SFC WG
Internet-Draft
Intended status: Experimental
Expires: March 5, 2021

CJ. Bernardos
UC3M
A. Mourad
InterDigital

September 1, 2020

SFC function mobility with Mobile IPv6
draft-bernardos-dmm-sfc-mobility-01

Abstract

Service function chaining (SFC) allows the instantiation of an ordered set of service functions and subsequent "steering" of traffic through them. In order to set up and maintain SFC instances, a control plane is required, which typically is centralized. In certain environments, such as fog computing ones, such centralized control might not be feasible, calling for distributed SFC control solutions. This document specifies Mobile IPv6 extensions to enable function migration in SFC.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 5, 2021.

Table of Contents

1. Introduction

Virtualization of functions provides operators with tools to deploy new services much faster, as compared to the traditional use of monolithic and tightly integrated dedicated machinery. As a natural next step, mobile network operators need to re-think how to evolve their existing network infrastructures and how to deploy new ones to address the challenges posed by the increasing customers' demands, as well as by the huge competition among operators. All these changes are triggering the need for a modification in the way operators and infrastructure providers operate their networks, as they need to significantly reduce the costs incurred in deploying a new service and operating it. Some of the mechanisms that are being considered and already adopted by operators include: sharing of network infrastructure to reduce costs, virtualization of core servers running in data centers as a way of supporting their load-aware elastic dimensioning, and dynamic energy policies to reduce the monthly electricity bill. However, this has proved to be tough to put in practice, and not enough. Indeed, it is not easy to deploy new mechanisms in a running operational network due to the high dependency on proprietary (and sometime obscure) protocols and interfaces, which are complex to manage and often require configuring multiple devices in a decentralized way.

Service Functions are widely deployed and essential in many networks. These Service Functions provide a range of features such as security, WAN acceleration, and server load balancing. Service Functions may be instantiated at different points in the network infrastructure such as data center, the WAN, the RAN, and even on mobile nodes.

Service functions (SFs), also referred to as VNFs, or just functions, are hosted on compute, storage and networking resources. The hosting environment of a function is called Service Function Provider or NFVI-PoP (using ETSI NFV terminology).

Services are typically formed as a composition of SFs (VNFs), with each SF providing a specific function of the whole service. Services also referred to as Network Services (NS), according to ETSI terminology.

With the arrival of virtualization, the deployment model for service function is evolving to one where the traffic is steered through the functions wherever they are deployed (functions do not need to be deployed in the traffic path anymore). For a given service, the abstracted view of the required service functions and the order in which they are to be applied is called a Service Function Chain (SFC). An SFC is instantiated through selection of specific service function instances on specific network nodes to form a service graph: this is called a Service Function Path (SFP). The service functions may be applied at any layer within the network protocol stack (network layer, transport layer, application layer, etc.).

The concept of fog computing has emerged driven by the Internet of Things (IoT) due to the need of handling the data generated from the end-user devices. The term fog is referred to any networked computational resource in the continuum between things and cloud. A fog node may therefore be an infrastructure network node such as an eNodeB or gNodeB, an edge server, a customer premises equipment (CPE), or even a user equipment (UE) terminal node such as a laptop, a smartphone, or a computing unit on-board a vehicle, robot or drone.

In fog computing, the functions composing an SFC are hosted on resources that are inherently heterogeneous, volatile and mobile [I-D.bernardos-sfc-fog-ran]. This means that resources might appear and disappear, and the connectivity characteristics between these resources may also change dynamically. These scenarios call for distributed SFC control solutions, where there are SFC pseudo controllers, enabling autonomous SFC self-orchestration capabilities. The concept of SFC pseudo controller (P-CTRL) is described in [I-D.bernardos-sfc-distributed-control], as well different procedures for their discovery and initialization.

This document specifies Mobile IPv6 extensions to enable function migration in SFC.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The following terms used in this document are defined by the IETF in [RFC7665]:

Service Function (SF): a function that is responsible for specific treatment of received packets (e.g., firewall, load balancer).

Service Function Chain (SFC): for a given service, the abstracted view of the required service functions and the order in which they are to be applied. This is somehow equivalent to the Network Function Forwarding Graph (NF-FG) at ETSI.

Service Function Forwarder (SFF): A service function forwarder is responsible for forwarding traffic to one or more connected service functions according to information carried in the SFC encapsulation, as well as handling traffic coming back from the SF.

SFI: SF instance.

Service Function Path (SFP): the selection of specific service function instances on specific network nodes to form a service graph through which an SFC is instantiated.

The following terms are used in this document:

SFC Pseudo Controller (P-CTRL): logical entity [I-D.bernardos-sfc-distributed-control], complementing the SFC controller/orchestrator found in current architectures and deployments. It is service specific, meaning that it is defined and meaningful in the context of a given network service. Compared to existing SFC controllers/orchestrators, which manage multiple SFCs instantiated over a common infrastructure, pseudo controllers are constrained to service specific lifecycle management.

SFC Central Controller (C-CTRL): central control plane logical entity in charge of configuring and managing the SFC components [RFC7665].

3. Function mobility signaling extending Mobile IPv6

This section describes Mobile IPv6 (MIPv6) extensions to perform function migration/mobility. This is an example of NS lifecycle management operation: the update of the location of a given function. We refer to this as function mobility, though it might involve or not the actual migration of the function.

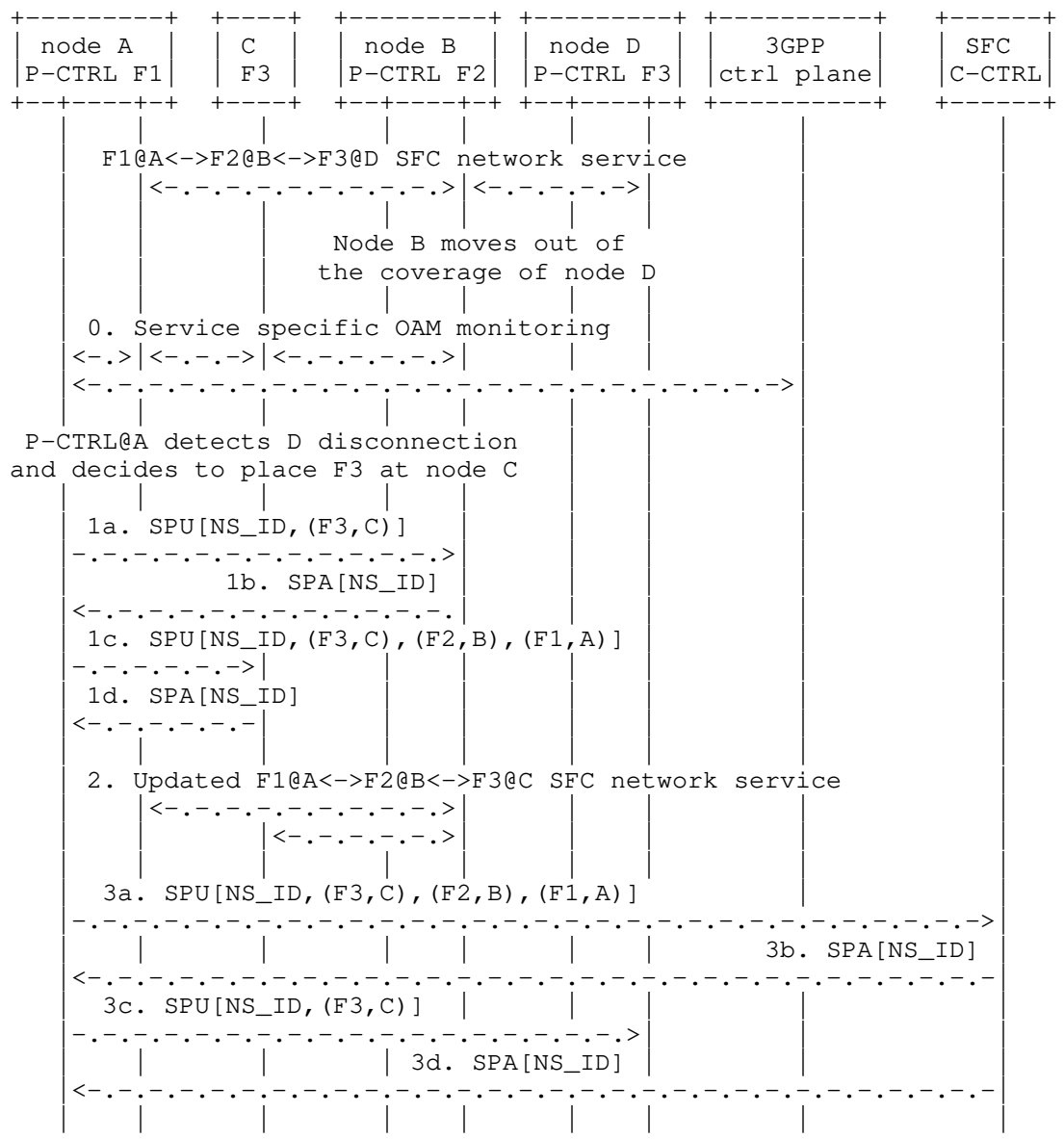


Figure 1: SFC mobility signaling

We next describe the signaling extensions with an example. For the sake of this example we assume that the function which location is updated is already available at the new target node (if not, it has to be previously migrated using any of the solutions available in the state-of-the-art). The different steps are described next:

- (The network service F1--F2--F3 is already instantiated and running. The only SFC P-CTRL active at this point is running at node A, and there is a candidate one at node B.)
- UE node B is moving out of the coverage of gNB node D.

1. This movement is detected by the active (designated) pseudo controller running at node A, thanks to local (service specific OAM) monitoring.
2. The active pseudo controller sends mobility signaling to all affected nodes, in this case node B (it has to update the network service path due to the F3 location update) and node C (as it starts being part of the SFC, hosting F3). The signaling messages are new mobility messages: Service Path Update (SPU) and Service Path Acknowledgement (SPA), which contain: (i) the identifier of the network service (NS_ID), and (ii) the updated elements of the network service path: (ID, updated location). The SPA acknowledges that the procedure has been performed correctly.
3. The network service F1--F2--F3 is updated so it now runs at A, B and C.
4. Whenever connectivity with nodes D and the centralized SFC controller is back, the pseudo controller also informs about the updated SFC path, sending SPU messages, which are acknowledged with SPA messages.

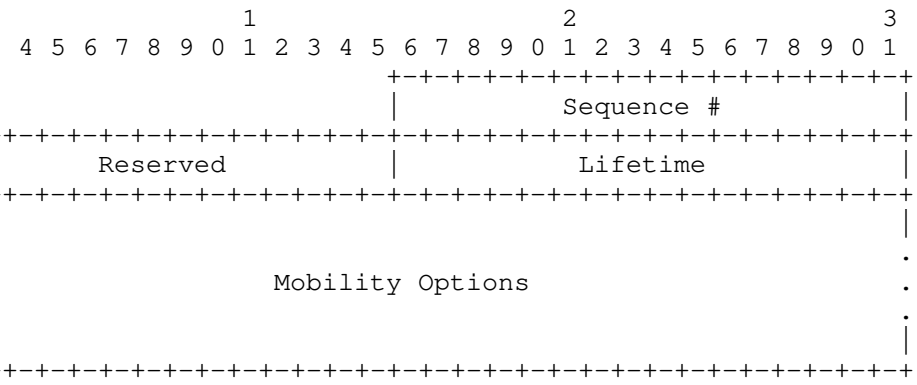
Note that this is an example of NS lifecycle management (function mobility) by a SFC pseudo controller, but that other operations are also possible, such as (non-limiting examples): scaling up/down, scaling in/out, termination, etc.

4. Mobile IPv6 extensions for SFC function mobility

4.1. Service Path Update

The Service Path Update (SPU) message is used by a CTRL to notify nodes in an SFC (e.g., SFF) of an update of the service path.

The Service Path Update uses the MH Type value TBD. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Sequence #

A 16-bit unsigned integer used by the receiving node to sequence Binding Updates and by the sending node to match a returned Service Path Acknowledgement with this Service Path Update.

Acknowledge (A)

The Acknowledge (A) bit is set by the sending mobile node to request a Service Path Acknowledgement be returned upon receipt of the Service Path Update.

Reserved

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Lifetime

16-bit unsigned integer. The number of time units remaining before the service path MUST be considered expired. A value of zero indicates that the Service Path MUST be deleted. A value of 0xFFFF indicates an infinite lifetime for the Service Path. One time unit is 4 seconds.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options that it does not understand.

The following options are valid in a Service Path Update:

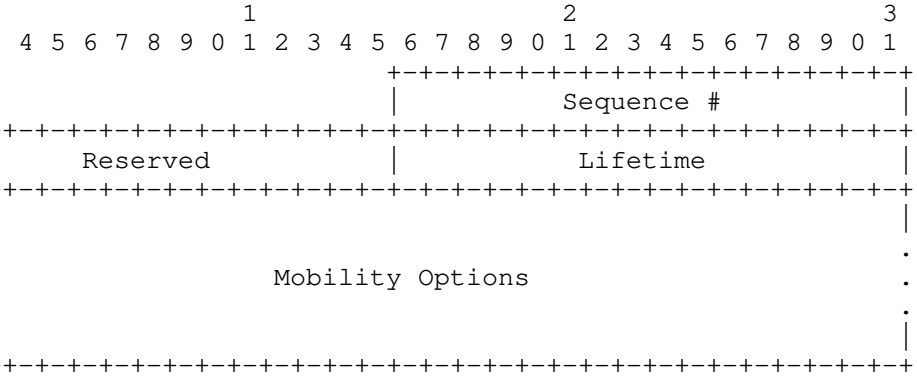
Network Service ID.

SFC node.

4.2. Service Path Acknowledgement

The Service Path Acknowledgement (SPA) message is used by a CTRL to acknowledge a received SPU.

The Service Path Acknowledge uses the MH Type value TBD. When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Sequence #

A 16-bit unsigned integer used to match the returned Service Path Acknowledgement with the Service Path Update.

Reserved

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Lifetime

16-bit unsigned integer. The number of time units remaining before the service path MUST be considered expired. A value of zero indicates that the Service Path MUST be deleted. A value of 0xFFFF indicates an infinite lifetime for the Service Path. One time unit is 4 seconds.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options that it does not understand.

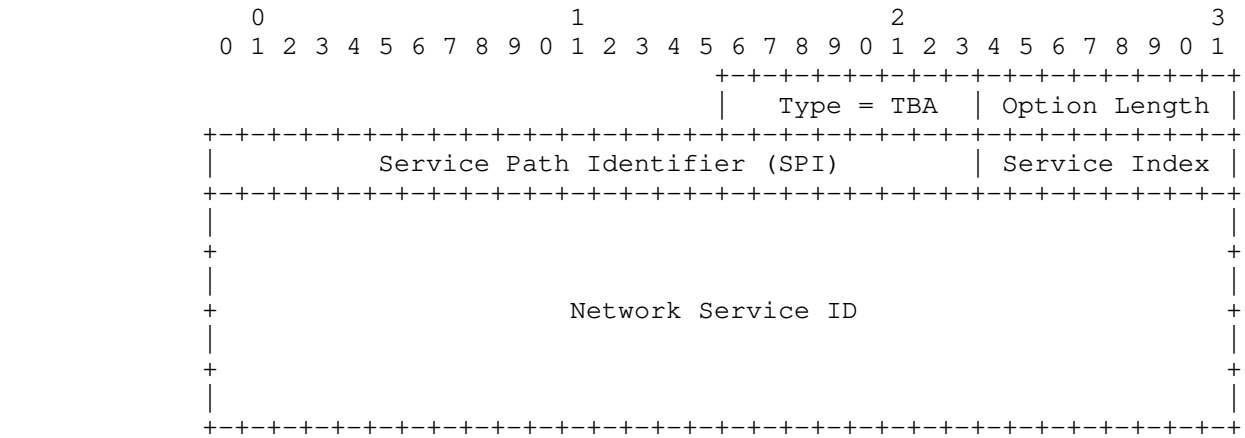
The following options are valid in a Service Path Acknowledgement:

Network Service ID.

4.3. New Mobility options

4.3.1. Network Service ID

The Network Service ID option has the following format:



Option Type

TBA by IANA.

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields.

Service Path Identifier (SPI)

Uniquely identifies a Service Function Path (SFP). Participating nodes MUST use this identifier for SFP selection. The initial Classifier MUST set the appropriate SPI for a given classification result.

Service Index (SI)

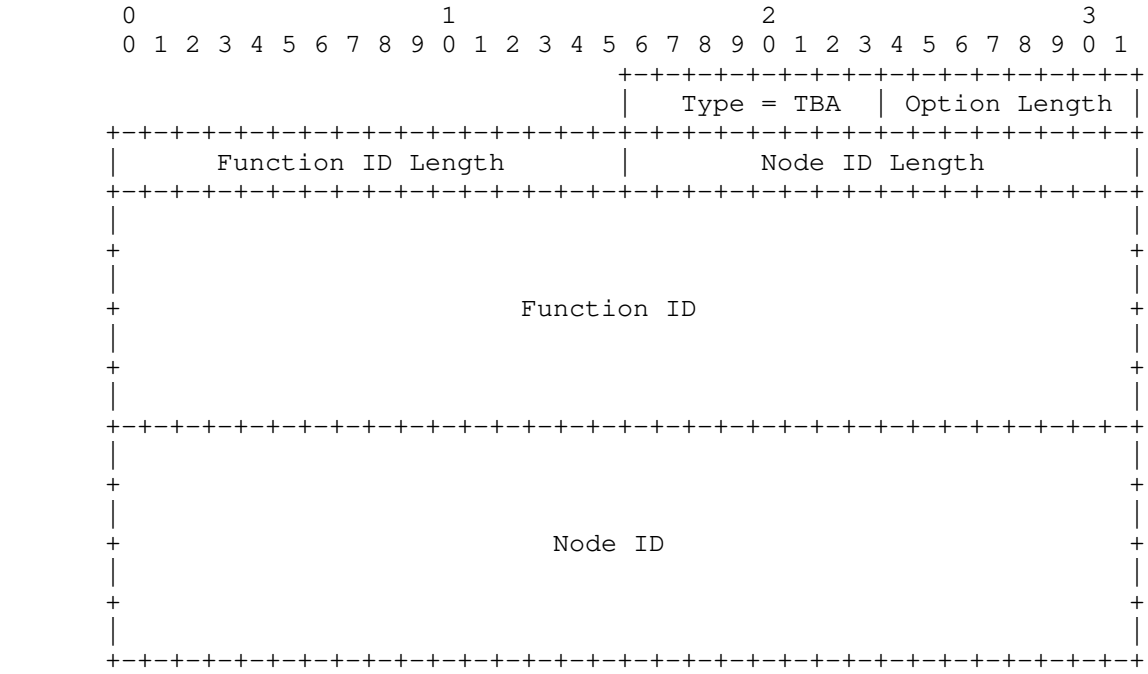
Provides location within the SFP.

Network Service ID

Variable length field that identifies the network service.

4.3.2. SFC node

The SFC node option has the following format:



Option Type

TBA by IANA.

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields.

Function ID Length

8-bit unsigned integer. Length of the Function ID field, in octets.

Node ID Length

8-bit unsigned integer. Length of the Node ID field, in octets.

Function ID

Variable length field that identifies the function.

Node ID

Variable length field that identifies the node.

There might be multiple SFC node options in a Service Function Update message, following the options the same order of the SFC/NS.

5. IANA Considerations

TBD.

6. Security Considerations

TBD.

7. Acknowledgments

The work in this draft has been partially supported by the H2020 5Growth (Grant 856709) and 5G-DIVE projects (Grant 859881).

8. References

8.1. Normative References

[I-D.bernardos-sfc-distributed-control]
Bernardos, C. and A. Mourad, "Distributed SFC control for fog environments", draft-bernardos-sfc-distributed-control-02 (work in progress), July 2020.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

8.2. Informative References

[I-D.bernardos-sfc-fog-ran]
Bernardos, C., Rahman, A., and A. Mourad, "Service Function Chaining Use Cases in Fog RAN", draft-bernardos-sfc-fog-ran-07 (work in progress), March 2020.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Alain Mourad
InterDigital Europe

Email: Alain.Mourad@InterDigital.com
URI: http://www.InterDigital.com/

DMM Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

U. Chunduri, Ed.
R. Li
Futurewei
S. Bhaskaran
Altiostar
J. Kaippallimalil, Ed.
Futurewei
J. Tantsura
Apstra, Inc.
L. Contreras
Telefonica
P. Muley
Nokia

November 2, 2020

Transport Network aware Mobility for 5G
draft-clt-dmm-tn-aware-mobility-08

Abstract

This document specifies a framework and mapping from slices in 5G mobile systems to transport slices in IP and Layer 2 transport networks. Slices in 5G systems are characterized by latency bounds, reservation guarantees, jitter, data rates, availability, mobility speed, usage density, criticality and priority. These characteristics should be mapped to the transport network slice characteristics that include bandwidth, latency and criteria such as isolation, directionality and disjoint routes. Mobile slice criteria need to be mapped to the appropriate transport slice and capabilities offered in backhaul, midhaul and fronthaul connectivity segments between radio side network functions and user plane function (gateway).

This document describes how mobile network functions map its slice criteria to identifiers in IP packets that transport network segments use to grant transport layer services during UE mobility scenarios. Applicability of this framework and underlying transport networks, which can enable different slice properties is also discussed. This is based on mapping between mobile and transport underlays (L2, Segment Routing, IPv6, MPLS and IPv4).

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The 3GPP architecture for 5GS is defined in [TS.23.501-3GPP], [TS.23.502-3GPP] and [TS.23.503-3GPP]. The architecture defines a comprehensive set of functions for access mobility, session handling and related functions for subscription management, authentication and policy among others. These network functions (NF) are defined using a service-based architecture (SBA) that allows NFs to expose their functions via an API and common service framework.

UPFs are the data forwarding entities in the 5GC architecture. The architecture allows the placement of Branching Point (BP) and Uplink Classifier (ULCL) UPFs closer to the access network (5G-AN). The 5G-AN can be a radio access network or any non-3GPP access network, for example, WLAN. The IP address is anchored by a PDU session anchor UPF (PSA UPF). 3GPP slicing and RAN aspects are further described in Appendix A.1.

5GS allows more than one UPF on the path for a PDU (Protocol Data Unit) session that provides various functionality including session anchoring, uplink classification and branching point for a multihomed IPv6 PDU session. The interface between the BP/ULCL UPF and the PSA UPF is called N9 [TS.23.501-3GPP]. 3GPP has adopted GTP-U for the N9 and N3 interface between the various UPF instances and the (R)AN and also for the F1-U interface between the DU and the CU in the RAN. 3GPP has specified control and user plane aspects in [TS.23.501-3GPP] to provide slice and QoS support. 3GPP has defined three broad slice types to cover enhanced mobile broadband (eMBB) communications, ultra-reliable low latency communications(URLLC) and massive internet of things (mIoT). ATIS [ATIS075] has defined an additional slice type for V2X services. There may be multiple instances of a slice type to satisfy some characteristics like isolation. The slice details in 3GPP, ATIS or NGMN do not specify how slice characteristics for QoS, hard /soft isolation, protection and other

aspects should be satisfied in IP transport networks. This is explored further in this document.

1.1. Problem Statement

5GS defines network slicing as one of the core capability of 5GC with slice awareness from Radio and 5G Core (5GC) network. The 5G System (5GS) as defined, does not consider the resources and functionalities needed from transport network for the selection of UPF. This is seen as independent functionality and currently not part of 5GS.

However, the lack of underlying Transport Network (TN) awareness may lead to selection of sub-optimal UPF(s) and/or 5G-AN during various procedures in 5GS (e.g., session establishment and various mobility scenarios). Meeting the specific slice characteristics on the F1-U, N3, N9 interfaces depends on the IP transport underlay providing these resources and capabilities. This could also lead to the inability in meeting SLAs for real-time, mission-critical or latency sensitive services.

The 5GS provides slices to its clients (UEs). The UE's PDU session spans the access network (radio network including the F1-U) and N3 and N9 transport segments which have an IP transport underlay. The 5G operator needs to obtain slice capability from the IP transport provider. Several UE sessions that match a slice may be mapped to an IP transport segment. Thus there needs to be a mapping between the slice capability offered to the UE (S-NSSAI) and what is provided by the IP transport.

1.2. Solution Approach

This document specifies an approach to fulfil the needs of 5GS to transport user plane traffic from 5G-AN to UPF in an optimized fashion. This is done by, keeping establishment and mobility procedures aware of underlying transport network along with slicing requirements.

Section 2 describes in detail on how TN aware mobility can be built irrespective of underlying TN technology used. How other IETF TE technologies applicable for this draft is specified in Section 3.2.

1.3. Acronyms

5QI - 5G QoS Indicator

5G-AN - 5G Access Network

AMF - Access and Mobility Management Function (5G)

BP - Branch Point (5G)

CSR - Cell Site Router

CP - Control Plane (5G)

CU - Centralized Unit (5G, gNB)

DN - Data Network (5G)

DU - Distributed Unit (5G, gNB)

eMBB - enhanced Mobile Broadband (5G)

FRR - Fast ReRoute

gNB - 5G NodeB

GBR - Guaranteed Bit Rate (5G)

GTP-U - GPRS Tunneling Protocol - Userplane (3GPP)

IGP - Interior Gateway Protocols (e.g. IS-IS, OSPFv2, OSPFv3)

LFA - Loop Free Alternatives (IP FRR)

mIOT - Massive IOT (5G)

MPLS - Multi Protocol Label Switching

NSSMF - Network Slice Selection Management Function

QFI - QoS Flow ID (5G)

PPR - Preferred Path Routing

PDU - Protocol Data Unit (5G)

PW - Pseudo Wire

RAN - Radio Access Network

RQI - Reflective QoS Indicator (5G)

SBI - Service Based Interface (5G)

SID - Segment Identifier

SMF - Session Management Function (5G)

SSC - Session and Service Continuity (5G)

SST - Slice and Service Types (5G)

SR - Segment Routing

TE - Traffic Engineering

ULCL - Uplink Classifier (5G)

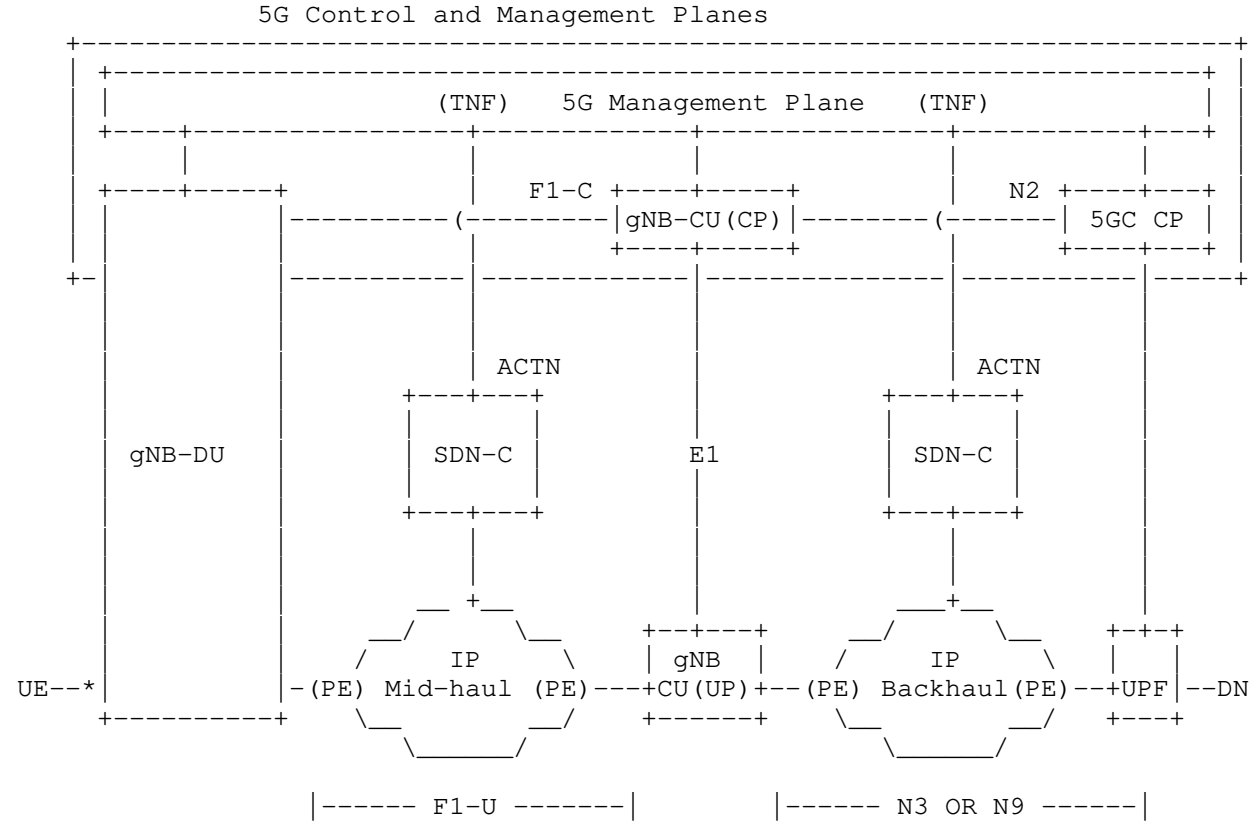
UP - User Plane(5G)

UPF - User Plane Function (5G)

URLLC - Ultra reliable and low latency communications (5G)

2. Transport and Slice aware Mobility in 5G Networks

3GPP architecture [TS.23.501-3GPP], [TS.23.502-3GPP] describe slicing in 5GS. However, the application of 5GS slices in transport network for backhaul, mid-haul and front haul are not explicitly covered. To support specific characteristics in backhaul (N3, N9), mid-haul (F1) and front haul, it is necessary to map and provision corresponding resources in the transport domain. This section describes how to provision the mapping information in transport network and apply it so that user plane packets can be provided the transport resources (QoS, isolation, protection, etc.) expected by the 5GS slices.



* Radio and Fronthaul

Figure 1: Backhaul and Mid-haul Transport Network for 5G

2.1. Backhaul and Mid-Haul Transport Network

Figure 1 depicts IP Xhaul network with SDN-C and PE (Provider Edge) routers provide IP transport service to 5GS user plane entities 5G-AN (e.g. gNB) and UPF. 5GS architecture with high level management, control and user plane entities and its interaction with the IP transport plane is shown here. The slice capability required in IP transport networks is estimated and provisioned by the functionality as specified in Section 2.4 (TNF) with support from various other control plane functions such as the Network Data Analytics Function (NWDAF), Network Function Repository Function (NRF) and Policy Control Function (PCF). The TNF is only a logical function that maybe realized in a 3GPP management function such as Network Slice Selection Management Function (NSSMF) defined in [TS.28.533-3GPP].

The TNF requests the SDN-C to provision the IP XHaul network using ACTN [RFC8453].

The 5G management plane in Figure 1 interacts with the 5G control plane - the 5GC (5G Core), gNB-CU (5G NodeB Centralized Unit) and gNB-DU (5G Node B Distributed Unit). Non-access stratum (NAS) signaling from the UE for session management, mobility is handled by the 5GC. When a UE initiates session establishment, it indicates the desired slice type in the S-NSSAI (Specific Network Slice Selection Assistance Information) field. The AMF uses the S-NSSAI, other subscription information and configuration in the NSSF to select the appropriate SMF and the SMF in turn selects UPFs (User Plane Functions) that are able to provide the specified slice resources and capabilities.

The AMF, SMF, NSSF, PCF, NRF, NWDAF and other control functions in 5GC are described in [TS.23.501-3GPP] Some of the slice capabilities along the user plane path between the (R)AN and UPFs (F1-U, N3, N9 segments) such as a low latency path, jitter, protection and priority needs these to be provided by the IP transport network.

The 5G user plane from UE to DN (Data Network) includes a mid-haul segment (F1-U between gNB DU(UP), gNB CU(UP)) and backhaul (N3 between gNB - UPF; N9 between UPFs). If the RAN uses lower layer split architecture as specified by O-RAN alliance, then the user plane path from UE to DN also includes the fronthaul interface. The fronthaul interface carries the radio frames in the form of In-phase (I) and Quadrature (Q) samples using eCPRI encapsulation over Ethernet or UDP over IP.

The N3, N9 and F1 user planes use GTP-U [TS.29.281-3GPP] to transport UE PDUs (IPv4, IPv6, IPv4v6, Ethernet or Unstructured). For the front haul described further in Section 2.2, an Ethernet transport with VLANs can be expected to be the case in many deployments.

Figure 1 also depicts the PE router, where transport paths are initiated/terminated can be deployed separately with UPF or both functionalities can be in the same node. The TNF provisions this in the SDN-C of the IP XHaul network using ACTN [RFC8453]. When a GTP encapsulated user packet from the (R)AN (gNB) or UPF with the slice information traverses the F1-U/N3/N9 segment, the PE router of the IP transport underlay can inspect the slice information and provide the provisioned capabilities. This is elaborated further in Section 2.5.

2.2. Front Haul Transport Network

The O-RAN Alliance has specified the fronthaul interface between the O-RU and the O-DU in [ORAN-WG4.CUS-O-RAN]. The radio layer information, in the form of In-phase (I) and Quadrature (Q) samples are transported using Enhanced Common Public Radio Interface (eCPRI) framing over Ethernet or UDP. On the Ethernet based fronthaul interface, the slice information is carried in the Ethernet header through the VLAN tags. The Ethernet switches in the fronthaul transport network can inspect the slice information (VLAN tag) in the Ethernet header and provide the provisioned capabilities. The mapping of I and Q samples of different radio resources (radio resource blocks or carriers etc.,.) to different slices and to their respective VLAN tags on the fronthaul interface is controlled by the O-RAN fronthaul C-Plane and M-Plane interfaces. On UDP based fronthaul interface, the slice information is carried in the IP or UDP header. The PE routers of the fronthaul transport network can inspect the slice information in the IP or UDP header and provide the provisioned capabilities. The fronthaul transport network is latency and jitter sensitive. The provisioned slice capabilities in the fronthaul transport network MUST take care of the latency and jitter budgets of the specific slice for the fronthaul interface. The provisioning of the fronthaul transport network is handled by the SDN-C pertaining to the fronthaul transport.

2.3. Mobile Transport Network Context (MTNC) and Scalability

The MTNC represents a slice, QoS configuration for a transport path between two 3GPP user plane functions. The Mobile-Transport Network Context Identifier (MTNC-ID) is generated by the TNF to be unique for each path and per traffic class (including QoS and slice aspects). Thus, there may be more than one MTNC-ID for the same QoS and path if there is a need to provide isolation (slice) of the traffic. It should be noted that MTNC are per class/path and not per user session (nor is it per data path entity). The MTNC-IDs are configured by the TNF to be unique within a provisioning domain.

Since the MTNC-IDs are not generated per user flow or session, there is no need for unique MTNC-IDs per flow/session. In addition, since the traffic estimation not performed at the time of session establishment, there is no provisioning delay experienced during session setup. The MTNC-ID space scales as a square of the number sites between which 3GPP user plane functions require paths. If there are T traffic classes across N sites, the number of MTNC-IDs in a fully meshed network is (N*(N-1)/2) * T. For example, if there are 3 traffic classes between 25 sites, there would be at most 900 MTNC-IDs required. Multiple slices for the same QoS class that need to be

fully isolated, will add to the MTNC provisioning. An MTNC-ID space of 16 bits (65K+ identifiers) can be expected to be sufficient.

2.4. Transport Network Function (TNF)

Figure 1 shows a view of the functions and interfaces for provisioning the MTNC-IDs. The focus is on provisioning between the 3GPP management plane (NSSMF), transport network (SDN-C) and carrying the MTNC-IDs in PDU packets for the transport network to grant the provisioned resources.

In Figure 1, the TNF (logical functionality within the NSSMF) requests the SDN-C in the transport domain to program the TE path using ACTN [RFC8453]. The SDN-C programs the Provider Edge (PE) routers and internal routers according to the underlay transport technology (e.g., MPLS, SR, PPR). The PE router inspects incoming PDU data packets for the UDP SRC port which mirrors the MTNC-ID, classifies and provides the VN service provisioned across the transport network.

The detailed mechanisms by which the NSSMF provides the MTNC-IDs to the control plane and user plane functions are for 3GPP to specify. Two possible options are outlined below for completeness. The NSSMF may provide the MTNC-IDs to the 3GPP control plane by either providing it to the Session Management Function (SMF), and the SMF in turn provisions the user plane functions (UP-NF1, UP-NF2) during PDU session setup. Alternatively, the user plane functions may request the MTNC-IDs directly from the TNF/NSSMF. Figure 1 shows the case where user plane entities request the TNF/NSSMF to translate the Request and get the MTNC-ID. Another alternative is for the TNF to provide a mapping of the 3GPP Network Instance Identifier, described in Section 2.7 and the MTNC-ID to the user plane entities via configuration.

The TNF should be seen as a logical entity that can be part of NSSMF in the 3GPP management plane [TS.28.533-3GPP]. The NSSMF may use network configuration, policies, history, heuristics or some combination of these to derive traffic estimates that the TNF would use. How these estimates are derived are not in the scope of this document. The focus here is only in terms of how the TNF and SDN-C are programmed given that slice and QoS characteristics across a transport path can be represented by an MTNC-ID. The TNF requests the SDN-C in the transport network to provision paths in the transport domain based on the MTNC-ID. The TNF is capable of providing the MTNC-ID provisioned to control and user plane functions in the 3GPP domain. Detailed mechanisms for programming the MTNC-ID should be part of the 3GPP specifications.

2.5. Transport Provisioning

Functionality of transport provisioning for an engineered IP transport that supports 3GPP slicing and QoS requirements in [TS.23.501-3GPP] is described in this section.

During a PDU session setup, the AMF using input from the NSSF selects a network slice and SMF. The SMF with user policy from Policy Control Function (PCF) sets 5QI (QoS parameters) and the UPF on the path of the PDU session. While QoS and slice selection for the PDU session can be applied across the 3GPP control and user plane functions as outlined in Section 2, the IP transport underlay across F1-U, N3 and N9 segments do not have enough information to apply the resource constraints represented by the slicing and QoS classification. Current guidelines for interconnection with transport networks [IR.34-GSMA] provide an application mapping into DSCP. However, these recommendations do not take into consideration other aspects in slicing like isolation, protection and replication.

IP transport networks have their own slice and QoS configuration based on domain policies and the underlying network capability. Transport networks can enter into an agreement for virtual network services (VNS) with client domains using the ACTN [RFC8453] framework. An IP transport network may provide such slice instances to mobile network operators, CDN providers or enterprises for example. The 3GPP mobile network, on the other hand, defines a slice instance for UEs as are the mobile operator's 'clients'. The Network Slice Selection Management Function (NSSMF) [TS 28.533] that interacts with a TN controller like an SDN-C (that is out of scope of 3GPP).

The ACTN VN service can be used across the IP transport networks to provision and map the slice instance and QoS of the 3GPP domain to the IP transport domain. An abstraction that represents QoS and slice instance in the mobile domain and mapped to ACTN VN service in the transport domain is represented here as MTNC-IDs. Details of how the MTNC-IDs are derived are up to functions that can estimate the level of traffic demand.

The 3GPP network/5GS provides slices instances to its clients (UE) that include resources for radio and mobile core segments. The UE's PDU session spans the access network (radio) and F1-U/N3/N9 transport segments which have an IP transport underlay. The 5G operator needs to obtain slice capability from the IP transport provider since these resources are not seen by the 5GS. Several UE sessions that match a slice may be mapped to an IP transport segment. Thus, there needs to be a mapping between the slice capability offered to the UE (NSSAI) and what is provided by the IP transport.

When the 3GPP user plane function (5G-AN, UPF) does not terminate the transport underlay protocol (e.g., MPLS), it needs to be carried in the IP protocol header from end-to-end of the mobile transport connection (N3, N9). [I-D.ietf-dmm-5g-uplane-analysis] discusses these scenarios in detail.

2.6. MTNC-ID in the Data Packet

When the 3GPP user plane function (5G-AN, UPF) and transport provider edge is on different nodes, the PE router needs to have the means by which to classify the PDU packet. The mapping information is provisioned between the 5G provider and IP transport network and corresponding information should be carried in each IP packet on the F1-U, N3, N9 interface. To allow the IP transport edge nodes to inspect the transport context information efficiently, it should be carried in an IP header field that is easy to inspect. It may be noted that the F1-U, N3 and N9 interfaces in 5GS are IP interfaces. Thus, Layer 2 alternatives such as VLAN will fail if there are multiple L2 networks on the F1-U or N3 or N9 path. GTP (F1-U, N3, N9 encapsulation header) field extensions offer a possibility, however these extensions are hard for a transport edge router to parse efficiently on a per packet basis. Other IP header fields like DSCP are not suitable as it only conveys the QoS aspects (but not other aspects like isolation, protection, etc.)

IPv6 extension headers like SRv6 may be options to carry the MTNC-ID when such mechanism is a viable (if complete transport network is IPv6 based). To minimise the protocol changes are required and make this underlay transport independent (IPv4/IPv6/MPLS/L2), an option is to provision a mapping of MTNC-ID to a UDP port range of the GTP encapsulated user packet. A simple mapping table between the MTNC-ID and the source UDP port number can be configured to ensure that ECMP /load balancing is not affected adversely by encoding the UDP source port with an MTNC-ID mapping. This mapping is configured in 3GPP user plane functions (5G-AN, UPF) and Provider Edge (PE) Routers that process MTNC-IDs.

PE routers can thus provision a policy based on the source UDP port number (which reflects the mapped MTNC-ID) to underlying transport path and then deliver the QoS/slice resource provisioned in the transport network. The source UDP port that is encoded is the outer IP (corresponding to GTP header) while the inner IP packet (UE payload) is unaltered. The source UDP port is encoded by the node that creates the GTP-U encapsulation and therefore, this mechanism has no impact to UDP checksum calculations.

3GPP network operators may use IPSec gateways (SEG) to secure packets between two sites - for example over an F1-U, N3 or N9 segment. The

MTNC identifier in the GTP-U packet should be in the outer IP source port even after IPSec encryption for PE transport routers to inspect and provide the level of service provisioned. Tunnel mode - which is the case for SEG/IPSec gateways - adds an outer IP header in both AH (Authenticated Header) and ESP (Encapsulated Security Payload) modes. The GTP-U / UDP source port with encoded MTNC identifier should be copied to the IPSec tunnel ESP header. One option is to use 16 bits from the SPI field of the ESP header to encode the MTNC identifier and use the remaining 16 bits in SPI field to identify an SA. Load balancing entropy for ECMP will not be affected as the MTNC encoding mechanism already accounts for this.

If the RAN uses O-RAN lower layer split architecture, then a fronthaul network is involved. On an Ethernet based fronthaul transport network, VLAN tag may be an option to carry the MTNC-ID. The VLAN ID provides a 12 bit space and is sufficient to support up to 4096 slices on the fronthaul transport network. The mapping of fronthaul traffic to corresponding network slice is based on the radio resource for which the fronthaul carries the I and Q samples. The mapping of fronthaul traffic to the VLAN tag corresponding to the network slice is specified in Section 2.2. On UDP based fronthaul transport network, the UDP source port can be used to carry the MTNC-ID.

2.7. Functionality for E2E Management

With the TNF functionality in 5GS Service Based Interface, the following additional functionalities are required for end-2-end slice management including the transport network:

- The Specific Network Slice Selection Assistance Information (S-NSSAI) of PDU session SHOULD be mapped to the assigned transport VPN and the TE path information for that slice.

- For transport slice assignment for various SSTs (eMBB, URLLC, MIoT) corresponding underlay paths need to be created and monitored from each transport end point (CSR and PE@UPF).

- During PDU session creation, apart from radio and 5GC resources, transport network resources needed to be verified matching the characteristics of the PDU session traffic type.

- The TNF MUST provide an API that takes as input the source and destination 3GPP user plane element address, required bandwidth, latency and jitter characteristics between those user plane elements and returns as output a particular TE path's identifier, that satisfies the requested requirements.

- Mapping of PDU session parameters to underlay SST paths need to be done. One way to do this to let the SMF install a Forwarding Action Rule (FAR) in the UPF via N4 with the FAR pointing to a "Network Instance" in the UPF. A "Network Instance" is a logical identifier for an underlying network. The "Network Instance" pointed by the FAR can be mapped to a transport path (through L2/ L3 VPN). FARs are associated with Packet Detection Rule (PDR). PDRs are used to classify packets in the uplink (UL) and the downlink (DL) direction. For UL procedures specified in Section 2.5, Section 2.6 can be used for classifying a packet belonging to a particular slice characteristic. For DL, at a PSA UPF, the UE IP address is used to identify the PDU session, and hence the slice a packet belongs to and the IP 5 tuple can be used for identifying the flow and QoS characteristics to be applied on the packet at UPF. If a PE is not co-located at the UPF then mapping to the underlying TE paths at PE happens based on the encapsulated GTP-U packet as specified in Section 2.6.

- In some SSC modes [I-D.chunduri-dmm-5g-mobility-with-ppr], if segmented path (CSR to PE@staging/ULCL/BP-UPF to PE@anchor-point-UPF) is needed, then corresponding path characteristics MUST be used. This includes a path from CSR to PE@UL-CL/BP UPF [TS.23.501-3GPP] and UL-CL/BP UPF to eventual UPF access to DN.

- Continuous monitoring of the underlying transport path characteristics should be enabled at the endpoints (technologies for monitoring depends traffic engineering technique used as described in Section 3.2). If path characteristics are degraded, reassignment of the paths at the endpoints should be performed. For all the affected PDU sessions, degraded transport paths need to be updated dynamically with similar alternate paths.

- During UE mobility event similar to 4G/LTE i.e., gNB mobility (F1 based, Xn based or N2 based), for target gNB selection, apart from radio resources, transport resources MUST be factored. This enables handling of all PDU sessions from the UE to target gNB and this require co-ordination of gNB, AMF, SMF with the TNF module.

Integrating the TNF as part of the 5GS Service Based Interfaces, provides the flexibility to control the allocation of required characteristics from the TN during a 5GS signaling procedure (e.g. PDU Session Establishment). If TNF is seen as separate and in management plane, this real time flexibility is lost. Changes to detailed signaling to integrate the above for various 5GS procedures as defined in [TS.23.502-3GPP] is beyond the scope of this document.

3. Transport Network Underlays

Apart from the various flavors of IETF VPN technologies to share the transport network resources and capacity, TE capabilities in the underlay network is an essential component to realize the 5G TN requirements. This section focuses on various transport underlay technologies (not exhaustive) and their applicability to realize Midhaul/Backhaul transport networks. Focus is on the user/data plane i.e., F1-U/N3/N9 interfaces as laid out in the framework Figure 1.

3.1. Applicability

- For 3 different SSTs, 3 transport TE paths can be signaled from any node in the transport network. For Uplink traffic, the 5G-AN will choose the right underlying TE path of the UPF based on the S-NSSAI the PDU Session belongs to and/or the UDP Source port (corresponds to the MTNC-ID Section 2.5) of the GTP-U encapsulation header. Similarly in the Downlink direction matching Transport TE Path of the 5G-AN is chosen based on the S-NSSAI the PDU Session belongs to. The table below shows a typical mapping:

GTP/UDP SRC PORT	SST in S-NSSAI	Transport Path Info	Transport Path Characteristics
Range Xx - Xy X1, X2(discrete values)	MIOT (massive IOT)	PW ID/VPN info, TE-PATH-A	GBR (Guaranteed Bit Rate) Bandwidth: Bx Delay: Dx Jitter: Jx
Range Yx - Yy Y1, Y2(discrete values)	URLLC (ultra-low latency)	PW ID/VPN info, TE-PATH-B	GBR with Delay Req. Bandwidth: By Delay: Dy Jitter: Jy
Range Zx - Zy Z1, Z2(discrete values)	EMBB (broadband)	PW ID/VPN info, TE-PATH-C	Non-GBR Bandwidth: Bx

Figure 2: Mapping of Transport Paths on F1-U/N3/N9

- It is possible to have a single TE Path for multiple input points through a MP2P TE tree structure separate in UL and DL direction.

- Same set of TE Paths are created uniformly across all needed 5G-ANs and UPFs to allow various mobility scenarios.

- Any modification of TE parameters of the path, replacement path and deleted path needed to be updated from TNF to the relevant ingress points. Same information can be pushed to the NSSF, and/or SMF as needed.

- TE Paths support for native L2, IPv4 and IPv6 data/user planes with optional TE features are desirable in some network segments. As this is an underlay mechanism it can work with any overlay encapsulation approach including GTP-U as defined currently for F1-U/N3/N9 interface.

In some E2E scenarios, security is desired granularly in the underlying transport network. In such cases, there would be a need to have separate sub-ranges under each SST to provide the TE path in preserving the security characteristics. The UDP Source Port range

captured in Figure 2 would be sub-divided to maintain the TE path for the current SSTs with the security. The current solution doesn't provide any mandate on the UE traffic in selecting the type of security.

3.2. Transport Network Technologies

While there are many Software Defined Networking (SDN) approaches are available, this sections is not intended to list all the possibilities in this space but merely captures the technologies for various requirements discussed in this document.

RSVP-TE [RFC3209] provides a lean transport overhead for the TE path for MPLS user plane. However, it is perceived as less dynamic in some cases and has some provisioning overhead across all the nodes in N3 and N9 interface nodes. Also, it has another drawback with excessive state refresh overhead across adjacent nodes and this can be mitigated with [RFC8370].

SR-TE [RFC8402] does not explicitly signal bandwidth reservation or mechanism to guarantee latency on the nodes/links on SR path. But SR allows path steering for any flow at the ingress and particular path for a flow can be chosen. Some of the issues and suitability for mobile use plane are documented at Section 5.3 of [I-D.bogineni-dmm-optimized-mobile-user-plane]. However, [I-D.ietf-dmm-srv6-mobile-uplane] presents various options for optimized mobile user plane with SRv6 with or without GTP-U overhead along with traffic engineering capabilities. SR-MPLS allows reduction of the control protocols to one IGP (without needing for LDP and RSVP-TE).

Preferred Path Routing (PPR) is an integrated routing and TE technology and the applicability for this framework is described in [I-D.chunduri-dmm-5g-mobility-with-ppr]. PPR does not remove GTP-U, unlike some other proposals laid out in [I-D.bogineni-dmm-optimized-mobile-user-plane]. Instead, PPR works with the existing cellular user plane (GTP-U) for F1-U/N3 and N9. In this scenario, PPR will only help providing TE benefits needed for 5G slices from transport domain perspective. It does so for any underlying user/data plane used in the transport network (L2/IPv4/IPv6/MPLS).

As specified with the integrated transport network function (TNF), a particular RSVP-TE path for MPLS or SR path for MPLS and IPv6 with SRH user plane or PPR with PPR-ID [I-D.chunduri-dmm-5g-mobility-with-ppr], can be supplied to SMF for mapping a particular PDU session to the transport path.

4. Acknowledgements

Thanks to Young Lee for discussions on this document including ACTN applicability for the proposed TNF. Thanks to Sri Gundavelli, Kausik Majumdar and 3GPP delegates who provided detailed feedback on this document.

5. IANA Considerations

This document has no requests for any IANA code point allocations.

6. Security Considerations

This document does not introduce any new security issues.

7. Contributing Authors

The following people contributed substantially to the content of this document and should be considered co-authors.

Xavier De Foy
InterDigital Communications, LLC
1000 Sherbrooke West
Montreal
Canada

Email: Xavier.Defoy@InterDigital.com

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

8.2. Informative References

[ATIS075] Alliance for Telecommunications Industry Solutions (ATIS), "IOT Categorization: Exploring the Need for Standardizing Additional Network Slices ATIS-I-0000075", September 2019.

[I-D.bogineni-dmm-optimized-mobile-user-plane]
Bogineni, K., Akhavain, A., Herbert, T., Farinacci, D., Rodriguez-Natal, A., Carofiglio, G., Auge, J., Muscariello, L., Camarillo, P., and S. Homma, "Optimized Mobile User Plane Solutions for 5G", draft-bogineni-dmm-optimized-mobile-user-plane-01 (work in progress), June 2018.

[I-D.ietf-dmm-5g-uplane-analysis]
Homma, S., Miyasaka, T., Matsushima, S., and D. Voyer, "User Plane Protocol and Architectural Analysis on 3GPP 5G System", draft-ietf-dmm-5g-uplane-analysis-03 (work in progress), November 2019.

[I-D.ietf-dmm-srv6-mobile-uplane]
Matsushima, S., Filsfils, C., Kohno, M., Camarillo, P., Voyer, D., and C. Perkins, "Segment Routing IPv6 for Mobile User Plane", draft-ietf-dmm-srv6-mobile-uplane-09 (work in progress), July 2020.

[IR.34-GSMA]
GSM Association (GSMA), "Guidelines for IPX Provider Networks (Previously Inter-Service Provider IP Backbone Guidelines, Version 14.0", August 2018.

[ORAN-WG4.CUS-O-RAN]
O-RAN Alliance (O-RAN), "O-RAN Fronthaul Working Group; Control, User and Synchronization Plane Specification; v2.0.0", August 2019.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC8370] Beeram, V., Ed., Minei, I., Shakir, R., Pacella, D., and T. Saad, "Techniques to Improve the Scalability of RSVP-TE Deployments", RFC 8370, DOI 10.17487/RFC8370, May 2018, <https://www.rfc-editor.org/info/rfc8370>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[TS.23.501-3GPP] 3rd Generation Partnership Project (3GPP), "System Architecture for 5G System; Stage 2, 3GPP TS 23.501 v2.0.1", December 2017.

[TS.23.502-3GPP] 3rd Generation Partnership Project (3GPP), "Procedures for 5G System; Stage 2, 3GPP TS 23.502, v2.0.0", December 2017.

[TS.23.503-3GPP] 3rd Generation Partnership Project (3GPP), "Policy and Charging Control System for 5G Framework; Stage 2, 3GPP TS 23.503 v1.0.0", December 2017.

[TS.28.533-3GPP] 3rd Generation Partnership Project (3GPP), "Management and Orchestration Architecture Framework (Release 15)", June 2018.

[TS.29.281-3GPP] 3rd Generation Partnership Project (3GPP), "GPRS Tunneling Protocol User Plane (GTPv1-U), 3GPP TS 29.281 v15.1.0", December 2018.

[TS.38.300-3GPP] 3rd Generation Partnership Project (3GPP), "NR; NR and NG-RAN Overall Description; Stage 2; v15.7.0", September 2019.

[TS.38.401-3GPP] 3rd Generation Partnership Project (3GPP), "NG-RAN; Architecture description; v15.7.0", September 2019.

Appendix A. New Control Plane and User Planes

A.1. Slicing Framework and RAN Aspects

The 3GPP architecture defines slicing aspects where the Network Slice Selection Function (NSSF) assists the Access Mobility Manager (AMF) and Session Management Function (SMF) to assist and select the right entities and resources corresponding to the slice requested by the User Equipment (UE). The User Equipment (UE) indicates information

regarding the set of slices it wishes to connect, in the Network Slice Selection Assistance Information (NSSAI) field during network registration procedure (Attach) and the specific slice the UE wants to establish an IP session, in the Specific NSSAI (S-NSSAI) field during the session establishment procedure (PDU Session Establishment). The AMF selects the right SMF and the SMF in turn selects the User Plane Functions (UPF) so that the QoS and capabilities requested can be fulfilled.

The architecture for the Radio Access Network (RAN) is defined in [TS.38.300-3GPP] and [TS.38.401-3GPP]. The 5G RAN architecture allows disaggregation of the RAN into a Distributed Unit (DU) and a Centralized Unit (CU). The CU is further split into control plane (CU-CP) and user plane (CU-UP). The interface between CU-UP and the DU for the user plane traffic is called the F1-U and between the CU-CP and DU for the control plane traffic is called the F1-C. The F1-C and the F1-U together are called the mid-haul interfaces. The DU does not have a CP/UP split. Apart from 3GPP, O-RAN Alliance has specified further disaggregation of the RAN at the lower layer (physical layer). The DU is disaggregated into a ORAN DU (O-DU) which runs the upper part of the physical layer, MAC and RLC and the ORAN Radio Unit (O-RU) which runs the lower part of the physical layer. The interface between the O-DU and the O-RU is called the Fronthaul interface and is specified in [ORAN-WG4.CUS-O-RAN].

A.2. Slice aware Mobility: Discrete Approach

In this approach transport network functionality from the 5G-AN to UPF is discrete and 5GS is not aware of the underlying transport network and the resources available. Deployment specific mapping function is used to map the GTP-U encapsulated traffic at the 5G-AN (e.g. gNB) in UL and UPF in DL direction to the appropriate transport slice or transport Traffic Engineered (TE) paths. These TE paths can be established using RSVP-TE [RFC3209] for MPLS underlay, SR [RFC3209] for both MPLS and IPv6 underlay or PPR [I-D.chunduri-dmm-5g-mobility-with-ppr] with MPLS, IPv6 with SRH, native IPv6 and native IPv4 underlays.

As per [TS.23.501-3GPP] and [TS.23.502-3GPP] the SMF controls the user plane traffic forwarding rules in the UPF. The UPFs have a concept of a "Network Instance" which logically abstracts the underlying transport path. When the SMF creates the packet detection rules (PDR) and forwarding action rules (FAR) for a PDU session at the UPF, the SMF identifies the network instance through which the packet matching the PDR has to be forwarded. A network instance can be mapped to a TE path at the UPF. In this approach, TNF as shown in Figure 1 need not be part of the 5G Service Based Interface (SBI). Only management plane functionality is needed to create, monitor,

manage and delete (life cycle management) the transport TE paths/ transport slices from the 5G-AN to the UPF (on N3/N9 interfaces). The management plane functionality also provides the mapping of such TE paths to a network instance identifier to the SMF. The SMF uses this mapping to install appropriate FARs in the UPF. This approach provide partial integration of the transport network into 5GS with some benefits.

One of the limitations of this approach is the inability of the 5GS procedures to know, if underlying transport resources are available for the traffic type being carried in PDU session before making certain decisions in the 5G CP. One example scenario/decision could be, a target 5G-AN selection during a N2 mobility event, without knowing if the target 5G-AN is having a underlay transport slice resource for the S-NSSAI and 5QI of the PDU session. The Integrated approach specified below can mitigate this.

Authors' Addresses

Uma Chunduri (editor)
Futurewei
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: umac.ietf@gmail.com

Richard Li
Futurewei
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: richard.li@futurewei.com

Sridhar Bhaskaran
Altiostar

Email: sridharb@altiostar.com

John Kaippallimalil (editor)
Futurewei

Email: john.kaippallimalil@futurewei.com

Jeff Tantsura
Apstra, Inc.

Email: jefftant.ietf@gmail.com

Luis M. Contreras
Telefonica
Sur-3 building, 3rd floor
Madrid 28050
Spain

Email: luismiguel.contrerasmurillo@telefonica.com

Praveen Muley
Nokia
440 North Bernardo Ave
Mountain View, CA 94043
USA

Email: praveen.muley@nokia.com

DMM Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

S. Homma
NTT
T. Miyasaka
KDDI Research
S. Matsushima
SoftBank
D. Voyer
Bell Canada

November 2, 2020

User Plane Protocol and Architectural Analysis on 3GPP 5G System
draft-ietf-dmm-5g-uplane-analysis-04

Abstract

This document analyzes the mobile user plane protocol and the architecture specified in 3GPP 5G documents. The analysis work is to clarify those specifications, extract protocol and architectural requirements and derive evaluation aspects for user plane protocols on IETF side. This work is corresponding to the User Plane Protocol Study work on 3GPP side.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

This document analyzes the mobile user plane protocol and the architecture specified by 3GPP 5G documents. The background of the work is that 3GPP requests through a liaison statement that the IETF

to provide any information for the User Plane Protocol Study work in 3GPP [CP-180116-3GPP]. Justification and the objectives of the study can be found from [CP-173160-3GPP].

We understand that the current user plane protocol, GTP-U [TS.29.281-3GPP], has been well developed in 3GPP, and deployed very widely as the successor of legacy network technologies, such as TDM circuit, or ATM virtual circuit. That GTP-U success seems based on IP overlay technique that is dramatically scaled compare to the previous ones because it successfully isolates mobile session states from the user plane transport network.

Even after that big success, it is definitely worth that 3GPP has decided to revisit user plane which seems to response to IPv6 deployment growth and [IAB-Statement] that encourages the industry to develop strategies for IPv6-only operation. It can be seen from the justification section in [CP-173160-3GPP].

The study description mentions that the study would be based on Release 16 requirement while only Release 15 specifications has been available now. However we believe that to provide adequate information for 3GPP, we need to clearly understand what the current user plane protocol is in Release 15, and architectural requirements for the user plane.

As the liaison statement indicates 3GPP specifications related to user plane, those documents should be a good start point to clarify their specifications and to extract protocol and architectural requirements from them.

1.1. Current Status of Mobile User Plane for 5G

3GPP RAN and CT4 decided to use GTP-U as the 5G user plane encapsulation protocol over N3 and N9 that respectively described in[TS.38.300-3GPP] and [TR.29.891-3GPP]. N3 is an interface between RAN and UPF and N9 is an interface between different UPFs [TS.23.501-3GPP].

In [TR.29.891-3GPP], it captured user plane requirements and concluded that GTP-U is adopted for the user plane protocol. It seems that GTP-U was only option to be chose and it focused on how to carry 5G specific QoS information between UPF and access networks. That is described in section 5.2 and 11.2 of [TR.29.891-3GPP]. Another aspects of user plane requirements couldn’t be found.

1.2. Our Way of Analysis Work

First, we analyze [TS.29.281-3GPP] for clarifying it as the current user plane protocol in the 5G system. [TR.29.891-3GPP] describes how GTP-U is selected as the user plane protocol for 5G in 3GPP. Clarified characteristics of the protocol are described in Section 3.

Then, to clarify what are required to the user plane protocol in architecture level, we analyze [TS.23.501-3GPP] as the 5G system architecture specification. [TS.23.502-3GPP] is the specification of system procedures that helps us to understand how the system works in the architecture. [TS.23.503-3GPP] is also helpful to find the role of user plane in the architecture that influences user plane protocol. Extracted architectural requirements are described in Section 4.

Based on the results of above, we identify some aspects where there might be gap between the current user plane protocol and the architectural requirements on which [TR.29.891-3GPP] does not discuss. That aspects are discussed Section 5. That's what we intend to be as a part of the reply to 3GPP. CT4 WG in 3GPP can utilize it as an input to evaluate the candidate protocols for user plane to the 5G system including the current protocol.

2. Terms and Abbreviations

This section describes terms of functions and interfaces relevant to user plane protocol which we extract from the 3GPP specifications since this document focuses on user plane.

In those specifications, there are so many unique terms and abbreviations in the 3GPP context which IETF community seems not familiar with. We will try to bring those terms with brief explanations to make sure common understanding for them.

GTP: GPRS Tunneling Protocol

GTP-U: User Plane part of GTP

> Noted that GTP version 1 (GTPv1-U) is the user-plane protocol specification which is defined in [TS.29.281-3GPP]. Unless there is no specific annotation, we refer GTP-U to GTPv1-U in this document.

PDU: Protocol Data Unit of end-to-end user protocol packet.

> Noted that the PDU in 3GPP includes IP header in case that PDU session type is IPv4 or IPv6. In contrast, in IETF it is supposed

that PDU is the payload of IP packet so that it doesn't include IP/TCP/UDP header in end-to-end.

T-PDU: Transport PDU.

G-PDU: GTP encapsulated user Plane Data Unit.

GTP-U has above two notions on PDU. T-PDU is a PDU that GTP-U header encapsulates. G-PDU is a PDU that includes GTP-U header. A G-PDU may include a T-PDU. G-PDU can be sent without T-PDU, but just with extension headers or TLV elements. It can be used for OAM related operations.

PDU session: Association between the UE and a Data Network that provides a PDU connectivity service.

Data Network (DN): The network of operator services, Internet access or 3rd party services.

User Plane (UP): Encapsulating user end-to-end PDU.

In fact, we can't find exact text that defines UP in the architecture specification. However when we see the figure 8.3.1-1 in [TS.23.501-3GPP], we specify UP as the layer right under PDU that directly encapsulates PDU. Underneath layers of UP are UP transport, such as IP/UDP, L2 and L1.

However 3GPP is consistent to use the term user plane when they indicate that layer. In IETF, we can see the terms data plane, or forwarding plane as variations which often makes us tend to be confused in terminology.

QFI: QoS Flow Identifier

UPF: User Plane Function

SMF: Session Management Function

SMF is a control plane function which provides session management service that handling PDU sessions in the control plane. SMF allocates tunnels corresponding to the PDU sessions and configure the tunnel to the UPF.

PFCP: Packet Forwarding Control Protocol

PFCP is used on N4 interface between SMF and UPF to configure the rules of packet detection, forwarding action, QoS enforcement, usage report and buffering for each PDU session.

PDR: Packet Detection Rule

FAR: Fowarding Action Rule

RAN: Radio Access Network

Noted that UP protocol provides a RAN to connect UPF. But the UP protocol is not appeared on the air in the RAN.

3. GTP-U Specification and Observation

In this section we analyze the GTP-U specification and summarize clarified characteristic of GTP-U to see if GTP-U meets the requirements of 5G architecture for user plane in later section.

3.1. GTP-U Tunnel

GTP-U is a tunneling protocol between given a pair of GTP-U tunnel endpoint nodes and encapsulates T-PDU from/to UE on top of IP/UDP. A Tunnel Endpoint Identifier (TEID) value allocated on each end point indicates which tunnel a particular T-PDU belongs to.

The receiving endpoint individually allocate a TEID and the sender tunnel endpoint node encapsulates the IP packet from/to UE with the TEID which is present in GTP-U header on top of IPv4 or IPv6, and UDP. That is described in section 4.2.1 of [TS.29.281-3GPP].

[GTP-U-1]: GTP-U is an unidirectional Point-to-Point tunneling protocol.

Figure 1 shows an example of GTP-U protocol stack for uplink (UL) and downlink (DL) traffic flow. Two GTP-U tunnels are required to form one bi-directional tunnel.

UL: From RAN to UPF1 (TEID=1), and from UPF1 to UPF2 (TEID=2)

DL: From UPF2 to UPF1 (TEID=3), and from UPF1 to RAN (TEID=4)

In 5GS, GTP-U tunnel is established at following interfaces to provide PDU Session between UE and 5GC.

N3: Between RAN and UPF

N9: Between different UPFs

GTP-U allows one tunnel endpoint node to send out a G-PDU to be received by multiple tunnel endpoints by utilizing IP multicast capability of underlay IP networks. That is described in section

4.2.6 of [TS.29.281-3GPP]. It looks GTP-U has Point-to-Multipoint (P2MP) tunneling capability. The P2MP tunneling is used for MBMS (Multimedia Broadcast Multicast Service) through GTP-U tunnel.

[GTP-U-2]: GTP-U supports Point-to-Multipoint tunneling.

UDP is utilized for GTP-U encapsulation and UDP destination port is 2152 which is assigned by IANA. Allocation of UDP source port depends on sender tunnel endpoint node and GTP-U supports dynamic allocation of UDP source port for load balancing objective. The specification of this dynamic allocation is described in section 4.4.2.0 of [TS.29.281-3GPP], however specific procedure, e.g., 5-tuple hashing, is not described in the document and depends on the implementation of GTP-U tunnel endpoint node.

[GTP-U-3]: GTP-U supports load balancing by using dynamic UDP source port allocation.

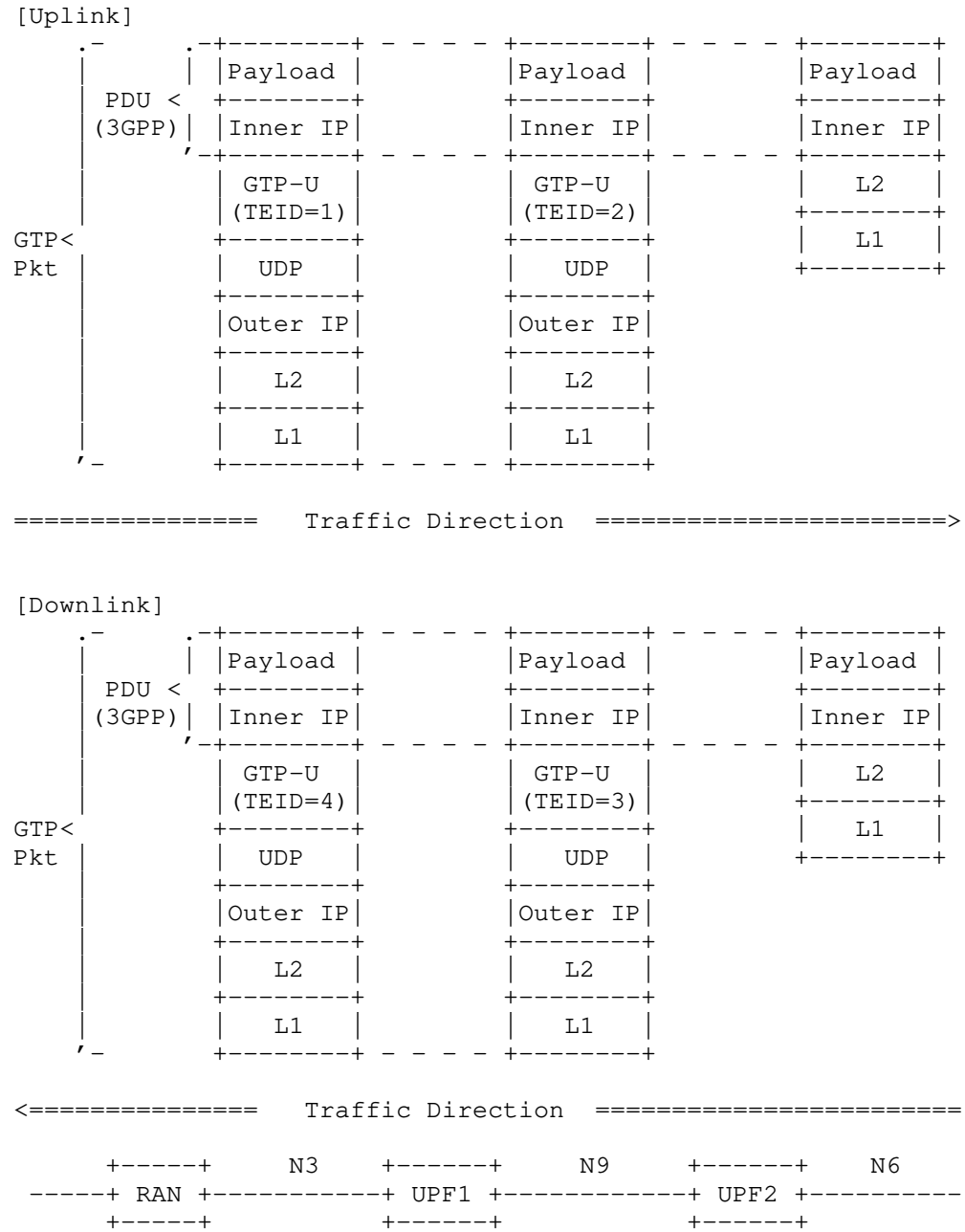


Figure 1: Protocol Stack by GTPv1-U for Uplink and Downlink Traffic Flow

IPv6 flow label [RFC6437] is also candidate method for load balancing especially for IP-in-IPv6 tunnel [RFC6438] like GTP-U. GTP-U also supports dynamic allocation of IPv6 flow label for load balancing objective. The specification of this dynamic allocation is described in section 4.4.2.0 of [TS.29.281-3GPP], however specific procedure, e.g., 5-tuple hashing, is not described in the document and depends on the implementation of GTP-U tunnel endpoint node.

[GTP-U-4]: GTP-U supports load balancing by using dynamic IPv6 flow label allocation.

GTP-U supports both IPv4 and IPv6 as the underlying network layer protocol. From Release 16, GTP-U updates their reference to IPv6 specification from [RFC2460] to [RFC8200] which allows UDP zero checksum for the protocols that use UDP as a tunnel encapsulation, such as GTP-U. As a result of the update, GTP-U over IPv6 also supports the UDP zero checksum if the sender and receiver tunnel endpoint node support the UDP zero checksum, which is described in section 4.4.2.0 of [TS.29.281-3GPP].

[GTP-U-5]: GTP-U supports UDP zero checksum.

"Unnecessary fragmentation should be avoided" is recommended and to avoid the fragmentation operator should configure MTU size at UE [TS.29.281-3GPP]. However, there's no reference and specification of Path MTU Discovery for IPv6 transport. If encapsulated IPv6 packet is too big on a network link between tunnel endpoint nodes, UE may not receive ICMPv6 Packet Too Big message and causes Path MTU Discovery black hole.

[GTP-U-6]: GTP-U does not support to response ICMP PTB for Path MTU Discovery.

Section 9.3 of [TS.23.060-3GPP] specifies advertisement of inner IPv6 link MTU size for UE by IPv6 RA message [RFC4861]. However, this document doesn't specify a procedure to measure MTU size in mobile network system and mobile network operator need to calculate MTU size for UE like Annex C of [TS.23.060-3GPP]. If link MTU of a router in a transport network is accidentally modified, UE cannot detect the event and send packet with initial MTU size, which may cause service disruption due to MTU exceed in the router link.

3.2. GTP-U Header Format

Figure 2 shows general and mandatory GTP-U header and Figure 3 shows extension GTP-U header.

[GTP-U-7]: GTP-U supports sequence number option in the header, but it is not recommended to be used by almost GTP-U entities.

GTP-U header has Sequence Number field to reorder incoming packets based on the sequence number. If Sequence Number Flag is set to '1' it indicates that Sequence Number Filed exists in GTP-U header and examined at receiving tunnel endpoint node to reorder incoming packets. However, the sequence number flag is set to '1' only for RAT HO procedure and sequence number flag should be set to '0' in normal case. Therefore, in normal case receiver tunnel endpoint node doesn't examine sequence number and can't reorder GTP-U packets based on the sequence number. This specification is described in section 5.1 of [TS.29.281-3GPP]. In 3GPP, sequential delivery is required only during handover procedure and is used by only RAN entities.

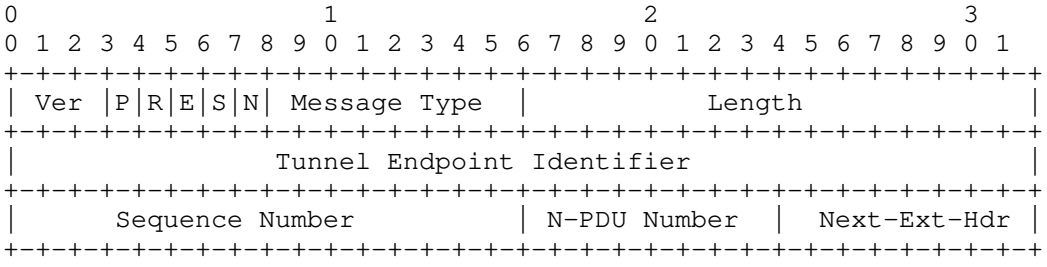


Figure 2: GTP-U Header

- Ver: Version field (Set to '1')
- P: Protocol Type (Set to '1')
- R: Reserved bit (Set to '0')
- E: Extension Header Flag (Set to '1' if extension header exists)
- S: Sequence Number Flag (Set to '1' if sequence number exists)
- N: N-PDU Number Flag (Set to '1' if N-PDU number exists)
- Message Type: Indicates the type of GTP-U message
- Length: Indicates the length in octets of the payload
- Tunnel Endpoint Identifier (TEID)
- Sequence Number: Indicates increasing sequence number for T-PDUs is transmitted via GTP-U tunnels

- N-PDU Number: It is used only for inter SGSN, 2G-3G handover case, etc.

- Next-Ext-Hdr: Indicates following extension header type

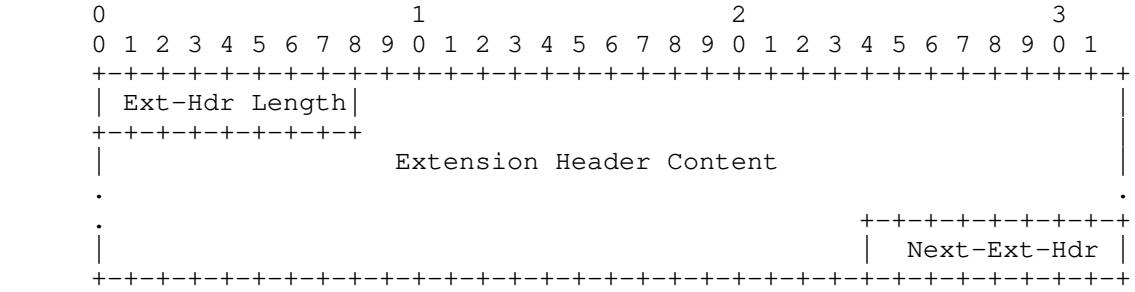


Figure 3: Extension GTP-U Header

- Ext-Hdr Length: Represents the length of the Extension header in units of 4 octets

- Extension Header Content: Contains 3GPP related information

- Next-Ext-Hdr: Indicates following extension header type

The extension GTP-U header is a variable-length and extendable header and contains 3GPP specific information. Following list summarizes every extension header which is used for user plane protocol. These extension headers are defined in [TS.29.281-3GPP]. In this list Next-Ext-Hdr is represented in binary.

- No more extension headers (Next-Ext-Hdr = 00000000)

- Service Class Indicator (Next-Ext-Hdr = 00100000)

- UDP Port (Next-Ext-Hdr = 01000000)

- RAN Container (Next-Ext-Hdr = 10000001)

- Long PDCP PDU Number (Next-Ext-Hdr = 10000010)

- Xw RAN Container (Next-Ext-Hdr = 10000011)

- NR RAN Container (Next-Ext-Hdr = 10000100)

- PDU Session Container (Next-Ext-Hdr = 10000101)

- PDCP PDU Number (Next-Ext-Hdr = 11000000)

[GTP-U-8]: GTP-U supports carrying QoS Identifiers transparently for Access Networks in an extension header.

GTP-U is designed to carry 3GPP specific information with extension headers. 3GPP creates PDU Session Container extension header for NGRAN of 5G to carry QFI. It is described in section 5.2.2.7 of [TS.29.281-3GPP].

[GTP-U-9]: GTP-U supports DSCP marking based on the QFI.

DSCP marking on outer IPv4 or IPv6 shall be set by sender tunnel endpoint node based on the QFI. This specification is described in section 4.4.1 of [TS.29.281-3GPP].

[GTP-U-10]: GTP-U does not specify extension header order.

In general, multiple GTP-U extension headers are able to contained in one GTP-U packet and the order of those extension headers is not specified by [TS.29.281-3GPP]. Thereby the receiving endpoint can't predict exact position where the target extension headers are. This could impact on header lookup performance on the node.

As for PDU Session Container extension header, there is a note in [TS.29.281-3GPP] as "For a G-PDU with several Extension Headers, the PDU Session Container should be the first Extension Header". This note was added at the version 15.3.0 of [TS.29.281-3GPP] which is published on June 2018 in order to accelerate the processing of GTP-U packet at UPF and RAN. It is only one rule regarding the extension header order.

[GTP-U-11]: GTP-U does not support to indicate next protocol type.

When Next-Ext-Hdr is set to 0x00 it indicates that no more extension headers follow. As GTP is designed to indicate protocol types for T-PDU by control-plane signaling, GTP-U doesn't have Next-Protocol-Header field to indicate the T-PDU type in the header.

3.3. Control Plane Protocol for GTP-U

Control plane protocol for GTP-U signals TEID between tunnel endpoint nodes. GTPv2-C [TS.29.274-3GPP] is the original control plane protocol tied with GTP-U in previous generation architectures before CUPS (Control and User Plane Separation).

3GPP decided to use extended PFCP (Packet Forwarding Control Protocol) [TS.29.244-3GPP] for N4 interface [TR.29.891-3GPP] to signal tunnel states from SMF to UPF.

3.4. GTP-U message

GTP-U supports in-band messaging to signal OAM. Currently GTP-U supports following messages [TS.29.281-3GPP].

- Echo Request
- Echo Response
- Supported Extension Headers Notification
- Error Indication
- End Marker

[GTP-U-12]: GTP-U supports active OAM as a path management message "Echo Request/Response".

A GTP-U tunnel endpoint node sends a Echo Request message to another nodes for keep-alive and received node sends a Echo Response message to sender node as acknowledgment. Echo Request message and Echo Response message are described in section 7.2.1 and section 7.2.2 of [TS.29.281-3GPP] respectively. [TR.29.891-3GPP] recommends not to send Echo Request message more often than 60s on each path.

Supported Extension Headers Notification message indicates a list of supported that tunnel endpoint node can support. This message is sent only in case a tunnel endpoint node receives GTP-U packet with unsupported extension header.

[GTP-U-13]: GTP-U supports tunnel management messages "Error Indication".

GTP-U has Error Indication message to notify that the receiving endpoint discard packets of which no session exist to the sending endpoint. Error Indication message is described in section 7.3.1 of [TS.29.281-3GPP].

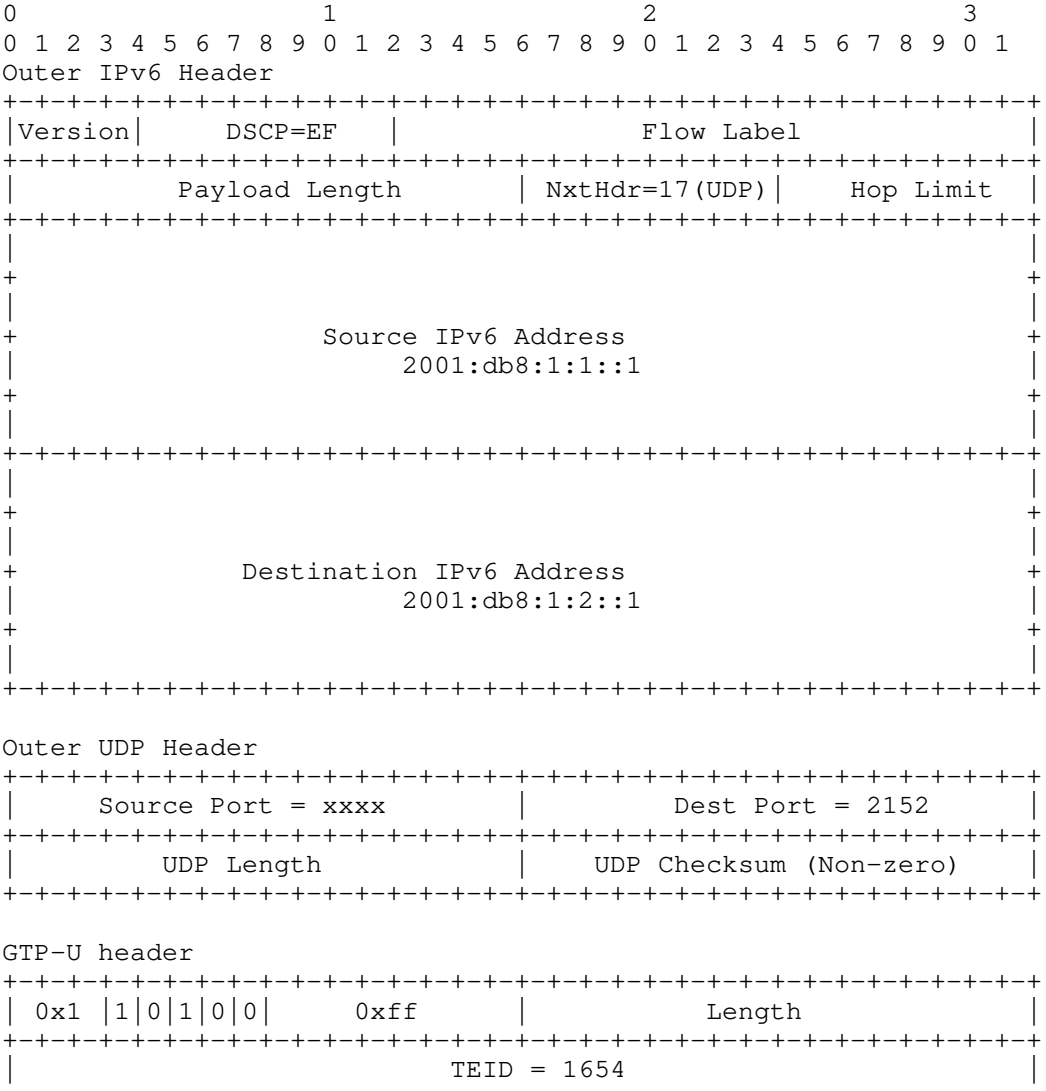
[GTP-U-14]: GTP-U supports tunnel management messages "End Marker".

GTP-U has End Marker message to indicate the end of the payload stream that needs to be sent on a GTP-U tunnel. End Marker message is described in section 7.3.2 of [TS.29.281-3GPP].

3.5. Packet Format

Figure 4 shows a packet format example of GTP-U over IPv6 that carries an extension header for QFI and an IPv6 PDU. All values in the example are illustration purpose only. The encoding of PDU Session Container for QFI refers to [TS.38.415-3GPP].

Outer IPv6 Header's DSCP value(EF) in Figure 4 is marked at sender tunnel endpoint node based on QFI value which is contained in GTP-U Extension Header (PDU Session Container).



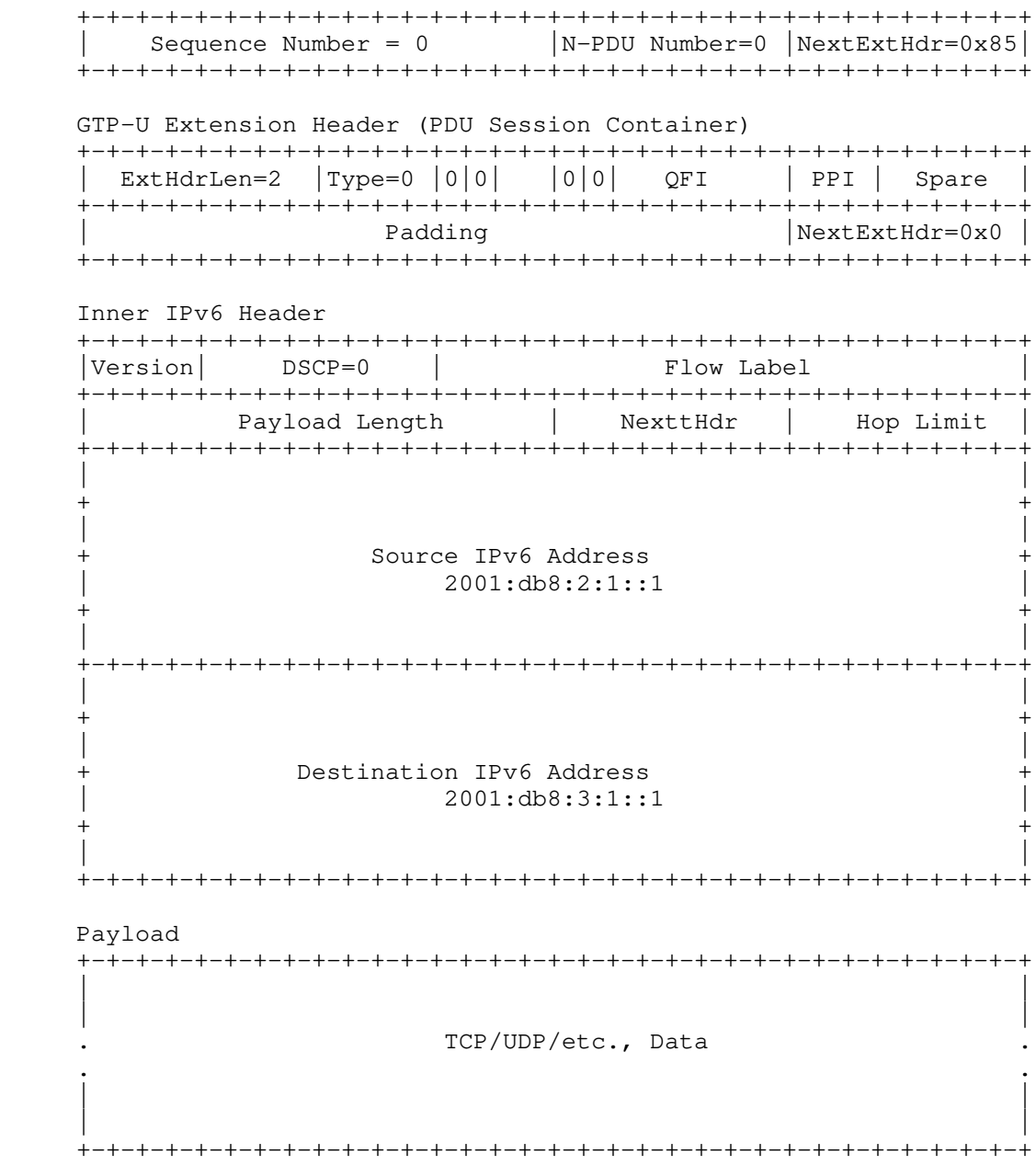


Figure 4: GTP-U Protocol Stack Example

3.6. Observations Summary

[GTP-U-1]: An unidirectional Point-to-Point tunneling protocol.

[GTP-U-2]: Supports Point-to-Multipoint tunneling.

[GTP-U-3]: Supports load balancing by using dynamic UDP port allocation.

[GTP-U-4]: Does not support IPv6 flow label for load balancing in case of IPv6 transport.

[GTP-U-5]: UDP zero checksum is not available in case of IPv6 transport.

[GTP-U-6]: Does not support to response ICMP PTB for Path MTU Discovery.

[GTP-U-7]: Supports sequence number option and sequence number flag in the header, but it is not recommended to be used by almost GTP-U entities.

[GTP-U-8]: Supports carrying QoS Identifiers transparently for Access Networks in extension headers.

[GTP-U-9]: Supports DSCP marking based on the QFI.

[GTP-U-10]: Does not specify the rule for the extension header order.

[GTP-U-11]: Does not support an indication of next-header type.

[GTP-U-12]: Supports active OAM as a path management message "Echo Request/Response".

[GTP-U-13]: Supports tunnel management messages "Error Indication".

[GTP-U-14]: Supports tunnel management messages "End Marker".

4. 5GS Architectural Requirements for User Plane Protocols

4.1. Overview of 5G System Architecture

The 5G system is designed for applying to diverse devices and services due to factors such as the diffusion of IoT devices, and the UP protocol is required to have capabilities for satisfying their requirements.

As a principle of the 5G system, User Plane (UP) functions are separated from the Control Plane (CP) functions for allowing independent scalability, evolution and flexible deployments.

Network slicing is also one of the fundamental concepts of the 5G system, and it provides logical network separation. In terms of user plane, multiple network slices can be comprised of UPFs on top of same physical network resources. Allocated resources and structures may be differentiated among the slices by which the required features or capabilities.

The 3GPP 5G architecture [TS.23.501-3GPP] defines slice types which are eMBB, URLLC and MIoT from Rel-15. In addition to that, V2X slice type is defined from Rel-16.

The architecture overview is shown in Figure 5. The details of functions are described in [TS.23.501-3GPP]. A UPF handles UP paths on N3, N9 and N6 interface, and the setup is controlled by SMF via N4 interface. A UP path will be manipulated based on application requirements for the PDU session corresponding to the path. An SMF is also capable to receive information regarding routing path with API from AF via NEF, PCF, and SMF.

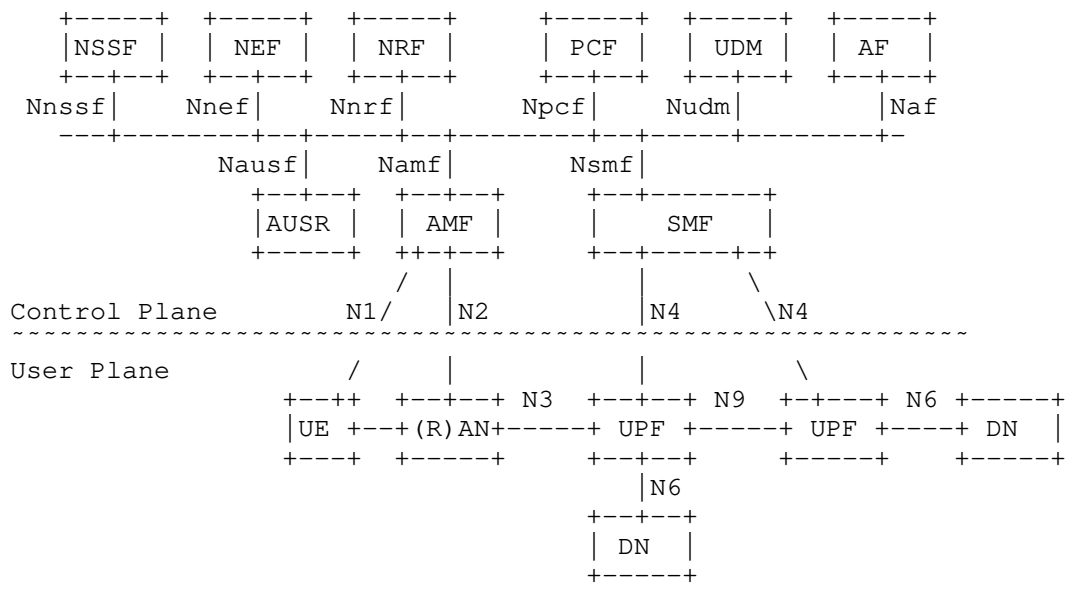


Figure 5: 5GS Architecture and Service-based Interfaces

This document mainly focuses on requirements for N9 interface as relevant to UP protocol of 5G system.

4.1.1. UPF Functionalities

UPF has a role to handle UP traffic, and provides functionalities to look up user data traffic and enforce the appropriate policies to it.

The followings are defined as UPF functionalities defined in the section 6.2.3 of [TS.23.501-3GPP]

- Anchor point for Intra-/Inter-RAT mobility (when applicable).
- External PDU Session point of interconnect to Data Network.
- Packet routing and forwarding (e.g. support of Uplink classifier to route traffic flows to an instance of a data network, support of Branching point to support multi-homed PDU Session).
- Packet inspection (e.g. Application detection based on service data flow template and the optional PFDs received from the SMF in addition).

- User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering).
- Lawful intercept (UP collection).
- Traffic usage reporting.
- QoS handling for user plane, e.g. UL/DL rate enforcement, Reflective QoS marking in DL.
- Uplink Traffic verification (SDF to QoS Flow mapping).
- Transport level packet marking in the uplink and downlink.
- Downlink packet buffering and downlink data notification triggering.
- Sending and forwarding of one or more "end marker" to the source NG-RAN node.
- ARP proxying and / or IPv6 Neighbour Solicitation Proxying for the Ethernet PDUs.
- Packet duplication in downlink direction and elimination in uplink direction in UP protocol layer.
- TSN Translator functionality to hold and forward user plane packets for de-jittering when 5G System is integrated as a bridge with the TSN network.

4.1.2. UP Traffic Detection

The traffic detection is described in the section 5.8.2.4 of [TS.23.501-3GPP]. In 3GPP UP packet forwarding model, UPF detects UP traffic flow which belong to a N4 session configured by SMF.

The protocol of N4 interface, PFCP, brings a set of traffic detection information from SMF to UPF as Packet Detection Information (PDI) in a PDR to establish/modify the N4 PFCP session. It is defined in section 7.5.2.2 of [TS.29.244-3GPP].

Combination of the following information is used for the traffic detection:

- For IPv4 or IPv6 PDU Session type
  - CN tunnel info (Tunnel ID and the endpoint IP address of 5G Core)

    * Network instance

    * QFI

    * IP Packet Filter Set

    * Application Identifier: The Application ID is an index to a set of application detection rules configured in UPF

  o For Ethernet PDU Session type

    * CN tunnel info(Tunnel ID and the endpoint IP address of 5G Core)

    * Network instance

    * QFI

    * Ethernet Packet Filter Set

  It is noted that Network Instance is encoded as Octet String in PFCP, and is NOT appeared in UP packet over the wire. It is expected like an attribute of the receiving IP interface of the UPF. It supports UPF to be able to connect to different IP domains of N3, N9 or N6, which run each independent policy in routing and addressing. The UPF detects traffic flow with Network Instance which the receiving interface attributed to.

  The IP Packet Filter Set and Ethernet Packet Filter Set defined in clause 5.7.6 of [TS.23.501-3GPP] are following:

  o IP Packet Filter Set:

    * Source/destination IP address or IPv6 prefix

    * Source/destination port number

    * Protocol ID of the protocol above IP/Next header type

    * Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.

    * Flow Label (IPv6)

    * Security parameter index

    * Packet filter direction

  o Ethernet Packet Filter Set:

* Source/destination MAC address

* Ethertype as defined in IEEE 802.3

* Customer-VLAN tag(C-TAG) and/or Service-VLAN tag(S-TAG) VID fields as defined in IEEE 802.1Q

* Customer-VLAN tag(C-TAG) and/or Service-VLAN tag(S-TAG) PCP/DEI fields as defined in IEEE 802.1Q

* IP Packet Filter Set, in case Ethertype indicates IPv4/IPv6 payload

* Packet filter direction

4.1.3. User Plane Configuration

User Plane configuration on a UPF is managed by an SMF through PFCP [TS.29.244-3GPP]. The SMF establishes PFCP sessions on the UPF per PDU session basis. The UPF maintains each configured PFCP session states during the sessions exist.

A PFCP session consists of the rules of packet detection, forwarding action, QoS enforcement, usage reporting and buffering action. Figure 6 depicts overview of the PFCP session state structure.

The listed information in Section 4.1.2 indicates packet detection information of packet detection rule for that the rest of related rules within the PFCP session to be derived. All rules are per session unique and no rules are shared with other sessions.

```
PFCP-Session* [F-SEID]
  +- F-SEID(Full Qualified Session Endpoint ID)    uint64
  +- PDU-Session-Type               [IPv4|IPv6|IPv4v6|Ether|Unstrct]
  +- DNN(Data Network Name)
  +- PDR(Packet Detection Rule)* [PDR-ID]
  |  +- PDR-ID    uint16
  |  +- PDI (Packet Detection Information)
  |  |  +- Traffic-Endpoint-ID?   -> Traffic-Endpoint-ID reference
  |  |  +- ....
  |  +- FAR/URR/QER-ID            -> FAR/URR/QER-ID references
  +- FAR(Forwarding Action Rule)* [FAR-ID]
  |  +- FAR-ID                    uint32
  |  +- Forwarding-Parameters
  |  |  +- Network-Instance?        Octet String
  |  |  +- Outer-Header-Creation
  |  |  |  +- Outer-Hdr-Creation-Desc   [GTPoUDP/IPv4|IPv6, etc.,]
```

```
   |  |  |  +- TEID, outer IP-Address for N3/N9
   |  |  |  +- C/S-TAG, UDP Port-number for N6
   |  |  +- Forwarding-Policy-ID?    Octet String
   |  |  +- ....
   |  +- Duplicating-Parameters
   |  |  +- ....
   |  +- BAR-ID?                    -> BAR-ID reference
   +- QER(QoS Enforcement Rule)* [QER-ID]
   |  +- QER-ID                     uint32
   |  +- MBR(Maximum Bit Rate)
   |  |  +- UL/DL-MBR?   bitrate_in_kbps (0..10000000)
   |  +- GBR(Guaranteed Bit Rate)
   |  |  +- UL/DL-GBR?   bitrate_in_kbps (0..10000000)
   |  +- QoS-flow-identifier?       QFI value(6-bits)
   |  +- Reflective-QoS?            boolean
   |  +- Paging-Policy-Indicator?   PPI value(3-bits)
   |  +- ....
   +- URR(Usage Reporting Rule)* [URR-ID]
   |  +- URR-ID                     uint32
   |  +- Measurement-Method, Period, Reporting-Triggers?
   |  +- Volume/Event/Time Threshold, Quota?
   |  +- Quota-Holding-Time?
   |  +- FAR-ID for Quota action?        -> FAR-ID reference
   |  +- ....
   +- BAR(Buffering Action Rule)* [BAR-ID]
   |  +- BAR-ID                     uint8
   |  +- Suggested-Buffering-Packets-Count
   +- Traffic-Endpoint* [Traffic-Endpoint-ID]
      +- Traffic-Endpoint-ID                  uint8
      +- TEID, Tunnle IP Address, UE Address...?
```

Figure 6: User Plane Configuration Model

4.2. Architectural Requirements for User Plane Protocols

This section lists the requirements for the UP protocol on the 5G system. The requirements are picked up from [TS.23.501-3GPP]. In addition, some of service requirements described in [TS.22.261-3GPP] are referred to clarify the originations of architectural requirements.

According to [TS.23.501-3GPP], the specifications potentially have assumptions that the UP protocol is a tunnel representing a single TEID between a pair of UPFs and it is corresponding to a single PDU session. In short, the UP protocol is a tunnel and it is assumed to be managed under per PDU session handling. Also, it should be a stateful tunnel in the UPFs along with the PDU session.

4.2.1. Fundamental Functionalities

The fundamental requirements for UP protocols are described below:

ARCH-Req-1: Supporting IPv4, IPv6, Ethernet and Unstructured PDU

The 5G system defines four types of PDU session as IPv4, IPv6, Ethernet, and Unstructured. Therefore, UP protocol must support to convey all of these PDU session types. This is described in [TS.23.501-3GPP].

Note: In TS 23.501 v15.2.0, IPv4v6 is added as a PDU session type.

ARCH-Req-2: Supporting IP connectivity for N3, N6, and N9 interfaces

The 5G system requires IP connectivity for N3, N6, and N9 interfaces. The IP connectivity is assumed that it comprises of IP routing and L1/L2 transport networks which are outside of 3GPP specifications.

It is desirable that the IP connectivity built on IPv6 networks when it comes to address space for end-to-end user plane coverage. But it is expected to take certain time. During the IPv6 networks are not deployed for all the coverage, UP protocol should support RANs and DNs running on IPv4 transport connect to UPF running on IPv6 transport.

Furthermore, on N6 interface, point-to-point tunneling based on UDP/IPv6 may be used to deliver unstructured PDU type data. Then, the content information of the PDU may be mapped into UDP port number, and the UDP port numbers is pre-configured in the UPF and DN. This is described in the section 9.2 of [TS.29.561-3GPP].

ARCH-Req-3: Supporting deployment of multiple UPFs as anchors for a single PDU session

The 5G system allows to deploy multiple UPFs as anchors for a single PDU session, and supports multihoming of a single PDU session for such anchor UPFs.

Multihoming is provided with Branching Point (BP). BP provides forwarding of UL traffic towards the different PDU Session Anchors based on the source IPv6 prefixes and merge of DL traffic to the UE. IPv6 multihoming only means multiple source IPv6 prefixes are used for a PDU session. It is identical to one classified as scenario 1 in [RFC7157].

Up link classifier (UL CL) is to forward uplink packets to multiple anchor UPFs based on the destination IP of the T-PDU regardless of

the source IP address. Noted that single source IP address/prefix PDU session is not defined as multihoming PDU session in 5GCS even though a PDU session has multiple anchor UPFs.

On UL side, P2P tunnels are established per destination anchor UPFs basis from one UL CL UPF to the anchor UPFs for the PDU session.

On DL side, one single multipoint-to-point (MP2P) tunnel exists from the source anchor UPFs to the destination BP UPF for the PDU session. It means that the paths from the anchor UPFs are merged into just one tunnel state at the destination BP UPF.

Multiple P2P paths on DL could also be used for multihoming. However it should be the multiple PDU sessions multihoming case where the destination gNB or UPF needs to maintain multiple tunnel states under the one PDU session to one UP tunnel architectural principle. It causes increase of load on tunnel states management in UPF due to increment of the anchor UPF for the PDU session.

However, P2P tunneling could increase explosively the number of states in UPF as the anchor UPF/DN incremented to the PDU session. Thereby single PDU session multihoming with MP2P path should be a better option for multihoming in terms of reducing total number of tunnel states.

SSC mode 3 for session continuity in hand-over case uses a single PDU multihoming with BP to make sure make-before-break. It is described in the section 5.6.4 and 5.6.9 of [TS.23.501-3GPP].

Multihoming is also assumed to be used for edge computing scenario. Edge computing enables some services to be hosted close to the UE's access point of attachment, and achieves an efficient service delivery through the reduced end-to-end latency and load on the transport network. In edge computing, local user's traffic is routed or steered to application in the local DN by UPF. This refers the section 5.13 of [TS.23.501-3GPP].

ARCH-Req-4: Supporting flexible UPF selection for PDU

The appropriate UPFs are selected for a PDU session based on parameters and information such as UPF's dynamic load or UE location information. Examples of parameters and information are described in the section 6.3.3 of [TS.23.501-3GPP].

This means that it is possible to make routing on user plane more efficient in the 5GS. For example, in case that UPFs are distributed geographically, decision of the destination UPF based on locations of end hosts (e.g., UE or NF in DN) enables to forward PDUs with a route

connecting between UPFs nearby the hosts directly. This would be useful UE-to-UE or UE-to-local_DN communication, and such usage is described in the section 6.5 of [TS.22.261-3GPP].

The 5GS allows operators to select parameters used for UPF selection. (In other words, any specific schemes on UPF selection are not defined in the current 3GPP documents.)

ARCH-Req-5: No limitation for number of UPFs in a data path

The number of UPF in the data path is not constrained by 3GPP specifications. This specification is described in the section 8.3.1 of [TS.23.501-3GPP].

Putting multiple UPFs, which provides specific function, in a data path enables flexible function deployment to make sure load distribution optimizations, etc.

Meanwhile, each UPF in a data path shall be controlled by an SMF via N4 interface. Thus putting an excess of UPF for data paths might cause increase of load of an SMF. Pragmatically, the number of UPF put in a data path is one or two (e.g., for MEC or roaming cases), and, at most, it would be three (e.g., for case where UE moves during a session).

It is expected that multiple UPFs with per session tunnel handling for a PDU session becomes complicated task more and more for a SMF by increasing number of UPFs.

ARCH-Req-6: Supporting aggregation of multiple QoS Flow indicated with QFI into a PDU Session

Against to the previous generation, 5G enables UPF to multiplex QoS Flows, equivalent with IP-CAN bearers in the previous generation, into one single PDU session. That means that a single tunnel includes multiple QFIs contrast to just one QoS Flow (a bearer) to one tunnel before 5G.

In even the 5GS, each flow is forwarded based on the appropriate QoS rules. QoS rules are configured by SMF as QoS profiles to UP components and these components perform QoS controls to PDUs based on rules. In downlink, a UPF pushes QFI into an extension header, and transmits the PDU to RAN or another UPF. Then, such UPF may perform transport level QoS packet marking (e.g., DSCP marking in the outer header). In uplink, each UE obtains the QoS rule from SMF, and transmit PDUs with QFI containing the QoS rules to the RAN. The following RAN and UPFs perform enforcement of QoS control and charging based on the QFI.

This specification is described in 5.7.1 of [TS.23.501-3GPP].

ARCH-Req-7: Supporting network slicing

The 5GS fundamentally supports network slicing for provision the appropriate end-to-end communication to various services. In the relevant documents (e.g., [TS.23.501-3GPP], [TS.28.530-3GPP]), a network slice is defined as virtual network and it is structured with 5GS NF instances, such as SMF, UPF including IP transport connectivity between RANs and DNS. Each network slice is independent and its user plane (including network functions and links) should be noninteractive against the others.

The 5G architecture specification has been updated with that Network Instance is defined as the glue of network slice between 5G slice and corresponding IP transport slice in addition to the original role of separating IP domains, which is described in Section 4.1.2.

It has been appeared from version 15.2.0 of [TS.23.501-3GPP] in section 5.6.12.

UP underlay transport networks and UPFs may be shared by 5G slices, as described in section 4 of [TS.28.530-3GPP]. The data model defined in [TS.29.510-3GPP] allows that a Network Instance, a UPF and its interfaces can belong to multiple slices as same as other type of NFs. UP endpoint IP prefix/address of an interface can also be shared with multiple interfaces on the UPF as the model doesn’t make them slice unique.

The slice lifecycle managements is described in the relevant documents: [TS.28.531-3GPP], [TS.28.532-3GPP], and [TS.28.533-3GPP].

ARCH-Req-8: End Marker support

The construction of End Marker packets specified in [TS.23.501-3GPP] may either be done in the CP/UP functions for indicating the end of the payload stream on a given UP tunnel. PDU packets arrive after an End Marker message on the tunnel may be silently discarded. For example, End Maker is used for handover procedures, and it can prevent reordering of arriving packets due to switch of anchor UPFs.

4.2.2. Supporting 5G Services

In the release 16 [TS.23.501-3GPP], some specifications have been added to support 5G specific services and communications. This section describes overviews of the specifications relevant to use plane functionalities.

ARCHI-Req-9: URLLC Support

The 5GS supports Ultra-Reliable Low Latency Communication (URLLC) for mission critical applications. The User Plane features are described below.

o Redundant UP transmission for URLLC

The 5G is expected to support services which are latency sensitive and require high reliability. Communication to realize such services is called Ultra-Reliable and Low-Latency Communication or URLLC. In URLLC, redundancy of QoS flows is required for providing highly reliable communication. For instance, a set of UP NFs (e.g., UPF or gNB) and interfaces between UE and DN are redundant, and packets are replicated and forwarded via each route. UEs and DN support dual connectivity and drop duplicated received packets. The scheme of packet dropping at UE is out of responsibility of 3GPP. The overview is shown in Figure 7.

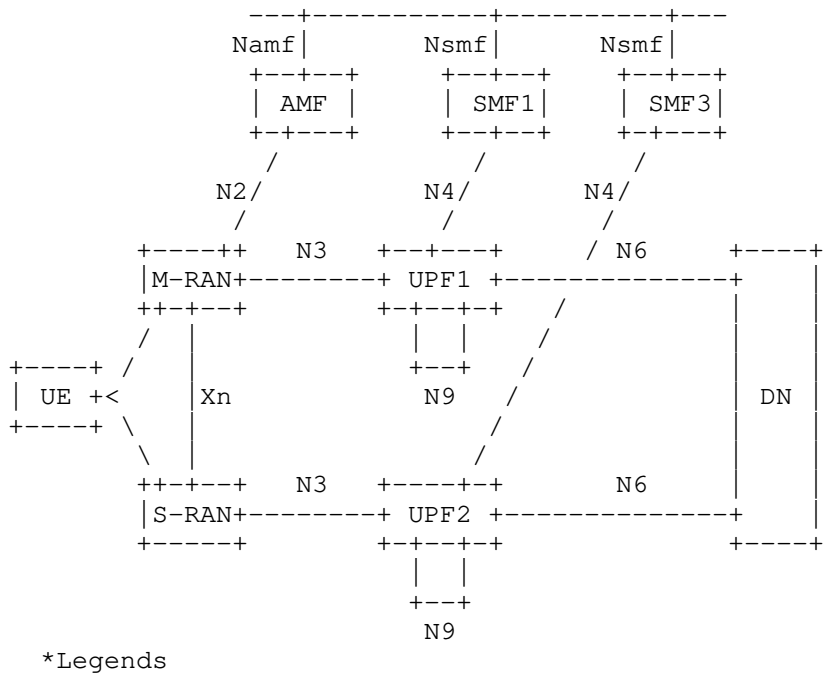


Figure 7: Redundant UP paths using dual connectivity

Otherwise, in case that RAN nodes and UPFs have enough reliability and they are not redundant by dual devices, reliable connectivity of QoS flows is provided by dual N3 tunnels between RAN and UPFs. Such tunnels are treated as individual ones, but they have the same sequence number. UP NFs identifies the duplication of PDU packets based on sequence number content in the UP tunnel headers. For uplink packets, a RAN node replicates each packet from a UE. An anchor UPF receives the duplicated packets, and drops ones which reach later in each duplicated packet pare. On the other hand, for downlink packets, a UPF replicates packets received from DN, and a RAN node drops the duplicated packets as well. The overviews of the ways are shown in Figure 8.

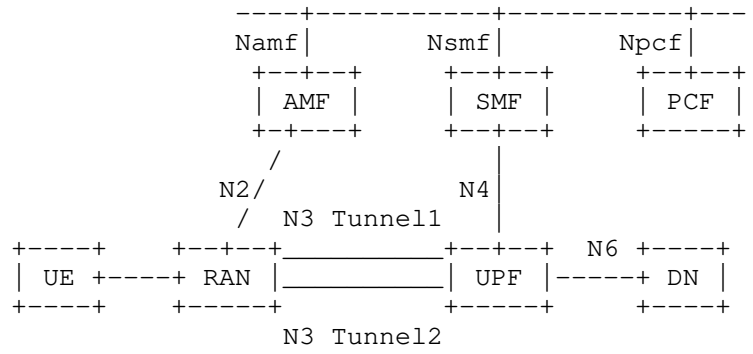


Figure 8: Redundant UP transmission with two N3 tunnels

In addition, there is a case that two intermediate UPFs (I-UPFs) between anchor UPF and RAN are used to support the redundant transmission based on two N3 and N9 tunnels between single anchor UPF and RAN node. The RAN node and anchor UPF support the packet replication and dropping of duplicated packets as described above. As described above, anchor UPF and RAN node detect packet duplication with sequence number of UP tunnels, and thus I-UPFs would forward the packets with the same sequence number on N3 and N9 tunnels. The overview is shown in Figure 9.

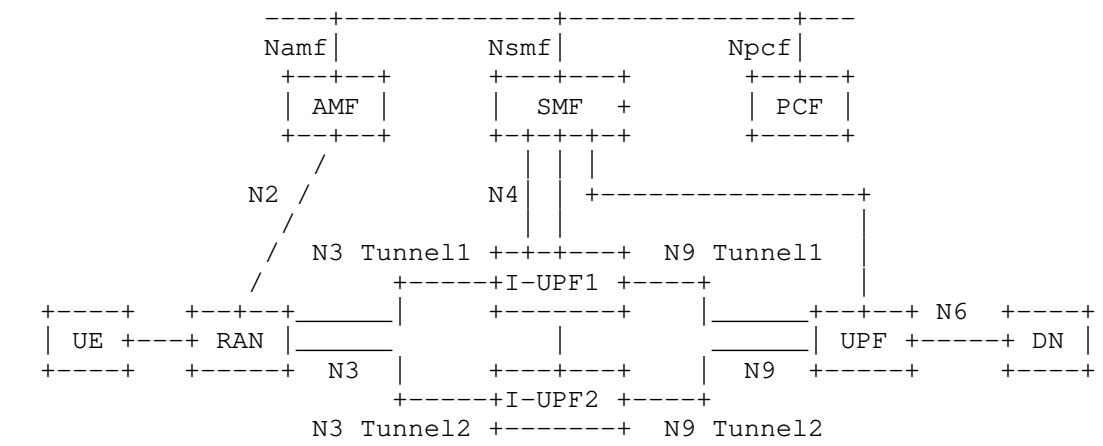


Figure 9: Redundant UP transmission with two I-UPF and N3/N9 tunnels

o Supporting QoS Monitoring for URLLC

QoS monitoring is also required for URLLC. It means that the user plane should be able to measure packet delay between anchor UPF and UE. The measurement would be in various granularities, in the basis of per QoS Flow per UE, or per UP path for example.

To help the measurement at anchor UPF and RAN, UP protocol requires to have capability to convey necessary information to do that; such as time information at sending or reception of a measurement packet. That information should exist in per F-TEID and QFI basis which indicates QoS Flow of the packet. UP protocol should also be able to indicate which packets include the corresponding information for each measurement.

The QoS monitoring requirement has been appeared in section 5.33.3 of [TS.23.501-3GPP] from Rel-16, version 16.2.0.

ARCHI-Req-10: Time Sensitive Communication Support

The 5GS supports Time Sensitive Communications (TSC) for realtime applications, and it can be integrated transparently as a bridge in an IEEE 802.1 TSN network. For TSN time synchronization, the E2E 5GS can be considered as a "time-aware system (ref [IEEE-Std-802.1AS])". The TSN Translators (TTs) at the edges of the 5GS need to support the [IEEE-Std-802.1AS] operations. For instance, UE, gNB, NW-TT (Network-side TSN Translator) and DS-TTs (Device-side TSN Translators) are synchronized with the Grandmaster (GM) located in the 5GS. In addition, the TTs fulfill some functions related to [IEEE-Std-802.1AS] (e.g., gPTP support, timestamping, rateRatio,

etc.). An overview of the 5G and TSN GM clock distribution model via the 5GS is shown in Figure 10.

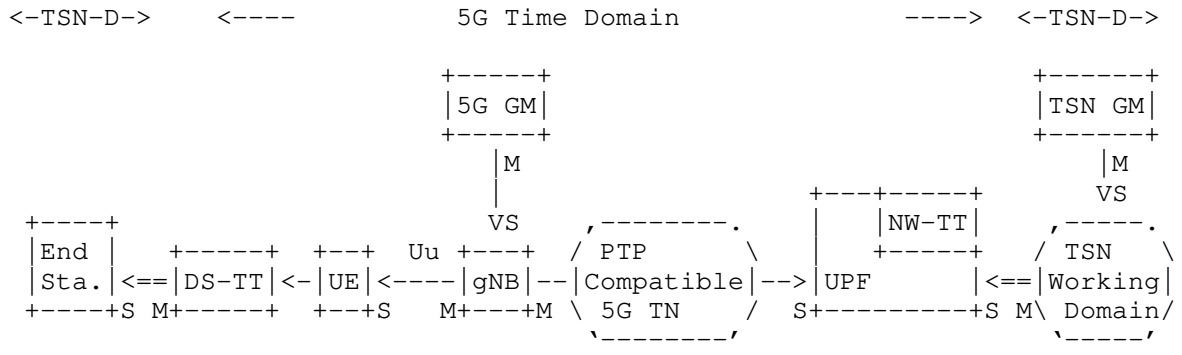


Figure 10: An overview of the 5G and TSN GM clock distribution model

In this model, two independent synchronizations are processing, and gNB only needs to be synchronized to the 5G GM clock. To enable TSN domain synchronization, the 5GS calculates and adds the measured residence time between the DS-TT and NW-TT into the Correction Field (CF) of the synchronization packet of the TSN working domain. The details are described in section 5.27 in [TS.23.501-3GPP].

From this feature, UP functions and protocol are needed to support TSN specified in [IEEE-Std-802.1AS] .

ARCHI-Req-11: Cellular IoT Support

For supporting Cellular IoT (CIoT) (ref. [TS.22.261-3GPP]), optimizations of functionalities of the 5GS is needed. CIoT is in earlier 3GPP release also referred to as Machine Type Communication (MTC). Some of CIoT functionalities relevant to user plane are described in this section. The details of CIoT support is described in section 5.31 in [TS.23.501-3GPP].

o Non-IP Data Delivery (NIDD)

The 5GS may support Non-IP Data Delivery (NIDD) to handle Mobile Originated (MO) and Mobile Terminated (MT) communication for unstructured data. Thus, User Plane Protocol should be conveyable such unstructured data units.

o Reliable Data Service (RDS)

Reliable Data Service (RDS) may be used for a PDU session of unstructured type. The service provides a mechanism for the NEF or UPF to determine if the data was successfully delivered to the UE and for the UE to determine if the data was successfully delivered to the NEF or UPF.

When the service is enabled, a protocol that uses a packet header to identify the requested acknowledgement from peered end-point may be used between end-points of the PDU session. In addition, port numbers in the header are used to identify the applications on the originator and receiver. The UE, NEF and the UPF may support reservation of the source and destination port numbers for their use and subsequent release of the reserved port numbers.

Therefore, UP protocol is required to have fields for containing information to determine normality of unstructured PDU sessions and used applications.

o High Latency Communication

Functions for High Latency Communication may be used to handle mobile terminated (MT) communication with UEs being unreachable while using power saving functions. "High latency" refers to the initial response time before normal exchange of packets is established. High latency communication is supported by extended buffering of downlink data in the UPF, SMF or NEF when a UE is using power saving functions in CM-IDL state and the UE is not reachable.

o Small Data Rate Control

The SMF may apply Small Data Rate Control for PDU sessions based on, for example, operator policy, DNN, S-NSSAI, RAT type etc. The rate control may indicate following parameters in each of uplink and downlink.

- an integer number of packets per time unit

- an integer number of additional allowed exception report packets per time unit once the rate control limit has been reached

The UE shall comply with this uplink rate control instruction. If the UE exceeds the uplink number of packet per time, the UE may still send uplink exception report if allowed and the number exception reports per time unit has not been exceeded.

For the UPF and NEF, Small Data Rate Control is based on a maximum allowed rate per direction. The UPF or NEF may enforce the uplink rate by discarding or delaying packets that exceed the maximum allowed rate. The UPF or NEF shall enforce the downlink rate by discarding or delaying packets that exceed the downlink part of the maximum allowed rate.

- User Plane CIoT 5GS Optimisation

User Plane CIoT 5GS Optimization enables transfer of user plane data from CM-IDLE without the need for using the Service Request procedure by negotiation between UE and AMF in advance. In case that there are many devices being CM-IDLE state for long time, it would be better that User Plane Protocol i s session less.

5. Evaluation Aspects

This section provides UP protocol evaluation aspects that are mainly we derived from the architectural requirements described in Section 4. Those aspects are not prioritized by the order here. Expected deployment scenarios explain the evaluations purpose in the corresponding aspects.

As we were noticed that the gaps between GTP-U specifications and 5G architectural requirements through the analysis, those each gap are briefly described in the evaluation aspect associated to it.

Since it is obvious that 5G system should be able to interwork with existing previous generation based systems, any aspects from coexisting and interworking point of view are not particularly articulated here. It may be described in a next version.

5.1. Supporting PDU Session Type Variations

Given that UP protocol is required to support all PDU session types: IPv4, IPv6, Ethernet, and Unstructured. However, it is expected that some deployment cases allow candidate protocol to adopt only one or few PDU session type(s) for simplicity of operations. As we can expect that IPv4 connectivity services will be available through IPv6-only PDU session that enabled by bunch of IPv6 transition solutions already available in the field.

For this, the expected evaluation points from this aspect should be whether there is substitutional means to cover other PDU session types. And how much it makes simple the system than deploying original PDU session types.

5.2. Nature of Data Path

As it is described in Section 4.2, the single PDU session multi-homing case requires multipoint-to-point (MP2P) data path. It should be much scalable than multi-homing with multiple PDU sessions because number of required path states in the UPFs are reduced as closed to egress endpoint. Against that point-to-point (P2P) protocol requires same number of states in each UPF throughout the path, and it could increase explosively the load on management of tunnel states.

From this point of view, the expected evaluation points from this aspect is whether the nature of candidate UP protocols are to utilize MP2P data path. Supporting MP2P data path by GTP-U could be a gap since GTP-U is a point-to-point tunneling protocol as it is described in Section 3.

Noted that 3GPP CT WG4 pointed out GTP-U was already required to allow one single tunnel endpoint to receive packets from multiple source endpoints ([C4-185491-3GPP]). It was an architectural requirement of 3GPP system from a previous generation. It means that MP2P data path requirement for UP protocol has been existed before the 5G system.

5.3. Supporting Transport Variations

The 5G system will be expected that the new radio spectrums in high frequency bands require operators to deploy their base stations much dense for much wider areas compare to previous generation footprints. To make sure that density and coverage, all available types of transport in the field must be employed between RAN to UPF, or UPF to UPF.

It is also expected that MTU size of each transport could be varied. Because one could be own fiber which the operator configure the MTU size as they like while others are third-party provided L2/L3 VPN lines which MTU size can’t be controlled by the operators.

The MTU between RAN and UPF can be discovered by offline means and the operator takes into account the MTU that is transferable on the radio interface and based on this the operator configures the right MTU to be used. That is then signaled to the UE either via PCO (for IPv4 case) or the IPv6 RA message (for IPv6 case).

In addition, for cases that third-parties provide VPN lines, it would be recommended MTU size discovery for each data path and dynamic MTU size adjustment mechanisms, while GTP-U does not support those mechanisms.

As the study item in 3GPP mentioned, IPv6 is preferable address family not only for UEs, but also for the UP transport, in terms of size of available address space to support dense and wide footprint of base stations. However it increases header size from 20bytes to 40bytes compare to IPv4. It could be a problem if the MTU size is uncontrollable, or only limited MTU size available to carry committed PDU size on the user plane.

The expected evaluation points from this aspect should be that the candidate protocols are able to dynamically adjust path MTU size with appropriate MTU size discovery mechanism. It also should be that how the candidate protocols leverage IPv6 to deal with header size increasing.

5.4. Data Path Management

As Section 4.2 described, the 5G systems allows user plane that flexible UPF selection, multiple anchor UPFs, and no limit on how many UPFs chained for the data path of the PDU session. UPF deployments in the field will thereby be distributed to be able to optimize the data path based on various logics and service scenarios.

That powerful user plane capability could make data path management through the control plane, or operation support systems (OSS) be complicated and difficult. Perhaps it could be the case where the UP protocol nature is P2P and it only supports per session base data path handling. Therefore it would be better that UP protocol could support to aggregate several PDU sessions into a tunnel or shall be a session-less tunnel.

Because it increases data path states by number of sessions, and number of endpoints of UPFs that makes data path handling much hectic and the control plane tend to be overloaded by not only usual attach/detach/hand-over operations, but also existing session manipulation triggered by UPF and transport nodes/paths restoration, etc.,

The expected evaluation points from this aspect should be that how much the candidate protocols can reduce data path management loads both on the control plane NFs and UPFs compare to the per session based handling for P2P paths. It could possibly include N3 and N6 in addition to N9 while it supports flexible user plane data path optimizations for some example scenarios.

5.5. QoS Control

The QoS model is based on QoS flows to which QFI indicates in the 5G system that allows multiple QoS flows are aggregated into a single PDU session. So that it is given that the UP protocol should convey QFIs for a PDU session and the UPF needs to lookup them. It makes sure that reflects QoS policy in the 5G system to corresponding forwarding policy in the user plane IP transports.

The expected evaluation points from this aspect should be whether the candidate protocols can provide stable ID space for QFI which shouldn't be a big deal since QFI just requires 6-bits space.

As we pointed out in Section 3.2, the lookup process could impact UPF performance if the QFI container position in the header is unpredictable. It could happen many times along the path because the each UPFs should do it again and again in case that various different QoS policies are deployed in the networks under the UP as we discussed in Section 5.3.

As [TS.29.281-3GPP] updated in version 15.3.0, it is recommended that the first extension header is the PDU session container in which QFI is present.

5.6. Traffic Detection and Flow Handling

As described in Section 4.1.1, UPF need to detect traffic flow specified by SMF within a PDU session, and enforce some processes to the PDU based on the pre-configured policy rule.

As similar with QoS flow lookup described in Section 5.5, UPFs along the path are repeatedly detecting an specified traffic flow in inner PDU. It could increase redundant flow detection load on every UPFs that could be avoided if the upstream UPF put some identifier which abstracts the detected flow into the packets. It enables following UPFs just find the ID to detect the indicated flow from the packet.

The expected evaluation points from this aspect should be whether the candidate protocols can provide means to reduce that redundant flow detection that could be enough bits space on stable ID space to put abstracted detected flow identifier.

5.7. Supporting Network Slicing Diversity

Network Instance has been defined as the glue of network slice between 5G and IP transport in addition to IP domain separation, as described in Section 4.1.2. It is expected that SMF is able to configure UPF to send UP packet to corresponding transport slice by

indicating Network Instance in FAR so that UPF can determine outgoing interface for the UP packet.

It is assumed that IP transport networks are Network Instance agnostic, i.e., transport slices are independently instantiated and not bound to specific IP address space in the 5GC, for preventing increase of routing table size.

As a transport slice may be shared with multiple IP domains, Network Instance could be instantiated for all combination of IP domains and transport slice. To indicate those combination in UP packet over the wire, the 5G architecture expects VPN solutions as described in section 5.6.12 of [TS.23.501-3GPP].

Binding Network Instance with corresponding VPN would be varied per VPN solutions and FAR is not able to do. Hence it is out of scope of 3GPP and it may be covered by IETF, or other SDOs.

Apart from binding, if it is the case where MPLS based VPNs, such as [RFC4364] and [RFC4664] are expected as the existing VPN solution which bound to Network Instance, there are some avaiable deployment options, such as 1). PE router integrates UPF, 2). CE router integrates UPF, 3). UPF connects to the VPN behind the CE router.

Option 1 could work since all legacy MPLS or Segment Routing [RFC8402] based solution are available for both VPN and transport slicing at the UPF integrated PE router. However it is hard to expect it in multi-vendor deployment case, where the PE routers providing vendor is different from the vendor who provides UPFs, for example.

Option 2 and 3 are expected as IP domain separation, but it is hard to see that it is able to indicate transport slice in addition to the IP domain. Other L2 and tunneling solutions should be same with those options.

The expected evaluation points from this aspect should be whether the candidate protocols can contain forwarding information associated to the assigned IP domain and transport slice for all possible deployment cases.

5.8. Reliable Communication support

As Section 4.2 described, more than two UP paths are required for a QoS flow of a PDU session between the anchor UPF and gNB. Those UP paths are to convey redundant duplicated packets.

To support reliable communication with above requirements, UPF and gNB must replicate the sending UP packets and eliminate the received duplicated UP packets. Not to mention that UP protocol should be able to make sure that the paths are not in fate sharing, the UP packet must have sequence number to indicate duplicate packets per QoS flow basis.

The expected evaluation points from this aspect should be whether the candidate protocols can indicate packet sequence and diversed paths in the context of QoS flow, not in UP tunnel context. The packet sequence information should be transparent through I-UPF(s) exist in the middle of the path even in case that the UP tunnels are terminated at the I-UPF(s).

6. Conclusion

We analyzed the 3GPP specifications of the 5G architecture in terms of user plane and the current protocol adopted to the user plane. After the analysis work, we believe that the results described in this document shows that we reach at certain level of understanding on the 5G systems and ready to provide our inputs to 3GPP.

We clarified GTP-U through the analysis and listed observed characteristics in Section 3.6. We also clarified the architectural requirements for UP protocol described in Section 4.2.

Our conclusion here is that it is hopefull if the evaluation aspects described in Section 5 help for the study progress. It is worth to study possible candidate UP protocols for the 5G system including current one based from the aspects.

7. Security Consideration

TBD

8. Acknowledgement

The authors would like to thank Tom Herbert, Takashi Ito, John Leddy, Pablo Camarillo, Daisuke Yokota, Satoshi Watanabe, Koji Tsubouchi and Miya Kohno for their detailed reviews, comments, and contributions.

A special thank you goes to Arashmid Akhavain for his technical review and feedback.

Lastly, the authors would like to thank 3GPP CT WG4 folks for their review and feedback.

9. Informative References

[C4-185491-3GPP]
3rd Generation Partnership Project (3GPP), "LS OUT on User Plane Analysis", July 2018, <http://www.3gpp.org/ftp/tsg_ct/WG4_protocollars_ex-CN4/TSGCT4_85bis_Sophia_Antipolis/Docs/C4-185491.zip>.

[CP-173160-3GPP]
3rd Generation Partnership Project (3GPP), "New Study Item on User Plane Protocol in 5GC", December 2017, <http://www.3gpp.org/ftp/tsg_ct/TSG_CT/TSGC_78_Lisbon/Docs/CP-173160.zip>.

[CP-180116-3GPP]
3rd Generation Partnership Project (3GPP), "LS on user plane protocol study", March 2018, <http://www.3gpp.org/ftp/tsg_ct/TSG_CT/TSGC_79_Chennai/Docs/CP-180116.zip>.

[IAB-Statement]
Internet Architecture Board (IAB), "IAB Statement on IPv6", November 2016, <https://www.iab.org/2016/11/07/iab-statement-on-ipv6/>.

[IEEE-Std-802.1AS]
Institute of Electrical and Electronics Engineers (IEEE), "Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks", March 2011, <https://www.ieee802.org/1/pages/802.1as.html>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <https://www.rfc-editor.org/info/rfc2460>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, DOI 10.17487/RFC4664, September 2006, <https://www.rfc-editor.org/info/rfc4664>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011, <https://www.rfc-editor.org/info/rfc6437>.

[RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, DOI 10.17487/RFC6438, November 2011, <https://www.rfc-editor.org/info/rfc6438>.

[RFC6935] Eubanks, M., Chimento, P., and M. Westerlund, "IPv6 and UDP Checksums for Tunneled Packets", RFC 6935, DOI 10.17487/RFC6935, April 2013, <https://www.rfc-editor.org/info/rfc6935>.

[RFC7157] Troan, O., Ed., Miles, D., Matsushima, S., Okimoto, T., and D. Wing, "IPv6 Multihoming without Network Address Translation", RFC 7157, DOI 10.17487/RFC7157, March 2014, <https://www.rfc-editor.org/info/rfc7157>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[TR.29.891-3GPP] 3rd Generation Partnership Project (3GPP), "3GPP TR 29.891 (V15.0.0): 5G System Phase 1, CT WG4 Aspects", December 2017, <http://www.3gpp.org/FTP/Specs/2017-12/Rel-15/29_series/29891-f00.zip>.

[TS.22.261-3GPP] 3rd Generation Partnership Project (3GPP), "3GPP TS 22.261 (V15.7.0): Service requirements for 5G system stage 1", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/22_series/22261-f70.zip>.

[TS.23.060-3GPP] 3rd Generation Partnership Project (3GPP), "3GPP TS 23.060 (V15.3.0): General Packet Radio Service (GPRS); Service description; Stage 2", June 2018, <http://www.3gpp.org/ftp//Specs/archive/23_series/23.060/23060-f30.zip>.

[TS.23.501-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 23.501 (V16.2.0): System Architecture for 5G System; Stage 2", September 2019, <http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/23501-g20.zip>.

[TS.23.502-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 23.502 (V15.4.0): Procedures for 5G System; Stage 2", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/23_series/23502-f40.zip>.

[TS.23.503-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 23.503 (V15.4.0): Policy and Charging Control System for 5G Framework; Stage 2", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/23_series/23503-f40.zip>.

[TS.28.530-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 28.530 (V15.1.0): Management and orchestration of networks and network slicing; Concepts, use cases and requirements (work in progress)", December 2018, <http://ftp.3gpp.org//Specs/archive/28_series/28.530/28530-f10.zip>.

[TS.28.531-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 28.531 (V15.1.0): Management and orchestration of networks and network slicing; Provisioning; Stage 1 (Release 15)", December 2018, <http://ftp.3gpp.org//Specs/archive/28_series/28.531/28531-f10.zip>.

[TS.28.532-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 28.532 (V15.1.0): Management and orchestration of networks and network slicing; Provisioning; Stage 2 and stage 3 (Release 15)", Decempber 2018, <http://www.3gpp.org/ftp//Specs/archive/28_series/28.532/28532-f10.zip>.

[TS.28.533-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 28.533 (V15.1.0): Management and orchestration of networks and network slicing; Management and orchestration architecture (Release 15)", December 2018, <http://www.3gpp.org/ftp//Specs/archive/28_series/28.533/28533-f10.zip>.

[TS.29.244-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 29.244 (V15.1.0): Interface between the Control Plane and the User Plane Nodes; Stage 3", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/29_series/29244-f40.zip>.

[TS.29.274-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 29.274 (V15.4.0): 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3", June 2018, <http://www.3gpp.org/ftp//Specs/archive/29_series/29.274/29274-f40.zip>.

[TS.29.281-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 29.281 (V16.1.0): GPRS Tunneling Protocol User Plane (GTPv1-U)", September 2020, <https://www.3gpp.org/ftp//Specs/archive/29_series/29.281/29281-g10.zip>.

[TS.29.510-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 29.510 (V15.2.0): 5G System; Network Function Repository Services; Stage 3", December 2018, <http://www.3gpp.org/FTP/Specs/2018-06/Rel-15/29_series/29510-f20.zip>.

[TS.29.561-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 29.561 (V15.1.0): 5G System; Interworking between 5G Network and external Data Networks; Stage 3", September 2018, <http://www.3gpp.org/FTP/Specs/2018-06/Rel-15/29_series/29561-f10.zip>.

[TS.38.300-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 38.300 (v15.4.0): NR and NG-RAN Overall Description; Stage 2", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/38_series/38300-f40.zip>.

[TS.38.401-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 38.401 (v15.4.0): NG-RAN; Architecture Description", December 2018, <http://www.3gpp.org/FTP/Specs/2018-03/Rel-15/38_series/38401-f40.zip>.

[TS.38.415-3GPP]
3rd Generation Partnership Project (3GPP), "3GPP TS 38.415 (v16.2.0): NG-RAN; PDU Session User Plane protocol", October 2020, <https://www.3gpp.org/ftp//Specs/archive/38_series/38.415/38415-g20.zip>.

Authors' Addresses

Shunsuke Homma
NTT

Email: homma.shunsuke@lab.ntt.co.jp

Takuya Miyasaka
KDDI Research

Email: ta-miyasaka@kddi-research.jp

Satoru Matsushima
SoftBank

Email: satoru.matsushima@g.softbank.co.jp

Daniel Voyer
Bell Canada

Email: daniel.voyer@bell.ca

DMM Working Group
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

M. Kohno
F. Clad
P. Camarillo
Z. Ali
Cisco Systems, Inc.

November 2, 2020

Architecture Discussion on SRv6 Mobile User plane
draft-kohno-dmm-srv6mob-arch-03

Abstract

This document discusses a solution approach and its architectural benefits of common data plane across domains and across overlay/ underlay.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2021.

Table of Contents

1. Introduction

Mobile architectures have evolved individually, and the user plane, GTP-U, has been defined as an overlay tunnel that is agnostic to the IP infrastructure.

However, it will not be able to efficiently meet the diverse SLA requirements of the 5G era. Also, it will not be able to meet the demands of new mobile first and/or data intensive applications.

This document discusses a solution approach and its architectural benefits of common data plane across domains (e.g., mobile including UE, IP transport, data center, applications) and across overlay/ underlay.

This approach is in a sense contrary to proposals that the underlying transport can be anything (L2, IPv4, IPv6, MPLS, SR, SRv6). But it is an approach to make the network as flat as possible, making it suitable for the distributed mobile deployment model.

2. Problem Definition

The current mobile user plane, GTP-U, defined as an overlay tunnel that is agnostic to the IP infrastructure, has the following limitations that prevent it from supporting new application demands.

- Non-optimal for any-to-any communication
- lack a way to map to the underlay

- o Non-optimal for edge/distributed computing
- o Lack a way for application developers to manipulate

In addition, the centralized tunnel terminating gateway becomes a scaling bottleneck and a single point of failure

For IP and data center networking, tunnel sessions can be eliminated when necessary and if possible (e.g. PPPoE -> IPoE, VXLAN/GENEVE/NSH -> SRv6), but such an architectural change used to be difficult for mobile domain.

3. Common data plane across domains and across overlay/underlay

[I-D.ietf-dmm-srv6-mobile-uplane] defines SRv6 mobile user plane as an alternative or co-existing solution to GTP-U.

Since SRv6 is a native IPv6 data plane, it can be a common data plane regardless of the domain.

SRv6 Network Programming [I-D.ietf-spring-srv6-network-programming] enables the creation of overlays with underlay optimization. In addition, SRv6 can be operated by application developers because of its implementation in the computing stack, e.g. VPP, Linux Kernel, smart NIC.

Data plane commonality offers significant advantage regarding function, scaling, and cost. In particular, the benefits of the 5G era are shown in Section 5.

Note that the interaction with underlay infrastructure is not a mandatory in the data plane commonality. It just gives a design option to interact with the underlay and optimize it, and it is totally fine to keep ovelray underlay-agnostic.

4. Terminology

The terminology used in this document leverages and conforms to [I-D.ietf-dmm-srv6-mobile-uplane].

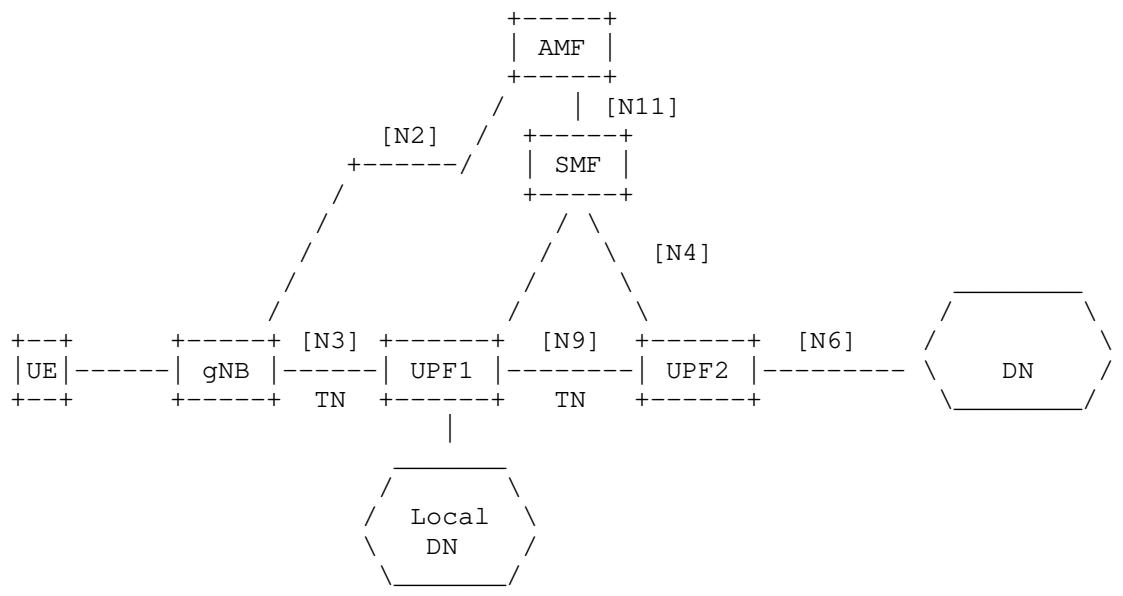


Figure 1: Reference Architecture

- UE : User Equipment
- gNB : gNodeB
- UPF : User Plane Function
- SMF : Session Management Function
- AMF : Access and Mobility Management Function
- 3GPP data plane entities : 3GPP entities responsible for data plane forwarding, i.e. gNB and UPF
- TN : Transport Network - IP network where 3GPP data plane entities connected
- DN : Data Network e.g. operator services, Internet access
- CUPS : Control Plane and User Plane Separation
- VNF : Virtual Network Function
- CNF : Cloud native Network Function

5. SRv6 mobile user plane and the 5G use cases

This section describes the advantages of the common data plane and of applying SRv6 mobile user plane for 5G use cases.

5.1. Network Slicing

Network slicing enables network segmentation, isolation, and SLA differentiation in terms of latency and availability. End-to-end

slicing will be achieved by mapping and coordinating IP network slicing, RAN and mobile packet core slicing.

However, as pointed out in [I-D.clt-dmm-tn-aware-mobility], the 5G System as defined, does not have underlying IP network awareness, which could lead to the inability in meeting SLAs.

Segment Routing has a comprehensive set of slice engineering technologies. How to build network slicing using the Segment Routing based technology is described in [I-D.ali-spring-network-slicing-building-blocks].

In the typical GTP-U over IP/MPLS/SR configuration, 3GPP data plane entity such as UPF is a CE to the transport networks PE. But if 3GPP they support SRv6 mobile user plane, they can directly participate in network slicing, and efficiently solves the following issues.

- o A certain Extra ID such as VLAN-ID is needed for segregating traffic and mapping it onto a designated slice.
- o PE and the PE-CE connection is a single point of failure, so some form of PE redundancy (using routing protocols, MC-LAG, etc.) is required.

And In some deployment scenarios, it may be better to have a transport network PE present. For such a case, the stateless slice identifier encoding [I-D.filsfils-spring-srv6-stateless-slice-id] can be applicable to enable per-slice forwarding policy using the IPv6 header.

5.2. Edge Computing

Edge computing, where the computing workload is placed closer to users, is recognized as one of the key pillars to meet 5G's demanding key performance indicators (KPIs), especially with regard to low latency and bandwidth efficiency. The computing workload includes network services, security, analytics, content cache and various applications. (UPF can also be viewed as a distributed network service function.)

Edge computing is more important than ever. This is because no matter how much 5G improves access speeds, it won't improve end-to-end throughput because it's largely bound to round trip delay.

However, the current MEC discussion [ETSI-MEC] focuses on how to properly select the UPF of adequate proximity, and not on how to interact with applications.

SRv6 has an advantage in enabling edge computing for the following reasons.

- Programmable and Flexible Traffic Steering : SRv6's flexible traffic steering capabilities and the network programming concept is suitable for flexible placement of computing workload.
- Common data plane across domains : SRv6/IPv6 can be a common data plane regardless of the domains such as mobile including UE, IP transport, data center, applications.
- Stateless Service Chaining : It does not require any per-flow state in network fabric.
- Interaction with Applications : SRv6 can be implemented in the compute stack and can be manipulated by applications using socket API. Also, SRv6 can carry meta data, which can be used for interacting with applications.
- Functionality without performance degradation : Various information can be exposed in IP header, but it does not degrade performance thanks to the longest match mechanism in the IP routing. Only who needs the information for granular processing are to lookup.

It is even more beneficial if service functions/applications directly support SRv6.

5.3. URLLC (Ultra-Reliable Low-Latency Communication) support

3GPP [TR.23725] investigates the key issues for meeting the URLLC requirements on latency, jitter and reliability in the 5G System. The solutions provided in the document are focused at improving the overlay protocol (GTP-U) and limits to provide a few hints into how to map such tight-SLA into the transport network. These hints are based on static configuration or static mapping for steering the overlay packet into the right transport SLA. Such solutions do not scale and hinder network economics.

Some of the issues can be solved more simply without GTP-U tunnel. SRv6 mobile user plane can exposes session and QoS flow information in IP header as discussed in the previous section. This would make routing and forwarding path optimized for URLLC, much simpler than the case with GTP-U tunnel.

Another issue that deserves special mention is the ultra-reliability issue. In 3GPP, in order to support ultra-reliability, redundant user planes paths based on dual connectivity has been proposed. The proposal has two main options.

- Dual Connectivity based end-to-end Redundant User Plane Paths
- Support of redundant transmission on N3/N9 interfaces

In the case of the former, UE and hosts have RHF(Redundancy Handling Function). In sending, RFH is to replicate the traffic onto two GTP-U tunnels, and in receiving, RHF is to merge the traffic.

In the case of the latter, the 3GPP data plane entities are to replicate and merge the packets with the same sequence for specific QoS flow, which requires further enhancements.

SRv6 mobile user plane has some advantages for URLLC traffic. First, it can be used to enforce a low-latency path in the network by means of scalable Traffic Engineering. Additionally, SRv6 provides an automated reliability protection mechanism known as TI-LFA, which is a sub-50ms FRR mechanism that provides protection regardless of the topology through the optimal backup path. It can be provisioned slice-aware.

With the case that dual live-live path is required, the problem is not only the complexity but that the replication point and the merging point would be the single point of failure. The SRv6 mobile user plane also has an advantage in this respect, because any endpoints or 3GPP data plane nodes themselves can be the replication/merging point when they are SRv6 aware.

Furthermore, SRv6 supports inband telemetry/time stamping for latency monitoring and control.

6. Control Plane Considerations

This draft focuses on commonalization of data plane, and control plane is out of scope for now. Having said that, IGP and BGP extension for SRv6 can be used as the control plane as they are.

As for the mobility management, BGP based Loc/ID mapping would be straightforward to implement. Or even pure ID based anchorless protocol such as hICN [I-D.auge-dmm-hicn-mobility] can be used.

The co-existence with the 3GPP control plane is for further study.

7. Incremental Deployment

Although it may seem difficult to migrate from the current mobile architecture, the conversion between GTP-U and SRv6 has been defined and can co-exist with the current mobile architecture as needed. Since the conversion is done completely statelessly (i.e., all necessary information is retained in the packet), there will not be a scaling bottleneck or a single point of failure.

With regard to the architectural migration, the insertion with no modification to the existing 3GPP architecture is considered first, and then the tighter integration of data plane is to be achieved. as described in [I-D.auge-dmm-hicn-mobility-deployment-options].

8. Security Considerations

TBD

9. IANA Considerations

NA

10. Acknowledgements

Authors would like to thank Satoru Matsushima and Shunsuke Homma for their insights and comments.

11. References

11.1. Normative References

[I-D.hegdeppsenak-isis-sr-flex-algo]
Psenak, P., Hegde, S., Filsfils, C., and A. Gulko, "ISIS Segment Routing Flexible Algorithm", draft-hegdeppsenak-isis-sr-flex-algo-02 (work in progress), February 2018.

[I-D.ietf-dmm-srv6-mobile-uplane]
Matsushima, S., Filsfils, C., Kohno, M., Camarillo, P., Voyer, D., and C. Perkins, "Segment Routing IPv6 for Mobile User Plane", draft-ietf-dmm-srv6-mobile-uplane-09 (work in progress), July 2020.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-15 (work in progress), January 2018.

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-24 (work in progress), October 2020.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

11.2. Informative References

[ETSI-MEC]
ETSI, "MEC in 5G Networks", ETSI White Paper No.28, June 2018.

[I-D.ali-spring-network-slicing-building-blocks]
Ali, Z., Filsfils, C., Camarillo, P., and D. Voyer, "Building blocks for Slicing in Segment Routing Network", draft-ali-spring-network-slicing-building-blocks-02 (work in progress), November 2019.

[I-D.auge-dmm-hicn-mobility]
Auge, J., Carofiglio, G., Muscariello, L., and M. Papalini, "Anchorless mobility through hICN", draft-auge-dmm-hicn-mobility-04 (work in progress), July 2020.

[I-D.auge-dmm-hicn-mobility-deployment-options]
Auge, J., Carofiglio, G., Muscariello, L., and M. Papalini, "Anchorless mobility management through hICN (hICN-AMM): Deployment options", draft-auge-dmm-hicn-mobility-deployment-options-04 (work in progress), July 2020.

[I-D.clt-dmm-tn-aware-mobility]
Chunduri, U., Li, R., Bhaskaran, S., Kaippallimalil, J., Tantsura, J., Contreras, L., and P. Muley, "Transport Network aware Mobility for 5G", draft-clt-dmm-tn-aware-mobility-07 (work in progress), September 2020.

[I-D.filsfils-spring-srv6-interop]
Filsfils, C., Clad, F., Camarillo, P., Abdelsalam, A., Salsano, S., Bonaventure, O., Horn, J., and J. Liste, "SRv6 interoperability report", draft-filsfils-spring-srv6-interop-02 (work in progress), March 2019.

[I-D.filsfils-spring-srv6-stateless-slice-id]
Filsfils, C., Clad, F., Camarillo, P., and K. Raza, "Stateless and Scalable Network Slice Identification for SRv6", draft-filsfils-spring-srv6-stateless-slice-id-01 (work in progress), July 2020.

[I-D.guichard-spring-srv6-simplified-firewall]
Guichard, J., Filsfils, C., daniel.bernier@bell.ca, d., Li, Z., Clad, F., Camarillo, P., and A. Abdelsalam, "Simplifying Firewall Rules with Network Programming and SRH Metadata", draft-guichard-spring-srv6-simplified-firewall-02 (work in progress), April 2020.

[I-D.ietf-dmm-fpc-cpdp]
Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", draft-ietf-dmm-fpc-cpdp-14 (work in progress), September 2020.

[I-D.rokui-5g-transport-slice]
Rokui, R., Homma, S., Lopez, D., Foy, X., Contreras, L., Ordonez-Lucena, J., Martinez-Julia, P., Boucadair, M., Eardley, P., Makhijani, K., and H. Flinck, "5G Transport Slice Connectivity Interface", draft-rokui-5g-transport-slice-00 (work in progress), July 2019.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[TR.23725]
3GPP, "Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)", 3GPP TR 23.725 16.2.0, June 2019.

[TR.29892]
3GPP, "Study on User Plane Protocol in 5GC", 3GPP TR 29.892 16.1.0, April 2019.

[TS.23501]
3GPP, "System Architecture for the 5G System", 3GPP TS 23.501 15.0.0, November 2017.

[TS.29244]
3GPP, "Interface between the Control Plane and the User Plane Nodes", 3GPP TS 29.244 15.0.0, December 2017.

[TS.29281]
3GPP, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 15.1.0, December 2017.

Authors' Addresses

Miya Kohno
Cisco Systems, Inc.
Japan

Email: mkohno@cisco.com

Francois Clad
Cisco Systems, Inc.
France

Email: fclad@cisco.com

Pablo Camarillo Garvia
Cisco Systems, Inc.
Spain

Email: pcamaril@cisco.com

Zafar Ali
Cisco Systems, Inc.
Canada

Email: zali@cisco.com