may select one or more UPFs (a single UPF in the example of FIG. **12**) to handle the PDU session. The SMF may send an N4 session message to the selected UPF. The N4 session message may be an N4 Session Establishment Request and/or an N4 Session Modification Request. The N4 session message may include packet detection, enforcement, and reporting rules associated with the PDU session. In response, the UPF may acknowledge by sending an N4 session establishment response and/or an N4 session modification response.

[0171] The SMF may send PDU session management information to the AMF. The PDU session management information may be a Namf_Communication_N1N2MessageTransfer message. The PDU session management information may include the PDU session ID. The PDU session management information may be a NAS message. The PDU session management information may include N1 session management information and/or N2 session management information. The N1 session management information may include a PDU session establishment accept message. The PDU session establishment accept message may include tunneling endpoint information of the UPF and quality of service (QoS) information associated with the PDU session.

[0172] The AMF may send an N2 request to the AN. The N2 request may include the PDU session establishment accept message. Based on the N2 request, the AN may determine AN resources for the UE. The AN resources may be used by the UE to establish the PDU session, via the AN, with the DN. The AN may determine resources to be used for the PDU session and indicate the determined resources to the UE. The AN may send the PDU session establishment accept message to the UE. For example, the AN may perform an RRC reconfiguration of the UE. After the AN resources are set up, the AN may send an N2 request acknowledge to the AMF. The N2 request acknowledge may include N2 session management information, for example, the PDU session ID and tunneling endpoint information of the AN.

[0173] After the data path for uplink data is set up at **1240**, the UE may optionally send uplink data associated with the PDU session. As shown in FIG. **12**, the uplink data may be sent to a DN associated with the PDU session via the AN and the UPF.

[0174] At **1250**, the network may update the PDU session context. The AMF may transmit a PDU session context update request to the SMF. The PDU session context update request may be a Nsmf_PDUSession_UpdateSMContext Request. The PDU session context update request may include the N2 session management information received from the AN. The SMF may acknowledge the PDU session context update. The acknowledgement may be a Nsmf_PDUSession_UpdateSMContext Response. The acknowledgement may include a subscription requesting that the SMF be notified of any UE mobility event. Based on the PDU session context update request, the SMF may send an N4 session message to the UPF. The N4 session message may be an N4 Session Modification Request. The N4 session message may include tunneling end point information of the AN. The N4 session message may include forwarding rules associated with the PDU session. In response, the UPF may acknowledge by sending an N4 session modification response.

[0175] After the UPF receives the tunneling endpoint information of the AN, the UPF may relay downlink data associated with the PDU session. As shown in FIG. **12**, the downlink data may be received from a DN associated with the PDU session via the AN and the UPF.

[0176] FIG. **13** illustrates examples of components of the elements in a communications network. FIG. **13** includes a wireless device **1310**, a base station **1320**, and a physical deployment of one or more network functions **1330** (henceforth “deployment **1330**”). Any wireless device described in the present disclosure may have similar components and may be implemented in a similar manner as the wireless device **1310**. Any other base station described in the present disclosure (or any portion thereof, depending on the architecture of the base station) may have similar components and may be implemented in a similar manner as the base station **1320**. Any physical core network deployment in the present disclosure (or any portion thereof, depending on the architecture of the base station) may have similar components and may be implemented in a similar manner as the deployment **1330**.

[0177] The wireless device **1310** may communicate with base station **1320** over an air interface **1370**. The communication direction from wireless device **1310** to base station **1320** over air interface **1370** is known as uplink, and the communication direction from base station **1320** to wireless device **1310** over air interface **1370** is known as downlink. Downlink transmissions may be separated from uplink transmissions using FDD, TDD, and/or some combination of duplexing techniques. FIG. **13** shows a single wireless device **1310** and a single base station **1320**, but it will be understood that wireless device **1310** may communicate with any number of base stations or other access network components over air interface **1370**, and that base station **1320** may communicate with any number of wireless devices over air interface **1370**.

[0178] The wireless device **1310** may comprise a processing system **1311** and a memory **1312**. The memory **1312** may comprise one or more computer-readable media, for example, one or more non-transitory computer readable media. The memory **1312** may include instructions **1313**. The processing system **1311** may process and/or execute instructions **1313**. Processing and/or execution of instructions **1313** may cause wireless device **1310** and/or processing system **1311** to perform one or more functions or activities. The memory **1312** may include data (not shown). One of the functions or activities performed by processing system **1311** may be to store data in memory **1312** and/or retrieve previously-stored data from memory **1312**. In an example, downlink data received from base station **1320** may be stored in memory **1312**, and uplink data for transmission to base station **1320** may be retrieved from memory **1312**. As illustrated in FIG. **13**, the wireless device **1310** may communicate with base station **1320** using a transmission processing system **1314** and/or a reception processing system **1315**. Alternatively, transmission processing system **1314** and reception processing system **1315** may be implemented as a single processing system, or both may be omitted and all processing in the wireless device **1310** may be performed by the processing system **1311**. Although not shown in FIG. **13**, transmission processing system **1314** and/or reception processing system **1315** may be coupled to a dedicated memory that is analogous to but separate from memory **1312**, and comprises instructions that may be processed and/or executed to carry out one or more of their respective functionalities. The wireless device **1310** may comprise one or more antennas **1316** to access air interface **1370**.

[0179] The wireless device **1310** may comprise one or more other elements **1319**. The one or more other elements **1319** may comprise software and/or hardware that provide features and/or functionalities, for example, a speaker, a microphone, a keypad, a display, a touchpad, a satellite transceiver, a universal serial bus (USB) port, a hands-free headset, a frequency modulated (FM) radio unit, a media player, an Internet browser, an electronic control unit (e.g., for a motor vehicle), and/or one or more sensors (e.g., an accelerometer, a gyroscope, a temperature sensor, a radar sensor, a lidar sensor, an ultrasonic sensor, a light sensor, a camera, a global positioning sensor (GPS) and/or the like). The wireless device **1310** may receive user input data from and/or provide user output data to the one or more one or more other elements **1319**. The one or more other elements **1319** may comprise a power source. The wireless device **1310** may receive power from the power source and may be configured to distribute the power to the other components in wireless device **1310**. The power source may comprise one or more sources of power, for example, a battery, a solar cell, a fuel cell, or any combination thereof.

[0180] The wireless device **1310** may transmit uplink data to and/or receive downlink data from base station **1320** via air interface **1370**. To perform the transmission and/or reception, one or more of the processing system **1311**, transmission processing system **1314**, and/or reception system **1315** may implement open systems interconnection (OSI) functionality. As an example, transmission processing system **1314** and/or reception system **1315** may perform layer 1 OSI functionality, and processing system **1311** may perform higher layer functionality. The wireless device **1310** may transmit and/or receive data over air interface **1370** using one or more antennas **1316**. For scenarios where the one or more antennas **1316** include multiple antennas, the multiple antennas may be used to perform one or more multi-antenna techniques, such as spatial multiplexing (e.g., single-user multiple-input multiple output (MIMO) or multi-user MIMO), transmit/receive diversity, and/or beamforming.

[0181] The base station **1320** may comprise a processing system **1321** and a memory **1322**. The memory **1322** may comprise one or more computer-readable media, for example, one or more non-transitory computer readable media. The memory **1322** may include instructions **1323**. The processing system **1321** may process and/or execute instructions **1323**. Processing and/or execution of instructions **1323** may cause base station **1320** and/or processing system **1321** to perform one or more functions or activities. The memory **1322** may include data (not shown). One of the functions or activities performed by processing system **1321** may be to store data in memory **1322** and/or retrieve previously-stored data from memory **1322**. The base station **1320** may communicate with wireless device **1310** using a transmission processing system **1324** and a reception processing system **1325**. Although not shown in FIG. **13**, transmission processing system **1324** and/or reception processing system **1325** may be coupled to a dedicated memory that is analogous to but separate from memory **1322**, and comprises instructions that may be processed and/or executed to carry out one or more of their respective functionalities. The wireless device **1320** may comprise one or more antennas **1326** to access air interface **1370**.

[0182] The base station **1320** may transmit downlink data to and/or receive uplink data from wireless device **1310** via air interface **1370**. To perform the transmission and/or reception, one or more of the processing system **1321**, transmission processing system **1324**, and/or reception system **1325** may implement OSI functionality. As an example, transmission processing system **1324** and/or reception system **1325** may perform layer 1 OSI functionality, and processing system **1321** may perform higher layer functionality. The base station **1320** may transmit and/or receive data over air interface **1370** using one or more antennas **1326**. For scenarios where the one or more antennas **1326** include multiple antennas, the multiple antennas may be used to perform one or more multi-antenna techniques, such as spatial multiplexing (e.g., single-user multiple-input multiple output (MIMO) or multi-user MIMO), transmit/receive diversity, and/or beamforming.

[0183] The base station **1320** may comprise an interface system **1327**. The interface system **1327** may communicate with one or more base stations and/or one or more elements of the core network via an interface **1380**. The interface **1380** may be wired and/or wireless and interface system **1327** may include one or more components suitable for communicating via interface **1380**. In FIG. **13**, interface **1380** connects base station **1320** to a single deployment **1330**, but it will be understood that wireless device **1310** may communicate with any number of base stations and/or CN deployments over interface **1380**, and that deployment **1330** may communicate with any number of base stations and/or other CN deployments over interface **1380**. The base station **1320** may comprise one or more other elements **1329** analogous to one or more of the one or more other elements **1319**.

[0184] The deployment **1330** may comprise any number of portions of any number of instances of one or more network functions (NFs). The deployment **1330** may comprise a processing system **1331** and a memory **1332**. The memory **1332** may comprise one or more computer-readable media, for example, one or more non-transitory computer readable media. The memory **1332** may include instructions **1333**. The processing system **1331** may process and/or execute instructions **1333**. Processing and/or execution of instructions **1333** may cause the deployment **1330** and/or processing system **1331** to perform one or more functions or activities. The memory **1332** may include data (not shown). One of the functions or activities performed by processing system **1331** may be to store data in memory **1332** and/or retrieve previously-stored data from memory **1332**. The deployment **1330** may access the interface **1380** using an interface system **1337**. The deployment **1330** may comprise one or more other elements **1339** analogous to one or more of the one or more other elements **1319**.

[0185] One or more of the systems **1311**, **1314**, **1315**, **1321**, **1324**, **1325**, and/or **1331** may comprise one or more controllers and/or one or more processors. The one or more controllers and/or one or more processors may comprise, for example, a general-purpose processor, a digital signal processor (DSP), a microcontroller, an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) and/or other programmable logic device, discrete gate and/or transistor logic, discrete hardware components, an on-board unit, or any combination thereof. One or more of the systems **1311**, **1314**, **1315**, **1321**, **1324**, **1325**, and/or **1331** may perform signal coding/processing, data processing, power control, input/output processing, and/or any other functionality that may enable wireless device **1310**, base station **1320**, and/or deployment **1330** to operate in a mobile communications system.

[0186] Many of the elements described in the disclosed embodiments may be implemented as modules. A module is defined here as an element that performs a defined function and has a defined interface to other elements. The modules described in this disclosure may be implemented in hardware, software in combination with hardware, firmware, wetware (e.g. hardware with a biological element) or a combination thereof, which may be behaviorally equivalent. For example, modules may be implemented as a software routine written in a computer language configured to be executed by a hardware machine (such as C, C++, Fortran, Java, Basic, Matlab or the like) or a modeling/simulation program such as Simulink, Stateflow, GNU Octave, or LabVIEWMathScript. It may be possible to implement modules using physical hardware that incorporates discrete or programmable analog, digital and/or quantum hardware. Examples of programmable hardware comprise computers, microcontrollers, microprocessors, DSPs, ASICs, FPGAs, and complex programmable logic devices (CPLDs). Computers, microcontrollers and microprocessors may be programmed using languages such as assembly, C, C++ or the like. FPGAs, ASICs and CPLDs are often programmed using hardware description languages (HDL) such as VHSIC hardware description language (VHDL) or Verilog that configure connections between internal hardware modules with lesser functionality on a programmable device. The mentioned technologies are often used in combination to achieve the result of a functional module.

[0187] The wireless device **1310**, base station **1320**, and/or deployment **1330** may implement timers and/or counters. A timer/counter may start at an initial value. As used herein, starting may comprise restarting. Once started, the timer/counter may run. Running of the timer/counter may be associated with an occurrence. When the occurrence occurs, the value of the timer/counter may change (for example, increment or decrement). The occurrence may be, for example, an exogenous event (for example, a reception of a signal, a measurement of a condition, etc.), an endogenous event (for example, a transmission of a signal, a calculation, a comparison, a performance of an action or a decision to so perform, etc.), or any combination thereof. In the case of a timer, the occurrence may be the passage of a particular amount of time. However, it will be understood that a timer may be described and/or implemented as a counter that counts the passage of a particular unit of time. A timer/counter may run in a direction of a final value until it reaches the final value. The reaching of the final value may be referred to as expiration of the timer/counter. The final value may be referred to as a threshold. A timer/counter may be paused, wherein the present value of the timer/counter is held, maintained, and/or carried over, even upon the occurrence of one or more occurrences that would otherwise cause the value of the timer/counter to change. The timer/counter may be un-paused or continued, wherein the value that was held, maintained, and/or carried over begins changing again when the one or more occurrence occur. A timer/counter may be set and/or reset. As used herein, setting may comprise resetting. When the timer/counter sets and/or resets, the value of the timer/counter may be set to the initial value. A timer/counter m ay be started and/or restarted. As used herein, starting may comprise restarting. In some embodiments, when the timer/counter restarts, the value of the timer/counter may be set to the initial value and the timer/counter may begin to run.

[0188] FIGS. **14**A, **14**B, **14**C, and **14**D illustrate various example arrangements of physical core network deployments, each having one or more network functions or portions thereof. The core network deployments comprise a deployment **1410**, a deployment **1420**, a deployment **1430**, a deployment **1440**, and/or a deployment **1450**. Each deployment may be analogous to, for example, the deployment **1330** depicted in FIG. **13**. In particular, each deployment may comprise a processing system for performing one or more functions or activities, memory for storing data and/or instructions, and an interface system for communicating with other network elements (for example, other core network deployments). Each deployment may comprise one or more network functions (NFs). The term NF may refer to a particular set of functionalities and/or one or more physical elements configured to perform those functionalities (e.g., a processing system and memory comprising instructions that, when executed by the processing system, cause the processing system to perform the functionalities). For example, in the present disclosure, when a network function is described as performing X, Y, and Z, it will be understood that this refers to the one or more physical elements configured to perform X, Y, and Z, no matter how or where the one or more physical elements are deployed. The term NF may refer to a network node, network element, and/or network device.

[0189] As will be discussed in greater detail below, there are many different types of NF and each type of NF may be associated with a different set of functionalities. A plurality of different NFs may be flexibly deployed at different locations (for example, in different physical core network deployments) or in a same location (for example, co-located in a same deployment). A single NF may be flexibly deployed at different locations (implemented using different physical core network deployments) or in a same location. Moreover, physical core network deployments may also implement one or more base stations, application functions (AFs), data networks (DNs), or any portions thereof. NFs may be implemented in many ways, including as network elements on dedicated or shared hardware, as software instances running on dedicated or shared hardware, or as virtualized functions instantiated on a platform (e.g., a cloud-based platform).

[0190] FIG. **14**A illustrates an example arrangement of core network deployments in which each deployment comprises one network function. A deployment **1410** comprises an NF **1411**, a deployment **1420** comprises an NF **1421**, and a deployment **1430** comprises an NF **1431**. The deployments **1410**, **1420**, **1430** communicate via an interface **1490**. The deployments **1410**, **1420**, **1430** may have different physical locations with different signal propagation delays relative to other network elements. The diversity of physical locations of deployments **1410**, **1420**, **1430** may enable provision of services to a wide area with improved speed, coverage, security, and/or efficiency.

[0191] FIG. **14**B illustrates an example arrangement wherein a single deployment comprises more than one NF. Unlike FIG. **14**A, where each NF is deployed in a separate deployment, FIG. **14**B illustrates multiple NFs in deployments **1410**, **1420**. In an example, deployments **1410**, **1420** may implement a software-defined network (SDN) and/or a network function virtualization (NFV).

[0192] For example, deployment **1410** comprises an additional network function, NF **1411**A. The NFs **1411**, **1411**A may consist of multiple instances of the same NF type, co-located at a same physical location within the same deployment **1410**. The NFs **1411**, **1411**A may be implemented independently from one another (e.g., isolated and/or independently controlled). For example, the NFs **1411**, **1411**A may be associated with different network slices. A processing system and memory associated with the deployment **1410** may perform all of the functionalities associated with the NF **1411** in addition to all of the functionalities associated with the NF **1411**A. In an example, NFs **1411**, **1411**A may be associated with different PLMNs, but deployment **1410**, which implements NFs **1411**, **1411**A, may be owned and/or operated by a single entity.

[0193] Elsewhere in FIG. **14**B, deployment **1420** comprises NF **1421** and an additional network function, NF **1422**. The NFs **1421**, **1422** may be different NF types. Similar to NFs **1411**, **1411**A, the NFs **1421**, **1422** may be co-located within the same deployment **1420**, but separately implemented. As an example, a first PLMN may own and/or operate deployment **1420** having NFs **1421**, **1422**. As another example, the first PLMN may implement NF **1421** and a second PLMN may obtain from the first PLMN (e.g., rent, lease, procure, etc.) at least a portion of the capabilities of deployment **1420** (e.g., processing power, data storage, etc.) in order to implement NF **1422**. As yet another example, the deployment may be owned and/or operated by one or more third parties, and the first PLMN and/or second PLMN may procure respective portions of the capabilities of the deployment **1420**. When multiple NFs are provided at a single deployment, networks may operate with greater speed, coverage, security, and/or efficiency.

[0194] FIG. **14**C illustrates an example arrangement of core network deployments in which a single instance of an NF is implemented using a plurality of different deployments. In particular, a single instance of NF **1422** is implemented at deployments **1420**, **1440**. As an example, the functionality provided by NF **1422** may be implemented as a bundle or sequence of subservices. Each subservice may be implemented independently, for example, at a different deployment. Each subservices may be implemented in a different physical location. By distributing implementation of subservices of a single NF across different physical locations, the mobile communications network may operate with greater speed, coverage, security, and/or efficiency.

[0195] FIG. **14**D illustrates an example arrangement of core network deployments in which one or more network functions are implemented using a data processing service. In FIG. **14**D, NFs **1411**, **1411**A, **1421**, **1422** are included in a deployment **1450** that is implemented as a data processing service. The deployment **1450** may comprise, for example, a cloud network and/or data center. The deployment **1450** may be owned and/or operated by a PLMN or by a non-PLMN third party. The NFs **1411**, **1411**A, **1421**, **1422** that are implemented using the deployment **1450** may belong to the same PLMN or to different PLMNs. The PLMN(s) may obtain (e.g., rent, lease, procure, etc.) at least a portion of the capabilities of the deployment **1450** (e.g., processing power, data storage, etc.). By providing one or more NFs using a data processing service, the mobile communications network may operate with greater speed, coverage, security, and/or efficiency.

[0196] As shown in the figures, different network elements (e.g., NFs) may be located in different physical deployments, or co-located in a single physical deployment. It will be understood that in the present disclosure, the sending and receiving of messages among different network elements is not limited to inter-deployment transmission or intra-deployment transmission, unless explicitly indicated.

[0197] In an example, a deployment may be a ‘black box’ that is preconfigured with one or more NFs and preconfigured to communicate, in a prescribed manner, with other ‘black box’ deployments (e.g., via the interface **1490**). Additionally or alternatively, a deployment may be configured to operate in accordance with open-source instructions (e.g., software) designed to implement NFs and communicate with other deployments in a transparent manner. The deployment may operate in accordance with open RAN (ORAN) standards.

[0198] Deterministic Networking (DetNet) is an effort by the IETF DetNet Working Group to study implementation of deterministic data paths for real-time applications with extremely low data loss rates, packet delay variation (jitter), and bounded latency, such as audio and video streaming, industrial automation, and vehicle control. DetNet may operate at the IP Layer 3 routed segments using e.g., a Software-Defined Networking layer to provide IntServ and DiffServ integration, and may deliver service over lower Layer 2 bridged segments using technologies such as MPLS and IEEE 802.1 Time-Sensitive Networking (TSN). TSN is a set of IEEE standards to ensure low latency in Ethernet networks. The standard ensures that latency of a so-called “TSN flow” between two devices is always below a certain limit (e.g., 1 ms). Deterministic Networking aims to migrate time-critical, high-reliability industrial control and audio-video applications from special-purpose Fieldbus networks (such as HDMI, CAN bus, PROFIBUS, RS-485, RS-422/RS-232, and/or the like) to packet networks and the IP in particular. DetNet may support both the new applications and existing IT applications on the same physical network. To support real-time applications, DetNet may implement reservation of data plane resources in intermediate nodes along the data flow path, calculation of explicit routes that may or may not depend on network topology, and redistribute data packets over time and/or space to deliver data even with the loss of a path.

[0199] In an example, the 3GPP network may act as a TSN bridge e.g., layer 2 switching and/or bridging. In an example, the 3GPP system may be deployed to act as a DetNet node. A DetNet node may operate at layer 3. DetNet provides a capability for the delivery of data flows with extremely low packet loss rates and bounded end-to-end delivery latency. DetNet is for networks that are under a single administrative control or within a closed group of administrative control; these include campus-wide networks and private WANs.

[0200] The DetNet QoS can be expressed in terms of: [0201] Minimum and maximum end-to-end latency from source to destination, timely delivery, and bounded jitter (packet delay variation) derived from these constraints. [0202] Packet loss ratio under various assumptions as to the operational states of the nodes and links. [0203] An upper bound on out-of-order packet delivery. Some DetNet applications are unable to tolerate any out-of-order delivery.

[0204] It is a distinction of DetNet that it is concerned solely with worst-case values for the end-to-end latency, jitter, and misordering. Average, mean, or typical values are of little interest, because they do not affect the ability of a real-time system to perform its tasks. In general, a trivial priority-based queuing scheme may give better average latency to a data flow than DetNet; however, it may not be a suitable option for DetNet because of its worst-case latency.

[0205] Three techniques may be employed by DetNet to provide these qualities of service: Resource allocation, Service protection, and Explicit routes.

[0206] In an example, resource allocation may operate by assigning resources, e.g., buffer space or link bandwidth, to a DetNet flow (or flow aggregate) along its path. Resource allocation greatly reduces, or even eliminates entirely, packet loss due to output packet contention within the network, but it can only be supplied to a DetNet flow that is limited at the source to a maximum packet size and transmission rate. As DetNet flows are assumed to be rate limited and DetNet is designed to provide sufficient allocated resources (including provisioned capacity), the use of transport-layer congestion control for App-flows is not required; however, if resources are allocated appropriately, use of congestion control may not impact transmission negatively.

[0207] In an example, resource allocation may address two of the DetNet QoS requirements: latency and packet loss. Given that DetNet nodes have a finite amount of buffer space, resource allocation may result in a maximum end-to-end latency. Resource allocation also addresses contention-related packet loss. Other important contributions to packet loss may be random media errors and equipment failures. Service protection is the name for the mechanisms used by DetNet to address these losses. The mechanisms employed are constrained by the need to meet the users' latency requirements. Packet replication and elimination and packet encoding may provide service protection, but other mechanisms may also be found. For instance, packet encoding can be used to provide service protection against random media errors, while packet replication and elimination can be used to provide service protection against equipment failures. This mechanism distributes the contents of DetNet flows over multiple paths in time and/or space, so that the loss of some of the paths does need not cause the loss of any packets.

[0208] Standard IT infrastructure may not efficiently handle latency-sensitive data. Switches and routers use fundamentally uncertain algorithms for processing packet/frames, which may result in sporadic data flow. A solution for smoothing out these flows is to properly configure DetNet nodes, DetNet resources, and/or the like. DetNet may employ deterministic algorithms for queuing, shaping and scheduling which allow each node to allocate bandwidth and latency according to requirements of each data flow, by computing the buffer size at a DetNet node.

[0209] In an example embodiment, a 3GPP system/network may be configured to act as a DetNet node. As depicted in example FIG. **28**, a 3GPP or 5G system (5GS) may be a logical DetNet node. A UE may be configured to act as a device side of the DetNet node. The UE may be connected to or be integrated with a translator device/module (DS-T). A UPF may be configured to act as a network side of the DetNet node. The UPF may be connected to or be integrated with a translator device/module (NW-T).

[0210] The DetNet node or DetNet system may comprise a DetNet controller entity that may act as a DetNet Control Plane. The DetNet control plane may support the dynamic creation, modification, and deletion of DetNet flows. This may include some or all of explicit path determination, link bandwidth reservations, restricting flows to specific links (e.g., IEEE 802.1 Time-Sensitive Networking (TSN) links), node buffer and other resource reservations, specification of required queuing disciplines along the path, ability to manage bidirectional flows, and/or the like, as needed for a (DetNet) flow.

[0211] The DetNet control plane may support DetNet flow aggregation and de-aggregation via the ability to dynamically create and delete flow aggregates (FAs), and be able to modify existing FAs by adding or deleting participating flows. The DetNet control plane may allow flow instantiation requests to originate in an end application (via an Application Programming Interface (API), via static provisioning, or via a dynamic control plane, such as a centralized SDN controller or distributed signaling protocols. The DetNet control plane may support queue control techniques.

[0212] The DetNet control plane may support advertising static and dynamic node and link resources such as capabilities and adjacencies to other network nodes (for dynamic signaling approaches) or to network controllers (for centralized approaches). The DetNet control plane may support scaling to handle the number of DetNet flows expected in a domain (which may require per-flow signaling or provisioning). The DetNet control plane may support provision flow identification information at each of the nodes along the path. Flow identification may differ depending on the location in the network and the DetNet functionality (e.g. transit node vs. relay node).

[0213] The DetNet control plane may support monitoring the performance of DetNet flows and nodes to ensure that they are meeting required objectives, both proactively and on-demand. The

DetNet control plane may support DetNet flow continuity check and connectivity verification functions. The DetNet control plane may support testing and monitoring of packet replication, duplicate elimination, and packet ordering functionality in the DetNet domain.

[0214] The DetNet control plane may support adaptation to DetNet domain topology changes such as links or nodes failures (fault recovery/restoration), additions and removals.

[0215] In an example, a DetNet flow may be a sequence of packets that conforms uniquely to a flow identifier and to which the DetNet service is to be provided. It may comprise any DetNet headers added to support the DetNet service and forwarding sub-layers.

[0216] In an example, a DetNet service may comprise a DetNet service sub-layer. In an example, DetNet functionality may be divided into two sub-layers. One of them is the DetNet service sub-layer, at which a DetNet service (e.g., service protection) is provided. DetNet service proxy may be a proxy that maps between App-flows and DetNet flows.

[0217] In an example, some service protection mechanisms may rely on switching from one flow to another when a failure of a flow is detected.

[0218] In an example, packet replication and elimination combines the DetNet member flows sent along multiple different paths and performs a packet-by-packet selection of which to discard, e.g., based on sequencing information.

[0219] In an example embodiment, failure may occur due to signaling, user plane failure, medie failure, equipment fault/failure, path failure, and/or the like. In an example embodiment, if a DetNet flow passes through one or more DetNet-unaware network nodes between two DetNet nodes providing the DetNet forwarding sub-layer for that flow, there is a potential for disruption or failure of the DetNet QoS. In an example embodiment, failure may occur at an ingress or egress interface of a DetNet node or DetNet system. The egress and/or the ingress may be located at the network side such as the UPF. In an example, the egress/ingress may be located at the device side of the DetNet node. In an example, a failure may be defined by a failure code indicating the cause or location of a failure.

[0220] In an example, the failure may be related to DetNet flow. In an example, the failure code (FailureCode) may be a non-zero code that specifies the error if the DetNet flow encounters a failure (e.g., packet replication and elimination is requested but not possible, or DningressStatus is Failed, or DnEgressStatus is Failed, or DnEgressStatus is PartialFailed).

[0221] In an example, the failure may be related to DetNet service failure that may be reported by a code such as DetNet service failure code (DnServiceFailureCode). The DetNet service failure code may be a non-zero code that specifies the error if the DetNet service encounters a failure (e.g., packet replication and elimination is requested but not possible, or DnServiceIngressStatus is Failed, or DnServiceEgressStatus is Failed, or DnServiceEgressStatus is PartialFailed).

[0222] In an example, failures may cause degradation of QoS and service for the DetNet, may cause packet loss, link failures, and/or the like.

[0223] In an example, a DetNet parameter may comprise at least one of a 1) DetNet flow parameter (DetNet flow information element IE) that may comprise characteristics of data flows; 2) DetNet service parameter (DetNet service IE) that may comprise characteristics of services being provided for data flows over a network; 3) DetNet configuration parameter (DetNet configuration IE) that may comprise in detail the settings and parameters required on network nodes to provide a data flow proper service.

[0224] In an example, the DetNet flow IE and the DeNet service IE may comprise three groups of information elements: App-flow related parameters (these describe the App-flow characteristics (e.g., identification, encapsulation, traffic specification, endpoints, status, etc.) and the App-flow service expectations (e.g., delay, loss, etc.)), DetNet flow related parameters(these describe the DetNet flow characteristics (e.g., identification, format, traffic specification, endpoints, rank, etc.)), DetNet service related parameters: these describe the expected service characteristics (e.g., delivery type, connectivity delay/loss, status, rank, etc.).

[0225] In an example, App-flow characteristics may comprise: [0226] FlowID: a unique (management) identifier of the App-flow. It can be used to define the N:1 mapping of App-flows to a DetNet flow. [0227] FlowType: set by the encapsulation format of the flow. It may be Ethernet (TSN), MPLS, or IP. [0228] DataFlowSpecification: a flow descriptor, defining which packets belongs to a flow using, specific packet header fields such as src-addr, dst-addr, label, VLAN-ID, and/or the like. [0229] TrafficSpecification: a flow descriptor, defining traffic parameters such as packet size, transmission time interval, and maximum packets per time interval. [0230] FlowEndpoints: delineate the start and termination reference points of the App-flow by pointing to the source interface/node and destination interface(s)/node(s). [0231] FlowStatus: indicates the status of the App-flow with respect to the establishment of the flow by the connected network, e.g., ready, failed, etc. [0232] FlowRank: indicates the rank of this flow relative to other flows in the connected network.

[0233] In an example, the DetNet parameter may comprise the App-flow characteristics.

[0234] In an example, App-flow requirements may comprise: [0235] FlowRequirements: defines the attributes of the App-flow regarding bandwidth, latency, latency variation, loss, and misordering tolerance. [0236] FlowBiDir: defines the data path requirement of the App-flow whether it must share the same data path and physical path for both directions through the network, e.g., to provide congruent paths in the two directions.

[0237] In an example, the DetNet flow IE may comprise: DetNet flow identifier ID DnFlowID (A unique (management) identifier is needed for each DetNet flow within the DetNet domain. It is specified by DnFlowID. It can be used to define the many to one mapping of DetNet flows to a DetNet service), DnPayloadType (The DnPayloadType attribute may be set according to the encapsulated App-flow format. The attribute can be Ethernet, MPLS, or IP), DnFlowFormat, DnFlowSpecification, DnTrafficSpecification, DnFlowEndpoints, DnFlowRank, DnFlowStatus, DnFlowRequirements, DnFlowBiDir, and/or the like.

[0238] In an example, the DetNet flow ID may protocol specific identifiers such as addresses, labels (e.g., for MPLS), and/or the like. For example, DetNet IP flows may be identified and specified by the following attributes: [0239] a. SourcelpAddress [0240] b. DestinationlpAddress [0241] c. IPv6FlowLabel [0242] d. Dscp (attribute) [0243] e. Protocol [0244] f. SourcePort [0245] g. DestinationPort [0246] h. IPSecSpi

[0247] In an example, DetNet traffic specification may comprise the following attributes: [0248] a. Interval: the period of time in which the traffic specification is specified. [0249] b. MaxPacketsPerInterval: the maximum number of packets that the Ingress will transmit in one Interval. [0250] c. MaxPayloadSize: the maximum payload size that the Ingress will transmit.

[0251] In an example, the DnFlowEndpoints attribute defines the starting and termination reference points of the DetNet flow by pointing to the ingress interface/node and egress interface(s)/node(s). Depending on the network scenario it defines an interface or a node. Interface can be defined for example if the App-flow is a TSN Stream and it is received over a well defined UNI interface. For example, for App-flows with MPLS encapsulation defining an ingress node is more common when per platform label space is used.

[0252] In an example, rank of the DetNet Flow, the DnFlowRank attribute may provides the rank of this flow relative to other flows in the DetNet domain. Rank (range: 0-255) is used by the DetNet domain to decide which flows can and cannot exist when network resources reach their limit. Rank is used to help to determine which flows can be bumped (i.e., removed from node configuration thereby releasing its resources) if for example a port of a node becomes oversubscribed (e.g., due to network re-configuration).

[0253] In an example, status of the DetNet Flow, DnFlowStatus may provide/comprise the status of the DetNet flow with respect to the establishment of the flow by the DetNet domain.

[0254] The DnFlowStatus may comprise the following attributes: [0255] a. DningressStatus is an enumeration for the status of the flow's Ingress reference point: [0256] None: no Ingress. [0257]

Ready: Ingress is ready. [0258] Failed: Ingress failed. [0259] OutOfService: Administratively blocked. [0260] b. DnEgressStatus is an enumeration for the status of the flow's Egress reference points: [0261] None: no Egress. [0262] Ready: all Egresses are ready. [0263] PartialFailed: One or more Egress ready, and one or more Egress failed. The DetNet flow can be used if the Ingress is Ready. [0264] Failed: All Egresses failed. [0265] OutOfService: Administratively blocked. [0266] c. FailureCode: A non-zero code that specifies the error if the DetNet flow encounters a failure (e.g., packet replication and elimination is requested but not possible, or DningressStatus is Failed, or DnEgressStatus is Failed, or DnEgressStatus is PartialFailed).

[0267] In an example, requirements of the DetNet Flow, DnFlowRequirements may specify requirements to ensure the service level desired for the DetNet flow. The DnFlowRequirements may comprise the following attributes: [0268] a. MinBandwidth [0269] b. MaxLatency [0270] c. MaxLatencyVariation [0271] d. MaxLoss [0272] e. MaxConsecutiveLossTolerance [0273] f. MaxMisordering

[0274] In an example, DetNet Service Related Parameters may comprise: [0275] a. DnServiceID [0276] b. DnServiceDeliveryType [0277] c. DnServiceDeliveryProfile [0278] d. DNServiceConnectivity [0279] e. DnServiceBiDir [0280] f. DnServiceRank [0281] g. DnServiceStatus

[0282] In an example, status of the DetNet Service may comprise the following. DnServiceStatus information group includes elements that specify the status of the service specific state of the DetNet domain. This information group informs the user whether or not the service is ready for use. The DnServiceStatus may comprise the following attributes: [0283] a. DnServiceIngressStatus is an enumeration for the status of the service's Ingress: [0284] None: no Ingress. [0285] Ready: Ingress is ready. [0286] Failed: Ingress failed. [0287] OutOfService: Administratively blocked. [0288] b. DnServiceEgressStatus is an enumeration for the status of the service's Egress: [0289] None: no Egress. [0290] Ready: all Egresses are ready. [0291] PartialFailed: One or more Egress ready, and one or more Egress failed. The DetNet flow can be used if the Ingress is Ready. [0292] Failed: All Egresses failed. [0293] OutOfService: Administratively blocked. [0294] c. DnServiceFailureCode: A non-zero code that specifies the error if the DetNet service encounters a failure (e.g., packet replication and elimination is requested but not possible, or DnServiceIngressStatus is Failed, or DnServiceEgressStatus is Failed, or DnServiceEgressStatus is PartialFailed).

[0295] In an example, 3GPP system may be deployed to act as a DetNet node. In an example, stringent requirements of DetNet traffic requires configuration of DetNet node on a UPF to act as the network side of the DetNet node. The DetNet node granularity may be at a UPF level. In an example, existing technologies for the 3GPP systems do not support DetNet configuration. Existing technologies may not properly configure resources to support DetNet traffic requirements. TSN related configurations may not properly serve the purpose since TSN configuration operates at the layer 2 level for bridging and switching, while DetNet operates at the layer 3 level, and administration of DetNet node requires proper node configurations.

[0296] In an example, embodiments of the present disclosure improve the system performance and enables configuration of a 3GPP network to act as a DetNet node by enhancement of signalling between user plane nodes and control plane nodes. Signalling enhancements comprise node level signalling and session level signalling. Messages comprising DetNet parameters may be sent to and received from different user plane nodes and control plane nodes as further described herein.

[0297] FIG. **15** illustrates an example AF (DetNet controller entity) initiated DetNet configuration, or DetNet flow creation procedure in a network in accordance with embodiments of the present disclosure. In an example, the AF (DetNet controller entity) may send a request to reserve resources for an AF session using a Nnef_AFsessionWithQoS_Create request message. In an example, the message comprises: a DetNet parameter, a DetNet flow id, a DetNet flow assistance information, a DetNet management container, a DetNet node ID, UE address, AF Identifier, Flow description(s) or External Application Identifier, QoS reference, (optional) Alternative Service. In an example, a period of time or a traffic volume for the requested QoS can be included in the AF request. The AF may, instead of a QoS Reference, provide the following individual QoS parameters: Requested 5GS delay (optional), Requested Priority (optional), Requested GFBR, Requested MFBR, flow direction, Burst Size (optional), Burst Arrival Time (optional) at UE (uplink) or UPF (downlink), Periodicity (optional), Time domain (optional), Survival Time (optional).

[0298] In an example embodiment, the DetNet parameter may comprise the DetNet service related parameters, requirements of the DetNet Flow, DnFlowRequirements, an identifier of a DetNet node, and/or the like.

[0299] In an example embodiment the DetNet flow id may comprise IP or MPLS related addresses, and/or labels (e.g., endpoint identifiers, or the like).

[0300] In an example embodiment, the DetNet flow assistance information may comprise the DetNet flow requirements e.g., DnFlowRequirements.

[0301] In an example embodiment, the DetNet management container may comprise DetNet resource information container, DetNet flow parameter, DetNet service parameter, DetNet configuration parameter, and/or the like.

[0302] In an example, the NEF may assign a Transaction Reference ID to the Nnef_AFsessionWithQoS_Create request. The NEF may authorizes the AF request and may apply policies to control the overall amount of QoS authorized for the AF.

[0303] In an example, the NEF may interact with the PCF by triggering a Npcf_PolicyAuthorization_Create request and may provide at least one of the DetNet node ID, the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, UE address, AF Identifier, Flow description(s), the QoS Reference and the optional Alternative Service Requirements.

[0304] In an example, if the NEF receives any of the individual QoS parameters for a DetNet flow or DetNet node, from the AF, the NEF may forward these received individual QoS parameters in the Ntsctsf_QoSandTSCAssistance_Create request message to the TSCTSF. If the AF is considered to be trusted by the operator, the AF uses the Ntsctsf_QoSandTSCAssistance_Create request message to interact directly with TSCTSF to request reserving resources for an AF session. A TSCTSF address may be locally configured (e.g., per DetNet domain, a single TSCTSF per DNN/S-NSSAI, and/or the like) in the NEF, PCF and trusted AF. Alternatively, the TSCTSF may be discovered from the NRF. The TSCTSF may interacts with the PCF by triggering a Npcf_PolicyAuthorization_Update request and may provide at least one of the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, UE address, AF Identifier, Flow description(s), the QoS Reference, Individual QoS Parameters and the optional Alternative Service Requirements.

[0305] In an example, the TSCTSF may perform calculation of required DetNet resources based on an element of the DetNet parameter. If the TSCTSF receives a DetNet parameter, or a QoS parameter associated with a DetNet node or DetNet flow, the TSCTSF may calculate a Requested PDB by subtracting the UE-DS-T Residence Time, or DS-TT residence time, provided by the PCF (if available), from the Requested 5GS delay. In an example, the TSCTSF may determine or modify the DetNet assistance information, the DetNet management container, the DetNet parameter, and/or the like. If the TSCTSF receives any of the following individual QoS parameters: flow direction, Burst Arrival Time, Periodicity, Time domain, Survival Time from the NEF, then the TSCTSF determines the TSC Assistance Container and sends it together with the Requested PDB, the TSC Assistance Container, and other received individual QoS parameters in the Npcf_PolicyAuthorization_Update request to the PCF. In an example, the TSCTSF may discover the PCF in case the TSCTSF has not received any notification from PCF (e.g. no UE-DS-TT Residence time), TSCTSF sends the Requested PDB, the DetNEt assistance information, the

DetNet parameter, the DetNet management container, the TSC Assistance Container, and other received individual QoS and Alternative QoS Related parameters to the PCF.

[0306] In an example, if the PCF or TSCTSF authorize request from the NEF, the PCF or the TSCTSF may send a request to a SMF, or a UPF to configure the UPF. In an example, the NEF may send a configuration message to the UPF by employing UPF services such as Nupf messages.

[0307] In an example, if the PCF determines that the SMF needs updated policy information, the PCF may send/issue a Npcf_SMPolicyControl_UpdateNotify request with updated policy information about the PDU Session as described in the PCF initiated SM Policy Association Modification procedure. In an example, the PDU session may be a PDU session serving the DetNet flow, or serving the DetNet node.

[0308] If the request is authorized, the PCF derives the required QoS parameters based on the information provided by the TSCTSF and determines whether this QoS is allowed (according to the PCF configuration), and notifies the result to the TSCTSF. In addition, if the Alternative Service Requirements are provided, the PCF derives the Alternative QoS parameter set(s) from the one or more QoS reference parameters (if provided) contained in the Alternative Service Requirements in the same prioritized order.

[0309] If the PCF receives the individual QoS parameters instead of QoS Reference, the PCF sets the PDB and MDBV according to the received Requested PDB and Burst Size received from the TSCTSF. If the Requested PDB is not provided, the PCF determines the PDB that matches the QoS Reference. It also sets the GF BR and MFBR according to requested values sent by the TSCTSF. The PCF may use the Requested Priority from the AF to determine QoS Flow Priority.

[0310] The TSCTSF may send a Ntsctsf_QoSandTSCAssistance_Create response message (Transaction Reference ID, Result) to the NEF. Result indicates whether the request is granted or not. If the AF is considered to be trusted by the operator, the TSCTSF may send the Ntsctsf_QoSandTSCAssistance_Create response message directly to AF. In an example, the NEF may send a Nnef_AFsessionWithQoS_Create response message (Transaction Reference ID, Result) to the AF. Result indicates whether the request is granted or not.

[0311] The NEF may send a Npcf_PolicyAuthorization_Subscribe message to the PCF to subscribe to notifications of Resource allocation status and may subscribe to other events. The TSCTSF may send a Npcf_PolicyAuthorization_Subscribe message to the PCF to subscribe to notifications of Resource allocation status and may subscribe to other events. When the event condition is met, e.g. that the establishment of the transmission resources corresponding to the QoS update succeeded or failed, the PCF sends Npcf_PolicyAuthorization_Notify message to the NEF notifying about the event. If the AF is considered to be trusted by the operator, the PCF sends the Npcf_PolicyAuthorization_Notify message directly to AF. When the event condition is met, e.g. that the establishment of the transmission resources corresponding to the QoS update succeeded or failed, the PCF sends Npcf_PolicyAuthorization_Notify message to the TSCTSF notifying about the event. The TSCTSF sends Ntsctsf_QoSandTSCAssistance_Notify message with the event reported by the PCF to the NEF. If the AF is considered to be trusted by the operator, the TSCTSF sends the Ntsctsf_QoSandTSCAssistance_Notify message directly to AF. The NEF may send Nnef_AFsessionWithQoS_Notify message with the event reported by the PCF to the AF.

[0312] FIG. **16** illustrates an example user plane configuration procedure in a network in accordance with embodiments of the present disclosure. In an example embodiment, the SMF may receive a message from the PCF, NEF or from the TSCTSF, indicating a request for DetNet resources associated with a DetNet flow. In an example, the SMF may receive a policy update message. In an example, when the SMF receives the request the SMF may determine to configure the UPF for the DetNet node. In an example, the configuration may be at a session level. In an example, the configuration may be at a node level. In an example, the SMF may determine a PDU session that serves the DetNet node or the DetNet flow. In an example, the SMF may determine an N4 session associated with the PDU session. The SMF may send an N4 request to the UPF. In an example, the N4 request may be an N4 session modification request, N4 session establishment request, an PFCP session modification request, a PFCP session establishment request, and/or the like. In an example, the N4 request may be an N4 association request, a PFCP association request, and/or the like. In an example, the N4 request may comprise at least one of the DetNet node ID, the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, and/or the like. In an example the N4 request may comprise a packet detection rule (PDR). In an example, the PDR may comprise at least one of the DetNet node ID, the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, and/or the like

[0313] In an example embodiment, the UPF may send an N4 response to the SMF indicating acceptance or rejection of the N4 request.

[0314] FIG. **17** illustrates a user plane configuration procedure in a network in accordance with embodiments of the present disclosure. In an example, the NEF may configure the UPF for the DetNet flow or the DetNet node. In an example, the NEF may send a message to the UPF based on Nupf messages. In an example, the message maybe a configuration message. In an example, the configuration message may comprise at least one of the DetNet node ID, the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, and/or the like.

[0315] In an example embodiment, the UPF may send a message to the SMF indicating allocation of resources for the DetNet and successful allocation of the DetNet node ID. In an example the UPF may send a report message to the SMF that may comprise an association of the UPF ID and the DetNEt flow ID, or a mapping of the UPF ID with the DetNet flow ID. In an example embodiment, the report message may comprise an association/mapping between the N4 session ID (PDU session ID) and the DetNet flow, an association/mapping between the N4 session ID (PDU session ID) and the DetNet node ID, and/or the like.

[0316] In an example embodiment, the SMF may send a NAS message to a UE that is configured to act as the device side of the DetNet node serving the DetNet flow. In an example, the NAS message may be a configuration message.

[0317] FIG. **18** illustrates an example DetNet configuration procedure in a network in accordance with embodiments of the present disclosure. In an example, the SMF may receive a request for establishment of a DetNet flow, or creation/configuration of a DetNet node as per an example embodiment described above. In an example, the SMF may send an N4 request to the UPF indicating a request to allocate a DetNet node ID. In an example, the N4 request may be an N4 session modification/establishment request, a PFCP session modification/establishment message, and, or the like. In an example as depicted in FIG. **20**, the N4 request may be an N4 association request, a PFCP association request message, and, or the like. In an example, the UPF may allocate or determine a DetNet node ID. The UPF may send an N4 response to the SMF that may comprise the DetNet node ID. In an example, the UPF may send a message to the NEF wherein the message may comprise the DetNet node ID. In an example, the message may be an Nnef parameter provision create/update message. In an example, the NEF may send the provisioned parameters to the AF or the DetNet control entity. In an example, the NEF may send to the TSCTSF a message (e.g., Ntsctsf QoS update/create message) comprising the DetNet node ID.

[0318] FIG. **19** illustrates an example DetNet configuration procedure between the NEF and then UPF in a network in accordance with embodiments of the present disclosure. In an example, the NEF may receive a request for establishment of a DetNet flow, or creation/configuration of a DetNet node as per an example embodiment described above. In an example, the NEF may send a request to the UPF indicating a request to allocate a DetNet node ID. In an example, the UPF may allocate or determine a DetNet node ID. The UPF may send a response to the NEF that may comprise the DetNet node ID. In an example, the UPF may send a message to the NEF wherein the message may comprise the DetNet node ID. In an example, the message may be an Nnef parameter provision create/update message. In an example, the NEF may send the provisioned parameters to the AF or the DetNet control entity. In an example, the NEF may send to the TSCTSF a message (e.g., Ntsctsf QoS update/create message) comprising the DetNet node ID. In an example, the NEF may send the provisioned parameters to the SMF. In an example, the NEF may send to the TSCTSF a message (e.g., Ntsctsf QoS update/create message) comprising the DetNet node ID. In an example, the SMF may perform a PDU session modification procedure. In an example, the SMF may trigger a configuration update towards the UE.

[0319] FIG. **21** illustrates an example DetNet resource configuration procedure in a network in accordance with embodiments of the present disclosure. In an example embodiment, the TSCTSF may receive the message from the NEF (e.g., Ntsctsf message) wherein the NEF may receive a Nnef_AF session create request from the AF. In an example, the TSCTSF may receive at least one of the DetNet node ID, the DetNet parameter, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, and/or the like. In an example the TSCTSF may determine and calculate required resources for the DetNet node and/or the DetNet flow. In an example the TSCTSF may determine a DetNet resource information container. In an example the DetNet resource information container may comprise a buffer space (size), number of buffers, and/or the like. In an example, the DetNet resource information container may comprise an element of the DetNet configuration IE, the DetNet flow IE and the DeNet service IE, the DetNet traffic specification, the DnFlowRequirements, and/or the like. In an example, the DetNet resource information container may comprise 5GS parameters mapped from the DetNet flow.

[0320] In an example, mapping relationship between DetNet flow and 5GS parameters may be employed as follows:

[0321] The DetNet flow identifier may be the unique identification. It can be mapped to QFI under 5GS QoS framework.

[0322] The DetNet IP flow description may describes the characteristics of service; it can be mapped to Packet filter Set under 5GS QoS framework.

[0323] The traffic specification requirements of DetNet flow are specific service requirements for specific flows. It can be mapped to QoS profile under 5GS QoS framework. The specific mapping methods may be as follows: [0324] The minimum guaranteed bandwidth is mapped to GFBR in QoS profile; [0325] The maximum delay is mapped to 5QI-PDB in QoS profile; [0326] Expand the parameters of 5QI in QoS profile, the maximum delay variation range is mapped to 5QI-PDB Deterministic; [0327] The maximum packet loss is mapped to 5QI-Error Rate in QoS profile; [0328] Expand the parameters of 5QI in QoS profile, the maximum continuous packet loss is mapped to 5QI-Max Continuous Error; [0329] Expand the parameters of 5QI in QoS profile, the maximum disorder that can be tolerated is mapped to 5QI-Misordering.

[0330] In an example, the TSCTSF may send the DetNet resource information container to the SMF. In an example, the PCF may send the DetNet resource information container to the SMF. In an example, the SMF may configure the UPF to allocate resources for the DetNet node and/or the DetNet flow. In an example, the SMF may send an N4/PFCP session modification/establishment request to the UPF that may comprise the DetNet resource information container. In an example the SMF may employ node level signaling. In an example, the SMF may send an N4/PFCP association request message to the UPF that may comprise the DetNet resource information container. In an example, the UPF may send a response message to the SMF upon allocation of resources based on the DetNet resource information container.

[0331] In an example embodiment as depicted in FIG. **21**, the NEF may send a request to the UPF to configure and allocate the DetNet resources. In an example, the request from the NEF to the UPF may comprise the DetNet resource information container.

[0332] In an example, the SMF may receive a request for establishment of a DetNet flow, or creation/configuration of a DetNet node as per an example embodiment described above. In an example, the SMF may send an N4 request to the UPF indicating a request to allocate a DetNet node ID. In an example, the UPF may allocate or determine a DetNet node ID. The UPF may send an N4 response to the SMF that may comprise the DetNet node ID. In an example, the UPF may send a message to the NEF wherein the message may comprise the DetNet node ID. In an example, the message may be an Nnef parameter provision create/update message. In an example, the NEF may send the provisioned parameters to the AF or the DetNet control entity. In an example, the NEF may send to the TSCTSF a message (e.g., Ntsctsf QoS update/create message) comprising the DetNet node ID.

[0333] In an example, a session management function (SMF) may receive from a network function a first message comprising a deterministic network (DetNet) parameter. In an example, the SMF may send to a user plane function (UPF), a second message comprising the DetNet parameter.

[0334] In an example, the DetNet parameter may comprise at least one of: an identifier of a DetNet flow; an identifier of a DetNet node; a DetNet resource information container; number of buffers for the DetNet; a DetNet assistance information; a DetNet flow requirement IE; a DetNet service parameter IE; and/or the like. In an example, the network function may be a network exposure function (NEF), a policy and charging control function (PCF), a Time Sensitive Communication and Time Synchronization Function (TSCTSF), and/or the like. In an example, the second message may be an N4/PFCP session establishment request message, an N4/PFCP session modification request message, an N4/PFCP association request message, and/or the like. In an example, the SMF may determine that a policy and charging control PCC authorization for a DetNet flow is required. In an example, the SMF may send to a PCF a policy association establishment request message that may comprise the DetNet parameter, the DetNet flow ID, the DetNet node ID, and/or the like. The SMF may receive from the PCF, a response message (e.g., Npcf_SMPolicyControl_Create response message) comprising policy information for the DetNet flow. In an example, the SMF may receive the first message from a DetNet control entity via an NEF. In an example, the DetNet control entity may be an application function, an application server, a third party entity, an external network node, and/or the like. In an example, the SMF may determine a PDU session associated with the DetNet flow (ID). In an example, the SMF may determine an N4 session associated with the PDU session of the DetNet flow.

[0335] In an example, the second message may comprise a packet detection rule (PDR) comprising one or more parameters for detection of DetNet traffic. In an example, the one or more parameters may comprise an identifier of a DetNet flow, an App-flow parameter comprising a flow type (e.g., TSN, MPLS, IP, and/or the like), and a data flow specification parameter(source address, destination address, label, VLAN ID, and/or the like.), flow end points comprising start and termination reference points of the App-flow by pointing to the source interface/node and destination interface(s)/node(s), and/or the like.

[0336] In an example, the SMF may send to the UPF, a third message requesting an identifier of a DetNet node. The SMF may receive from the UPF a fourth message comprising the identifier of the DetNet assigned/allocated by the UPF.

[0337] In an example embodiment, a network exposure function (NEF) may receive from a network function a first message comprising a deterministic network (DetNet) parameter. The NEF may send to a user plane function (UPF), a second message comprising the DetNet parameter.

[0338] In an example, the DetNet parameter may comprise at least one of: an identifier of a DetNet flow; a DetNet resource information container; number of buffers for the DetNet; [0339] a DetNet assistance information; an identifier of a DetNet node; a DetNet flow requirement IE, a DetNet service parameter IE, and/or the like.

[0340] In an example, the network function may be an application function (AF), a policy and charging control function (PCF), a TSCTSF, and/or the like. In an example, the second message may be to configure the UPF for the DetNet node.

[0341] In an example, a session management function (SMF) may receive from a network function a first message comprising a deterministic network (DetNet) parameter. In an example, the SMF may send to a user plane function (UPF), a second message requesting an identifier of a DetNet node. The SMF may receive from the UPF a third message comprising the identifier of the DetNet assigned by the UPF. In an example, the SMF may send to a DetNet controller, a third message comprising the identifier of the DetNet node. In an example, the DetNet controller may be an application function (AF). In an example, the third message may be sent via an NEF.

[0342] In an example embodiment, a network exposure function (NEF) may receive from a network function a first message comprising a request to configure a deterministic network (DetNet) node. In an example, the NEF may send to a user plane function (UPF), a second message comprising the request. In an example, the NEF may receive from the UPF, a response message that may comprise the identifier of the DetNet node allocated/assigned by the UPF.

[0343] In an example embodiment, a user plane function (UPF) may receive from a network function a first message comprising a request to configure a deterministic network (DetNet) node. In an example, the UPF may determine/allocate an identifier of the DetNet node. In an example, the UPF may send to a DetNet controller, a second message comprising the identifier of the DetNet node. In an example, the NEF may receive from the UPF, a response message that may comprise the identifier of the DetNet node assigned/allocated by the UPF.

[0344] In an example, the DetNet controller may be an application function (AF). In an example, the response message may be sent via an NEF. In an example, the UPF may receive from a SMF an N4/PFCP association request message to configure the UPF for a DetNet service, a DetNet node, a DetNet flow, and/or the like. In an example, the UPF may send to a SMF an N4/PFCP association response message comprising the identifier of the DetNet node allocated by the UPF.

[0345] In an example, 3GPP system may be deployed to act as a DetNet node. In an example, failure and QoS degradation may cause packet loss and DetNet flow and service failures. Constant monitoring of a status of DetNet resources may cause additional signalling. In an example, the DetNet node may serve one or more DetNet flows or data packet transmission for DetNet applications. Addition of a DetNet flow may cause the system to fail as a result of overutilization. Existing technologies may not take into account the status of the DetNet resources when for example, a new flow is added. In existing technologies, when a SMF receives a request for a new PDU session that may be associated to a DetNet flow, the Status of user plane resources is not taken into consideration and the request may be accepted. Utilization of DetNet resources beyond a threshold may cause failures. For example, when the number of buffers available are below the required number of buffers requested by the DetNet control plane, packet loss may occur.

[0346] Embodiments of the present disclosure improves the system performance by configuration of monitoring of DetNet resources status when certain conditions are met. Embodiments of the present disclosure improves the system performance by configuration of reporting of DetNet resources status when certain conditions are met, hence reducing signaling overhead of reporting. Example embodiments enhance the signaling performance by utilizing the status report for the selection of UPFs, establishment of new PDU sessions, and/or the like. Example embodiments enhance the system performance by enhancement of signaling between the RAN node and the core network for configuration of reporting and reporting procedures.

[0347] FIG. **22** illustrates an example event reporting configuration procedure in a network in accordance with embodiments of the present disclosure. In an example, the AF (DetNet controller entity) may send a request to the network to configure reporting status of DetNet resources. The AF may send the request that may comprise Nnef_AFsessionWithQoS_Create request message. In an example, the message comprises a list of DetNet reporting events, a DetNet reporting configuration information, a DetNet flow id, a DetNet flow assistance information, a DetNet management container, a DetNet node ID, UE address, AF Identifier, Flow description(s) or External Application Identifier, QoS reference, (optional) Alternative Service. In an example, a period of time or a traffic volume for the requested QoS can be included in the AF request. In an example, the list of DetNet reporting events may be related to DetNet flow (e.g., DnFlowStatus), the DetNet service (e.g., DnServiceStatus), the DetNet node and/or the like. In an example, the AF may subscribe to one or more events such as status, failure, resource status, and/or the like. In an example, the list of DetNet reporting events may comprise the status, the failure, the resource status, and/or the like.

[0348] In an example embodiment, a report may comprise an event. In an example, the event may be a DetNet flow failure, a DetNet service failure, a DetNet node failure, a DetNet resource status update, a status of a DetNet resource, and/or the like.

[0349] In an example embodiment, the report may comprise the list of DetNet reporting events may be related to DetNet flow (e.g., DnFlowStatus), the DetNet service (e.g., DnServiceStatus), the DetNet node availability (status) and/or the like. In an example, the report may comprise an identifier of the DetNet flow associated with the report, an identifier of the DetNet service associated with the report an identifier of the DetNet node associated with the report, and/or the like.

[0350] In an example, the DetNet reporting configuration information may comprise a threshold for reporting a status or reporting an event. In an example, the DetNet reporting configuration information may comprise a condition for reporting a status or reporting an event. For example, the threshold or condition may indicate that if the utilization or occupation of a resource exceed a certain value, a report may be provided. For example, the condition or threshold may indicate that buffer space or utilization of a buffer at a node (e.g., RAN, UPF, UE, and/or the like) exceeds % 70, % 50 or another value, a report may be performed by the node. For example, the condition or threshold may indicate that if performance of a path is above/below a certain value or a within a range of values, a reporting may be performed. In an example, the performance may be delay, packet loss ratio, available bandwidth, jitter, and/or the like.

[0351] In an example, the NEF may forward/send the request to the PCF. In an example, the NEF may forward the request to the TSCTSF. In an example, the PCF, the TSCTSF, the NEF, and/or the like may send a request to the SMF. The request may comprise the list of DetNet reporting events, the DetNet reporting configuration information, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, the DetNet node ID, and/or the like.

[0352] In an example embodiment as depicted in FIG. **22**, the SMF, may send a request to the UPF. The request may comprise the list of DetNet reporting events, the DetNet reporting configuration information, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, the DetNet node ID, and/or the like.

[0353] In an example embodiment as depicted in FIG. **22**, the NEF, may send a request to the UPF. The request may comprise the list of DetNet reporting events, the DetNet reporting configuration information, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, the DetNet node ID, and/or the like.

[0354] In an example, the UPF may determine to report an event to the SMF. In an example, the UPF may determine to report the event to the NEF. In an example embodiment, the SMF may forward the report to the NEF. In an example, the NEF may receive the report from the SMF or the UPF and the NEF may send the report to the AF.

[0355] In an example, the determining may be based on an element of the DetNet reporting configuration information such as a condition or a threshold being met.

[0356] In an example, embodiment, the event may be a failure, a resource usage status, resource usage exceeding a threshold, buffer space reaching to full utilization, and/or the like. In an example, the event may be related to the DetNet flow, the DetNet service, an interface of the DetNet node on the UPF or the NW-T, and/or the like.

[0357] In an example, when the SMF receives the request the SMF may determine to configure the UPF for reporting the status of the DetNet node, the DetNet resources, the DetNet flow, the DetNet service, and/or the like. In an example, the configuration may be at a session level. In an example, the configuration may be at a node level. In an example, the SMF may determine a PDU session that serves the DetNet node or the DetNet flow. In an example, the SMF may determine an N4 session associated with the PDU session. The SMF may send an N4 request to the UPF. In an example, the N4 request may be an N4 session modification request, N4 session establishment request, an PFCP session modification request, a PFCP session establishment request, and/or the like. In an example, the N4 request may be an N4 association request, a PFCP association request, and/or the like. In an example embodiment, the UPF may send the report via an N4 response to the SMF.

[0358] In an example embodiment as depicted in FIG. **22**, the report may be utilized by the network to allocate resources, to determine whether to accept requests, and/or the like. For example, the SMF may receive from a wireless device via an AMF a request to modify or establish a PDU session for a DetNet flow. In an example, the SMF may determine to accept or reject the request based on an element of the report that may comprise the status of DetNet resources, the status of the DetNet service, available number of buffers, available user plane DetNet resources, status/performance of a path terminating at the UPF, and/or the like. In an example, embodiment the SMF may send an N4 request such as an N4 session establishment/modification request to the UPF that is associated with the DetNet node. In an example, the UPF may determine to accept or reject the N4 request based on the status of the DetNet resources, the status of the DetNet service, available number of buffers, available user plane DetNet resources, status/performance of a path terminating at the UPF, and/or the like.

[0359] FIG. **23** illustrates a reporting configuration procedure in a network in accordance with embodiments of the present disclosure. As per an example embodiment described in FIG. **23**, the SMF may receive the request to configure reporting of the status of the DetNet resources. In an example, the SMF may send an element of the request to the AMF. In an example, the message from the SMF to the AMF may indicate reporting configuration for a RAN node serving the DetNet node, the DetNet flow, the DetNet service, and/or the like. In an example, the message from the SMF to the AMF may comprise the list of DetNet reporting events, the DetNet reporting configuration information, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, the DetNet resource information container, the DetNet node ID, and/or the like.

[0360] In an example, the AMF may send an N2 request message to the RAN node wherein the N2 request message may comprise the list of DetNet reporting events, the DetNet reporting configuration information, the DetNet flow id, the DetNet flow assistance information, the DetNet management container, the DetNet resource information container, the DetNet node ID, and/or the like.

[0361] In an example, the RAN node may translate/map the DetNet resource information container to one or more parameters at the RAN node or a cell of the RAN node.

[0362] In an example embodiment, the RAN node may send a report to a network node such as the AMF, the UPF, the NEF, the TSCTSF, the PCF, and/or the like. In an example, the report from the RAN node may be performed via user plane. In an example, the report from the RAN node may be performed via the control plane.

[0363] In an example, the reporting via the user plane may comprise the following. In an example, the RAN node may determine to send a report wherein the determining may be based on an element of the DetNet reporting configuration information such as a condition or a threshold being met.

[0364] In an example, generic tunneling protocol GTP-U may define a set of messages between the two ends of the user plane of the interfaces Iu, Gn, Gp, S1-U, S11-U, S2a, S2b, S4, S5, S8, S12, X2, M1, Sn, Xn, N3, N9 and N19.

[0365] GTP-U messages may be sent across a GTP user plane tunnel. A GTP-U message may be either a signalling message across the user plane tunnel, or a G-PDU message.

[0366] GTP-U signalling messages are used for user plane path management, or for user plane tunnel management.

[0367] G-PDU is a vanilla user plane message, which carries the original packet (T-PDU). In G-PDU message, GTP-U header is followed by a T-PDU.

[0368] A T-PDU is an original packet, for example an IP datagram, Ethernet frame or unstructured PDU Data, from an UE, or from a network node in an external packet data network.

[0369] The complete range of message types defined for GTPv1 is defined in 3GPP TS 29.060. The table below includes those applicable to GTP user plane. The three columns to the right define which of the three protocols sharing the common header of GTPv1 (GTP-C, GTP-U or GTP′) might implement the specific message type.

TABLE-US-00001 Messages in GTP-U Message Type value (Decimal) MessageReference GTP-C GTP-U GTP′ 1 Echo Request X X x 2 Echo Response X X x 3-25 Reserved in 3GPP TS 32.295 and 3GPP TS 29.060 26 Error Indication X 27-30 Reserved in 3GPP TS 29.060 31 Supported Extension Headers Notification X X 32-252 Reserved in 3GPP TS 29.060 253 Tunnel Status X 254 End Marker X 255 G-PDU X

[0370] In an example, The Tunnel Status message may be a GTP-U entity, if it supports the message, may send one or more Tunnel Status message to the peer GTP-U entity to provide the status information related to the corresponding GTP-U tunnel in the sending GTP-U entity. Table below specifies the information element included in the Tunnel Status message.

[0371] If a Tunnel Status message is received with a TEID for which there is no context, or the message is not supported, then the receiver shall ignore this message. [0372] Information Elements in Tunnel Status message [0373] Information element Presence requirement [0374] GTP-U Tunnel Status Information Mandatory [0375] Private Extension Optional [0376] DetNet Buffer status

[0377] DetNet link/tunnel status

[0378] In an example, the GTP-U message may comprise a status of DetNet resources on the RAN node side or a terminating point of a tunnel serving the DetNet flow, the DetNet service, and/or the like. In an example, the GTP-U message may comprise the report. In an example the tunnel status IE may comprise the report. In an example, the GTP-U message may be sent from the RAN node to the UPF.

[0379] In an example, the UPF in response to receiving the report from the RAN node may send a message to the NEF, the message may comprise the report.

[0380] In an example, the UPF in response to receiving the report from the RAN node may send a message to the SMF, the message may comprise the report.

[0381] In an example, the reporting via the control plane may comprise the following. In an example, the RAN node may determine to send a report wherein the determining may be based on an element of the DetNet reporting configuration information such as a condition or a threshold being met.

[0382] In an example, the RAN node (e.g., NG-RAN node) may send a message to the AMF via N2 interface. The message may comprise the following.

[0383] NR Composite Available Capacity Group: This IE indicates the overall available resource level per cell and per SSB area in the cell in downlink and uplink. [0384] IE/Group Name Presence Range Semantics description [0385] Composite Available Capacity Downlink M For the downlink

[0386] Composite Available Capacity Uplink M For the uplink

[0387] NR Composite Available Capacity: This IE indicates the overall available resource level in the cell in either downlink or uplink. [0388] IE/Group Name Presence Range Semantics description

[0389] NR Cell Capacity Class Value O

[0390] NR Capacity Value M ‘0’ indicates no resource is available, measured on a linear scale.

[0391] NR Cell Capacity Class Value: This IE indicates the value that classifies the cell capacity with regards to the other cells. This IE only indicates resources that are configured for traffic purposes.

[0392] IE/Group Name Presence Range IE type and reference Semantics description

[0393] NR Capacity Class Value M INTEGER (1 . . . 100, . . .) Value 1 indicates the minimum cell capacity, and 100 indicates the maximum cell capacity. There should be a linear relation between cell capacity and Cell Capacity Class Value.

[0394] NR Capacity Value: This IE indicates the amount of resources per cell and per SSB area that are available relative to the total NG-RAN resources. The capacity value should be measured and reported so that the minimum NG-RAN resource usage of existing services is reserved according to implementation. This IE can be weighted according to the ratio of cell capacity class values, if available.

[0395] IE/Group Name Presence Range IE type and reference Semantics description

[0396] NR Capacity Value M INTEGER (0 . . . 100) Value 0 indicates no available capacity, and 100 indicates maximum available capacity with respect to the whole cell. Capacity Value should be measured on a linear scale.

[0397] In an example embodiment, at least one of the elements of the message from the RAN node to the AMF may comprise the report (e.g., status of DetNet resources). In an example embodiment, the report may comprise the event. In an example, the event may be a DetNet flow failure, a DetNet service failure, a DetNet node failure, a DetNet resource status update, a status of a DetNet resource, and/or the like. In an example embodiment, the report may comprise a status of buffers allocated for the DetNet.

[0398] FIG. **24** illustrates a reporting configuration procedure in a network in accordance with embodiments of the present disclosure. In an example embodiment, the report message may be sent from the RAN node (NG-RAN) to the NEF. In an example embodiment, the report message may be sent from the RAN node (NG-RAN) to the TSCTSF. In an example embodiment, the report message may comprise the event. In an example, the event may be a DetNet flow failure, a DetNet service failure, a DetNet node failure, a DetNet resource status update, a status of a DetNet resource, and/or the like. In an example embodiment, the report may comprise a status of buffers allocated for the DetNet.

[0399] FIG. **25** illustrates a reporting configuration procedure in a network in accordance with embodiments of the present disclosure. In an example, during a PDU session establishment or modification procedure, or a service request procedure, the SMF may select a UPF. In an example, the selection may be based on an element of a NAS message received from the UE. In an example, the NAS message may comprise the DetNEt flow ID, the DetNet node ID, and/or the like. In an example, the SMF may select a UPF for the DetNet flow or based on the DetNet node ID received from the UE. In an example, the UPF may send the DetNet resource status or the report to the SMF. In an example, the SMF may employ the report received from the UPF to determine whether to select the UPF or allocate a new UPF or more user plane resources for the DetNet flow.

[0400] In an example, the UPF may send the report to the NRF based on the conditions determined by an element of the DetNet reporting configuration information. The NRF may utilize an element of the report to select a network function such as the UPF.

[0401] In an example, as depicted in FIG. **26**, the SMF may utilize an NRF to select the UPF. In an example, the SMF may select a user plane function (UPF) by utilizing the NRF and based on a parameter of the report, a DetNet parameter, and/or the like. The SMF may select the UPF based on a DetNet capability, DetNet flow requirement, one or more elements of the DetNet resource information container, required buffer space (or number of buffers), DetNet capability support, and/or the like. The SMF may query a network repository function (NRF) to select the UPF. The SMF may employ a Nnrf_NFDiscovery service, Nnrf_NFDiscovery_Request service operation, and/or the like of the NRF. The SMF may send a discovery request message (e.g., Nnrf_NFDiscovery_Request message, Nnrf_discovery_request message, and/or the like) comprising the a NF type (e.g., UPF), DetNet capability, DetNet flow requirement, one or more elements of the DetNet resource information container, required buffer space (or number of buffers), DetNet capability support, TSN capability support, and/or the like to the NRF indicating a request to select/discover a UPF for the DetNet flow or DetNet node. The NRF may send a query response (e.g., Nnrf_NFdiscovery_response, and/or the like) message comprising an identifier of the UPF, an address of the UPF, and/or the like.

[0402] In an example, as depicted in FIG. **27**, the SMF may add a new UPF to the DetNet node in response to receiving the report from the UPF. In an example, the SMF may reallocate the existing UPF based on the report. For example, the report may indicate that the DetNet resources have reached a utilization that may not be able to support the DetNet requirements.

[0403] In an example, the AF may determine that DetNet resources are not sufficient. In an example, the determining may be based on an element of the report. The AF may send a request to the network via the NEF to allocate more DetNet resources. The NEF may send a request to the SMF to allocate, reallocate or add new UPF.

[0404] In an example embodiment, a SMF may receive from a network node, a first request message to configure reporting a status of DetNet resources. In an example, the first request message may comprise: a list of reporting events, a threshold value for triggering a status report, determining, by the SMF a reporting event based on the list of reporting events, In an example, the SMF may send to a UPF a second request message comprising: the reporting event (an event to be reported), a threshold value (condition) associated with the reporting event. In an example, the SMF may receive from the UPF, a report message comprising at least one of: a report (e.g., the report as described in example embodiments), and the status of DetNet resources.

[0405] In an example, the list of reporting events may comprise a status of buffer (utilization), number of buffers available, a status of a DetNet flow, a status of a DetNet service, a status of DetNet ingress, a status of DetNet egress, and/or the like. In an example, the first request message may comprise a condition for reporting the status of DetNet resources. In an example, the SMF may receive from a wireless device a request (for establishment or modification) of a PDU session. In an example, the SMF may determine based on the status of DetNet resources whether to accept or reject the request for the PDU session. In an example, the SMF may send to the wireless device a response message indicating acceptance or rejection of the request for the PDU session. In an example, the response message may be a NAS message that may comprise a rejection cause. In an example, the rejection cause may indicate the reason for rejection being insufficient DetNet resources. In an example, the PDU session may be for the DetNet flow. In an example, the SMF may receive from the wireless device a request for a PDU session. The SMF may send to the UPF, an N4 session (establishment/modification) request message. The SMF may receive from the UPF an N4 session response indicating rejection or acceptance of the N4 session request. In an example, the SMF may send to the wireless device a response message indicating acceptance or rejection of the request for the PDU session. In an example, the UPF may determine based on the status of DetNet resources whether to accept or reject the request for the N4 session.

[0406] In an example, the SMF may select a UPF for a PDU session of a DetNet, wherein the selection is based on the status of the DetNet resources. In an example, the SMF may send to an NRF, a query message to discover/select a UPF for a DetNet flow, the query message comprising: an identifier of the DetNet flow, an identifier of the DetNet node, DetNet flow requirement IE, a DetNet resource information container, and/or the like. In an example, SMF may receive from the NRF an identifier of the UPF associated with the DetNet node, the DetNet flow, the DetNet service, and/or the like.

[0407] In an example, the SMF may determine to reallocate the UPF based on an element of the report (e.g., status of DetNet resources). In an example, the SMF may send to the DetNet control entity (the AF), the report. In an example, the DetNet control entity may send a request for reallocation of the UPF associated with the DetNet Node to allocate more resources for the DetNet flow, the DetNet service, and/or the like. In an example, the SMF may send to the DetNet control entity (the AF), the report. The DetNet control entity may send a request to add a new UPF for the DetNet node.

[0408] In an example, the first message may be to configure for monitoring of the DetNet resource status. The first message may be to configure the UPF for reporting of the DetNet resources status information.

[0409] In an example embodiment, a UPF may receive from a SMF, a first request message to configure reporting a status of DetNet resources, the first request message comprising: a list of reporting events, a threshold value for triggering a status report, and/or the like. In an example, the UPF may determine to report an event based on an element of the first request message. In an example, the UPF may send to a network node, a report message comprising the report, the status of DetNet resources, and/or the like.

[0410] In an example, the first request message may comprise a condition for reporting the status of DetNet resources. In an example, the network node may be at least one of: a network exposure function (NEF), an application function (AF), a network repository function (NRF), a Time Sensitive communication Time Synchronization function (TSCTSF), a SMF, and/or the like.

[0411] In an example, the UPF may receive from the SMF, an N4 session (establishment/modification) request. The UPF may send to the SMF an N4 session response indicating rejection or acceptance of the N4 session request. In an example, the UPF may determine based on the status of DetNet resources whether to accept or reject the request for the N4 session.

[0412] In an example, the UPF may receive from a base station, a status of DetNet resources for the RAN node. In an example, the UPF may send to an AF via an NEF, the status of DetNet resources for the RAN node.

[0413] In an example, a base station may receive from a first network node, a first request message to: configure reporting a status of DetNet resources, and to configure monitoring of the DetNet resources. In an example, the first request message may comprise a list of reporting events, a threshold value for triggering a status report, and/or the like. In an example, the base station may determine to report an event based on an element of the first request message. In an example, the base station may send to a second network node, a report message comprising: the report, the status of DetNet resources, and/or the like.

[0414] In an example, the first request message may comprise a condition for reporting the status of DetNet resources. In an example, the first network node may be at least one of: an access and mobility management function (AMF), a session management function (SMF), a UPF, a TSCTSF, and/or the like. In an example, the second network node may be at least one of: an access and mobility management function (AMF), a session management function (SMF), a NEF, a UPF, a TSCTSF, and/or the like.

Claims

1. A method comprising: sending, by a session management function (SMF) of a deterministic network (DetNet) node to a policy and charging control function (PCF), a request message comprising one or more parameters, the one or more parameters comprising interface information indicating a status associated with an interface of the DetNet node; and receiving, by the SMF from the PCF, policy information for a protocol data unit (PDU) session associated with the DetNet node.

2. The method of claim 1, further comprising receiving, by the SMF from a user plane function (UPF) of the DetNet node, a parameter identifying the DetNet node.

3. The method of claim 2, wherein the one or more parameters comprise the parameter identifying the DetNet node.

4. The method of claim 1, wherein the one or more parameters comprise at least one of: an identifier of a DetNet flow of the DetNet node; a DetNet resource information container; a number of buffers for the DetNet; a DetNet assistance information; a DetNet flow requirement information element (IE); or a DetNet service parameter IE.

5. The method of claim 1, further comprising sending, by the SMF to a user plane function (UPF) of the DetNet node, a second message indicating that the UPF operates as a network side of the DetNet node.

6. The method of claim 5, further comprising receiving, by the SMF from the UPF, a confirmation message indicating that user plane resources of the UPF are configured for the DetNet flow.

7. The method of claim 1, further comprising determining by the SMF that a policy and charging control PCC authorization for a DetNet flow is required.

8. A method comprising: receiving, by a policy and charging control function (PCF) from a session management function (SMF) of a deterministic network (DetNet) node, a request message comprising one or more parameters, the one or more parameters comprising interface information indicating a status associated with an interface of the DetNet node and sending, by the PCF to the SMF and in response to receiving the request message, policy information for a protocol data unit (PDU) session associated with the DetNet node.

9. The method of claim 8, wherein the one or more parameters comprise a parameter identifying the DetNet node.

10. The method of claim 9, wherein the parameter identifying the DetNet node is received by the SMF from a user plane function (UPF) of the DetNet node.

11. The method of claim 10, wherein the SMF sends, to a user plane function (UPF) of the DetNet node, a second message indicating that the UPF operates as a network side of the DetNet node.

12. The method of claim 8, wherein the one or more parameters comprise at least one of: an identifier of a DetNet flow of the DetNet node; a DetNet resource information container; a number of buffers for the DetNet; a DetNet assistance information; a DetNet flow requirement information element (IE); or a DetNet service parameter IE.

13. The method of claim 8, wherein the PCF receives the one of more DetNet parameters from the SMF in a policy association establishment request message.

14. The method of claim 8, wherein the policy information comprises updated policy information.

15. A policy and charging control function (PCF) comprising one or more processors and memory storing instructions that, when executed by the one or more processors, cause the PCF to: receive, from a session management function (SMF) of a deterministic network (DetNet) node, a request message comprising one or more parameters, the one or more parameters comprising interface information indicating a status associated with an interface of the DetNet node; and send, to the SMF and in response to receiving the request message, policy information for a protocol data unit (PDU) session associated with the DetNet node.

16. The PCF of claim 15, wherein the one or more parameters comprise a parameter identifying the DetNet node.

17. The PCF of claim 16, wherein the parameter identifying the DetNet node is received by the SMF from a user plane function (UPF) of the DetNet node.

18. The PCF of claim 15, wherein the one or more parameters comprise at least one of: an identifier of a DetNet flow of the DetNet node; a DetNet resource information container; a number of buffers for the DetNet; a DetNet assistance information; a DetNet flow requirement information element (IE); or a DetNet service parameter IE.

19. The PCF of claim 15, wherein the PCF receives the one of more DetNet parameters from the SMF in a policy association establishment request message.

20. The PCF of claim 15, wherein the policy information comprises updated policy information.