

DMM Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 10 November 2022

S. Matsushima, Ed.  
SoftBank  
C. Filsfils  
M. Kohno  
P. Camarillo, Ed.  
Cisco Systems, Inc.  
D. Voyer  
Bell Canada  
C.E. Perkins  
Lupin Lodge  
9 May 2022

Segment Routing IPv6 for Mobile User Plane  
draft-ietf-dmm-srv6-mobile-uplane-21

Abstract

This document specifies the applicability of SRv6 (Segment Routing IPv6) to the user-plane of mobile networks. The network programming nature of SRv6 accomplishes mobile user-plane functions in a simple manner. The statelessness of SRv6 and its ability to control both service layer path and underlying transport can be beneficial to the mobile user-plane, providing flexibility, end-to-end network slicing, and SLA control for various applications.

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 10 November 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions and Terminology . . . . .	3
2.1. Terminology . . . . .	3
2.2. Conventions . . . . .	4
2.3. Predefined SRv6 Endpoint Behaviors . . . . .	4
3. Motivation . . . . .	5
4. 3GPP Reference Architecture . . . . .	5
5. User-plane modes . . . . .	6
5.1. Traditional mode . . . . .	7
5.1.1. Packet flow - Uplink . . . . .	8
5.1.2. Packet flow - Downlink . . . . .	9
5.2. Enhanced mode . . . . .	9
5.2.1. Packet flow - Uplink . . . . .	10
5.2.2. Packet flow - Downlink . . . . .	11
5.2.3. Scalability . . . . .	12
5.3. Enhanced mode with unchanged gNB GTP behavior . . . . .	12
5.3.1. Interworking with IPv6 GTP . . . . .	12
5.3.2. Interworking with IPv4 GTP . . . . .	15
5.3.3. Extensions to the interworking mechanisms . . . . .	18
5.4. SRv6 Drop-in Interworking . . . . .	18
6. SRv6 Segment Endpoint Mobility Behaviors . . . . .	19
6.1. Args.Mob.Session . . . . .	20
6.2. End.MAP . . . . .	20
6.3. End.M.GTP6.D . . . . .	21
6.4. End.M.GTP6.D.Di . . . . .	22
6.5. End.M.GTP6.E . . . . .	23
6.6. End.M.GTP4.E . . . . .	24
6.7. H.M.GTP4.D . . . . .	25
6.8. End.Limit: Rate Limiting behavior . . . . .	26
7. SRv6 supported 3GPP PDU session types . . . . .	27
8. Network Slicing Considerations . . . . .	27
9. Control Plane Considerations . . . . .	27
10. Security Considerations . . . . .	28
11. IANA Considerations . . . . .	28
12. Acknowledgements . . . . .	29
13. Contributors . . . . .	29
14. References . . . . .	29

14.1. Normative References . . . . .	29
14.2. Informative References . . . . .	30
Appendix A. Implementations . . . . .	32
Authors' Addresses . . . . .	32

## 1. Introduction

In mobile networks, mobility systems provide connectivity over a wireless link to stationary and non-stationary nodes. The user-plane establishes a tunnel between the mobile node and its anchor node over IP-based backhaul and core networks.

This document specifies the applicability of SRv6 (Segment Routing IPv6) to mobile networks.

Segment Routing [RFC8402] is a source routing architecture: a node steers a packet through an ordered list of instructions called "segments". A segment can represent any instruction, topological or service based.

SRv6 applied to mobile networks enables a source-routing based mobile architecture, where operators can explicitly indicate a route for the packets to and from the mobile node. The SRv6 Endpoint nodes serve as mobile user-plane anchors.

## 2. Conventions and 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].

### 2.1. Terminology

- \* CNF: Cloud-native Network Function
- \* NFV: Network Function Virtualization
- \* PDU: Packet Data Unit
- \* PDU Session: Context of a UE connects to a mobile network.
- \* UE: User Equipment
- \* UPF: User Plane Function
- \* VNF: Virtual Network Function (including CNFs)

The following terms used within this document are defined in [RFC8402]: Segment Routing, SR Domain, Segment ID (SID), SRv6, SRv6 SID, Active Segment, SR Policy, Prefix SID, Adjacency SID and Binding SID.

The following terms used within this document are defined in [RFC8754]: SRH, SR Source Node, Transit Node, SR Segment Endpoint Node and Reduced SRH.

The following terms used within this document are defined in [RFC8986]: NH, SL, FIB, SA, DA, SRv6 SID behavior, SRv6 Segment Endpoint Behavior.

## 2.2. Conventions

An SR Policy is resolved to a SID list. A SID list is represented as <S1, S2, S3> where S1 is the first SID to visit, S2 is the second SID to visit, and S3 is the last SID to visit along the SR path.

(SA,DA) (S3, S2, S1; SL) represents an IPv6 packet with:

- \* Source Address is SA, Destination Address is DA, and next-header is SRH
- \* SRH with SID list <S1, S2, S3> with Segments Left = SL
- \* Note the difference between the <> and () symbols: <S1, S2, S3> represents a SID list where S1 is the first SID and S3 is the last SID to traverse. (S3, S2, S1; SL) represents the same SID list but encoded in the SRH format where the rightmost SID in the SRH is the first SID and the leftmost SID in the SRH is the last SID. When referring to an SR policy in a high-level use-case, it is simpler to use the <S1, S2, S3> notation. When referring to an illustration of the detailed packet behavior, the (S3, S2, S1; SL) notation is more convenient.
- \* The payload of the packet is omitted.

SRH[n]: A shorter representation of Segment List[n], as defined in [RFC8754]. SRH[SL] can be different from the DA of the IPv6 header.

- \* gNB::1 is an IPv6 address (SID) assigned to the gNB.
- \* U1::1 is an IPv6 address (SID) assigned to UPF1.
- \* U2::1 is an IPv6 address (SID) assigned to UPF2.
- \* U2:: is the Locator of UPF2.

## 2.3. Predefined SRv6 Endpoint Behaviors

The following SRv6 Endpoint Behaviors are defined in [RFC8986].

- \* End.DT4: Decapsulation and Specific IPv4 Table Lookup
- \* End.DT6: Decapsulation and Specific IPv6 Table Lookup
- \* End.DT46: Decapsulation and Specific IP Table Lookup
- \* End.DX4: Decapsulation and IPv4 Cross-Connect
- \* End.DX6: Decapsulation and IPv6 Cross-Connect
- \* End.DX2: Decapsulation and L2 Cross-Connect

\* End.T: Endpoint with specific IPv6 Table Lookup

This document defines new SRv6 Segment Endpoint Behaviors in Section 6.

### 3. Motivation

Mobile networks are becoming more challenging to operate. On one hand, traffic is constantly growing, and latency requirements are tighter; on the other-hand, there are new use-cases like distributed NFVi that are also challenging network operations.

The current architecture of mobile networks does not take into account the underlying transport. The user-plane is rigidly fragmented into radio access, core and service networks, connected by tunneling according to user-plane roles such as access and anchor nodes. These factors have made it difficult for the operator to optimize and operate the data-path.

In the meantime, applications have shifted to use IPv6, and network operators have started adopting IPv6 as their IP transport. SRv6, the IPv6 dataplane instantiation of Segment Routing [RFC8402], integrates both the application data-path and the underlying transport layer into a single protocol, allowing operators to optimize the network in a simplified manner and removing forwarding state from the network. It is also suitable for virtualized environments, like VNF/CNF to VNF/CNF networking. SRv6 has been deployed in dozens of networks [I-D.matsushima-spring-srv6-deployment-status].

SRv6 defines the network-programming concept [RFC8986]. Applied to mobility, SRv6 can provide the user-plane behaviors needed for mobility management. SRv6 takes advantage of the underlying transport awareness and flexibility together with the ability to also include services to optimize the end-to-end mobile dataplane.

The use-cases for SRv6 mobility are discussed in [I-D.camarilloelmalaky-springdmm-srv6-mob-usecases], and the architectural benefits are discussed in [I-D.kohno-dmm-srv6mob-arch].

### 4. 3GPP Reference Architecture

This section presents a reference architecture and possible deployment scenarios.

Figure 1 shows a reference diagram from the 5G packet core architecture [TS.23501].

The user plane described in this document does not depend on any specific architecture. The 5G packet core architecture as shown is based on the latest 3GPP standards at the time of writing this draft.

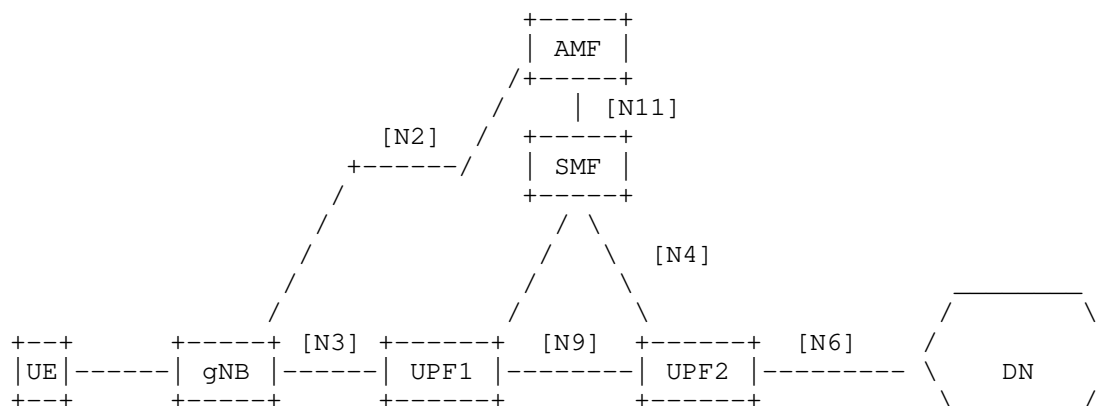


Figure 1: 3GPP 5G Reference Architecture

- \* UE: User Endpoint
- \* gNB: gNodeB with N3 interface towards packet core (and N2 for control plane)
- \* UPF1: UPF with Interfaces N3 and N9 (and N4 for control plane)
- \* UPF2: UPF with Interfaces N9 and N6 (and N4 for control plane)
- \* SMF: Session Management Function
- \* AMF: Access and Mobility Management Function
- \* DN: Data Network e.g. operator services, Internet access

This reference diagram does not depict a UPF that is only connected to N9 interfaces, although the mechanisms defined in this document also work in such case.

Each session from a UE gets assigned to a UPF. Sometimes multiple UPFs may be used, providing richer service functions. A UE gets its IP address from the DHCP block of its UPF. The UPF advertises that IP address block toward the Internet, ensuring that return traffic is routed to the right UPF.

## 5. User-plane modes

This section introduces an SRv6 based mobile user-plane.

In order to simplify the adoption of SRv6, we present two different "modes" that vary with respect to the use of SRv6. The first one is the "Traditional mode", which inherits the current 3GPP mobile architecture. In this mode GTP-U protocol [TS.29281] is replaced by

SRv6, however the N3, N9 and N6 interfaces are still point-to-point interfaces with no intermediate waypoints as in the current mobile network architecture.

The second mode is the "Enhanced mode". This is an evolution from the "Traditional mode". In this mode the N3, N9 or N6 interfaces have intermediate waypoints -SIDs- that are used for Traffic Engineering or VNF purposes transparent to 3GPP functionalities. This results in optimal end-to-end policies across the mobile network with transport and services awareness.

In both, the Traditional and the Enhanced modes, we assume that the gNB as well as the UPFs are SR-aware (N3, N9 and -potentially- N6 interfaces are SRv6).

In addition to those two modes, we introduce two mechanisms for interworking with legacy access networks (those where the N3 interface is unmodified). In this document we introduce them as a variant to the Enhanced mode, however they are equally applicable to the Traditional mode.

One of these mechanisms is designed to interwork with legacy gNBs using GTP/IPv4. The second mechanism is designed to interwork with legacy gNBs using GTP/IPv6.

This document uses SRv6 Segment Endpoint Behaviors defined in [RFC8986] as well as new SRv6 Segment Endpoint Behaviors designed for the mobile user plane that are defined in this document in Section 6.

Note that the modes discussed throughout this section (with the exception of Section 5.4) only have informational purpose to implementors as well as operators deploying this technology. Indeed, it is expected that the operator defines his own operational model that best suits their needs.

### 5.1. Traditional mode

In the traditional mode, the existing mobile UPFs remain unchanged with the sole exception of the use of SRv6 as the data plane instead of GTP-U. There is no impact to the rest of the mobile system.

In existing 3GPP mobile networks, a PDU Session is mapped 1-for-1 with a specific GTP tunnel (TEID). This 1-for-1 mapping is mirrored here to replace GTP encapsulation with the SRv6 encapsulation, while not changing anything else. There will be a unique SRv6 SID associated with each PDU Session, and the SID list only contains a single SID.

The traditional mode minimizes the changes required to the mobile system; hence it is a good starting point for forming a common ground.

The gNB/UPF control-plane (N2/N4 interface) is unchanged, specifically a single IPv6 address is provided to the gNB. The same control plane signalling is used, and the gNB/UPF decides to use SRv6 based on signaled GTP-U parameters per local policy. The only information from the GTP-U parameters used for the SRv6 policy is the TEID, QFI, and the IPv6 Destination Address.

Our example topology is shown in Figure 2. The gNB and the UPFs are SR-aware. In the descriptions of the uplink and downlink packet flow, A is an IPv6 address of the UE, and Z is an IPv6 address reachable within the Data Network DN. A new SRv6 Endpoint Behavior, End.MAP, defined in Section 6.2, is used.

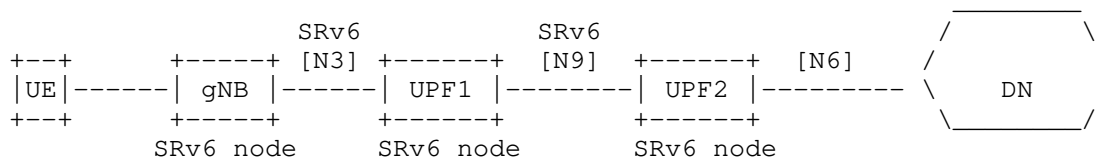


Figure 2: Traditional mode - example topology

#### 5.1.1. Packet flow - Uplink

The uplink packet flow is as follows:

```

UE_out   : (A,Z)
gNB_out  : (gNB, U1::1) (A,Z)    -> H.Encaps.Red <U1::1>
UPF1_out : (gNB, U2::1) (A,Z)    -> End.MAP
UPF2_out : (A,Z)                 -> End.DT4 or End.DT6

```

When the UE packet arrives at the gNB, the gNB performs a H.Encaps.Red operation. Since there is only one SID, there is no need to push an SRH. gNB only adds an outer IPv6 header with IPv6 DA U1::1. gNB obtains the SID U1::1 from the existing control plane (N2 interface). U1::1 represents an anchoring SID specific for that session at UPF1.

When the packet arrives at UPF1, the SID U1::1 is associated with the End.MAP SRv6 Endpoint Behavior. End.MAP replaces U1::1 by U2::1, that belongs to the next UPF (U2).



When the packet arrives at UPF2, the SID U2::1 corresponds to an End.DT4/End.DT6/End.DT46 SRv6 Endpoint Behavior. UPF2 decapsulates the packet, performs a lookup in a specific table associated with that mobile network and forwards the packet toward the data network (DN).

#### 5.1.2. Packet flow - Downlink

The downlink packet flow is as follows:

```
UPF2_in : (Z,A)
UPF2_out: (U2::, U1::2) (Z,A)    -> H.Encaps.Red <U1::2>
UPF1_out: (U2::, gNB::1) (Z,A)   -> End.MAP
gNB_out  : (Z,A)                  -> End.DX4, End.DX6, End.DX2
```

When the packet arrives at the UPF2, the UPF2 maps that flow into a PDU Session. This PDU Session is associated with the segment endpoint <U1::2>. UPF2 performs a H.Encaps.Red operation, encapsulating the packet into a new IPv6 header with no SRH since there is only one SID.

Upon packet arrival on UPF1, the SID U1::2 is a local SID associated with the End.MAP SRv6 Endpoint Behavior. It maps the SID to the next anchoring point and replaces U1::2 by gNB::1, that belongs to the next hop.

Upon packet arrival on gNB, the SID gNB::1 corresponds to an End.DX4, End.DX6 or End.DX2 behavior (depending on the PDU Session Type). The gNB decapsulates the packet, removing the IPv6 header and all its extensions headers, and forwards the traffic toward the UE.

#### 5.2. Enhanced mode

Enhanced mode improves scalability, provides traffic engineering capabilities, and allows service programming [I-D.ietf-spring-sr-service-programming], thanks to the use of multiple SIDs in the SID list (instead of a direct connectivity in between UPFs with no intermediate waypoints as in Traditional Mode).

Thus, the main difference is that the SR policy MAY include SIDs for traffic engineering and service programming in addition to the anchoring SIDs at UPFs.

Additionally in this mode the operator may choose to aggregate several devices under the same SID list (e.g., stationary residential meters connected to the same cell) to improve scalability.

The gNB/UPF control-plane (N2/N4 interface) is unchanged, specifically a single IPv6 address is provided to the gNB. A local policy instructs the gNB to use SRv6.

The gNB MAY resolve the IP address received via the control plane into a SID list using a mechanism like PCEP, DNS-lookup, LISP control-plane or others. The resolution mechanism is out of the scope of this document.

Note that the SIDs MAY use the arguments Args.Mob.Session if required by the UPFs.

Figure 3 shows an Enhanced mode topology. The gNB and the UPF are SR-aware. The Figure shows two service segments, S1 and C1. S1 represents a VNF in the network, and C1 represents an intermediate router used for Traffic Engineering purposes to enforce a low-latency path in the network. Note that neither S1 nor C1 are required to have an N4 interface.

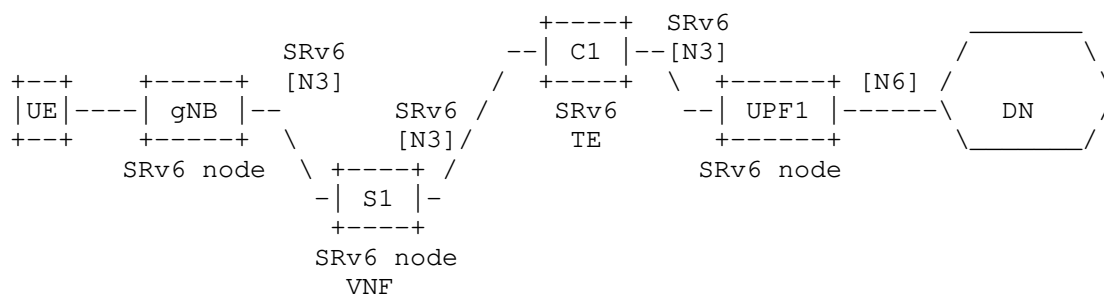


Figure 3: Enhanced mode - Example topology

#### 5.2.1. Packet flow - Uplink

The uplink packet flow is as follows:

```

UE_out   : (A,Z)
gNB_out  : (gNB, S1) (U1::1, C1; SL=2) (A,Z)->H.Encaps.Red<S1,C1,U1::1>
S1_out   : (gNB, C1) (U1::1, C1; SL=1) (A,Z)
C1_out   : (gNB, U1::1) (A,Z)                ->End with PSP
UPF1_out : (A,Z)                             ->End.DT4,End.DT6,End.DT2U

```

UE sends its packet (A,Z) on a specific bearer to its gNB. gNB's control plane associates that session from the UE(A) with the IPv6 address B. gNB's control plane does a lookup on B to find the related SID list <S1, C1, U1::1>.

When gNB transmits the packet, it contains all the segments of the SR policy. The SR policy includes segments for traffic engineering (C1) and for service programming (S1).

Nodes S1 and C1 perform their related Endpoint functionality and forward the packet.

When the packet arrives at UPF1, the active segment (U1::1) is an End.DT4/End.DT6/End.DT2U which performs the decapsulation (removing the IPv6 header with all its extension headers) and forwards toward the data network.

#### 5.2.2. Packet flow - Downlink

The downlink packet flow is as follows:

```

UPF1_in : (Z,A)                                ->UPF1 maps the flow w/
                                                SID list <C1,S1, gNB>
UPF1_out: (U1::1, C1) (gNB::1, S1; SL=2) (Z,A) ->H.Encaps.Red
C1_out  : (U1::1, S1) (gNB::1, S1; SL=1) (Z,A)
S1_out  : (U1::1, gNB::1) (Z,A)                ->End with PSP
gNB_out : (Z,A)                                ->End.DX4/End.DX6/End.DX2

```

When the packet arrives at the UPF1, the UPF1 maps that particular flow into a UE PDU Session. This UE PDU Session is associated with the policy <C1, S1, gNB>. The UPF1 performs a H.Encaps.Red operation, encapsulating the packet into a new IPv6 header with its corresponding SRH.

The nodes C1 and S1 perform their related Endpoint processing.

Once the packet arrives at the gNB, the IPv6 DA corresponds to an End.DX4, End.DX6 or End.DX2 behavior at the gNB (depending on the underlying traffic). The gNB decapsulates the packet, removing the IPv6 header, and forwards the traffic towards the UE. The SID gNB::1 is one example of a SID associated to this service.

Note that there are several means to provide the UE session aggregation. The decision on which one to use is a local decision made by the operator. One option is to use the Args.Mob.Session (Section 6.1). Another option comprises the gNB performing an IP lookup on the inner packet by using the End.DT4, End.DT6, and End.DT2 behaviors.

### 5.2.3. Scalability

The Enhanced Mode improves since it allows the aggregation of several UEs under the same SID list. For example, in the case of stationary residential meters that are connected to the same cell, all such devices can share the same SID list. This improves scalability compared to Traditional Mode (unique SID per UE) and compared to GTP-U (dedicated TEID per UE).

### 5.3. Enhanced mode with unchanged gNB GTP behavior

This section describes two mechanisms for interworking with legacy gNBs that still use GTP: one for IPv4, and another for IPv6.

In the interworking scenarios as illustrated in Figure 4, the gNB does not support SRv6. The gNB supports GTP encapsulation over IPv4 or IPv6. To achieve interworking, an SR Gateway (SRGW) entity is added. The SRGW maps the GTP traffic into SRv6.

The SRGW is not an anchor point and maintains very little state. For this reason, both IPv4 and IPv6 methods scale to millions of UEs.

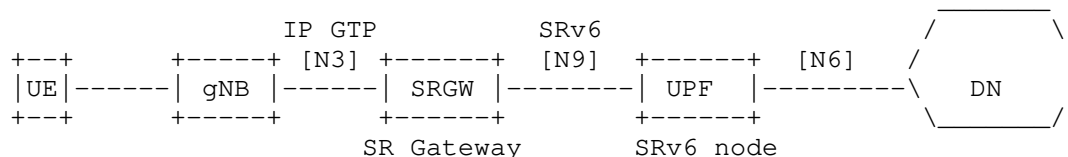


Figure 4: Example topology for interworking

Both of the mechanisms described in this section are applicable to either the Traditional Mode or the Enhanced Mode.

#### 5.3.1. Interworking with IPv6 GTP

In this interworking mode the gNB at the N3 interface uses GTP over IPv6.

Key points:

- \* The gNB is unchanged (control-plane or user-plane) and encapsulates into GTP (N3 interface is not modified).
- \* The 5G Control-Plane towards the gNB (N2 interface) is unmodified, though multiple UPF addresses need to be used - one IPv6 address (i.e. a BSID at the SRGW) is needed per <SLA, PDU session type>. The SRv6 SID is different depending on the required <SLA, PDU session type> combination.

- \* In the uplink, the SRGW removes GTP, finds the SID list related to the IPv6 DA, and adds SRH with the SID list.
- \* There is no state for the downlink at the SRGW.
- \* There is simple state in the uplink at the SRGW; using Enhanced mode results in fewer SR policies on this node. An SR policy is shared across UEs as long as they belong to the same context (i.e., tenant). A set of many different policies (i.e., different SLAs) increases the amount of state required.
- \* When a packet from the UE leaves the gNB, it is SR-routed. This simplifies network slicing [I-D.ietf-lsr-flex-algo].
- \* In the uplink, the SRv6 BSID steers traffic into an SR policy when it arrives at the SRGW.

An example topology is shown in Figure 5.

S1 and C1 are two service segments. S1 represents a VNF in the network, and C1 represents a router configured for Traffic Engineering.

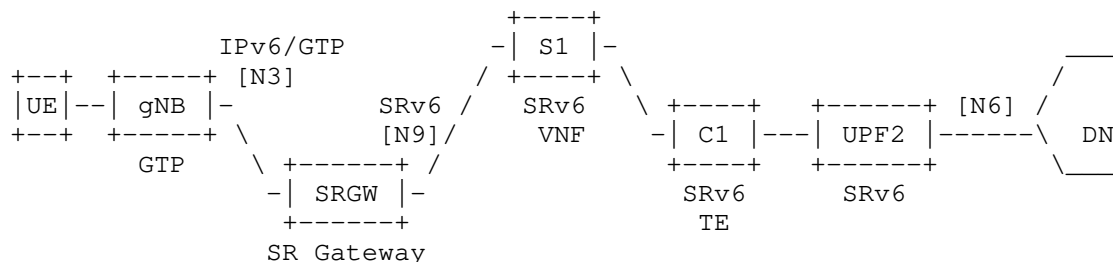


Figure 5: Enhanced mode with unchanged gNB IPv6/GTP behavior

#### 5.3.1.1. Packet flow - Uplink

The uplink packet flow is as follows:

```

UE_out   : (A,Z)
gNB_out  : (gNB, B) (GTP: TEID T) (A,Z)      -> Interface N3 unmodified
                                                (IPv6/GTP)
SRGW_out : (SRGW, S1) (U2::T, C1; SL=2) (A,Z) -> B is an End.M.GTP6.D
                                                SID at the SRGW
S1_out   : (SRGW, C1) (U2::T, C1; SL=1) (A,Z)
C1_out   : (SRGW, U2::T) (A,Z)                -> End with PSP
UPF2_out : (A,Z)                             -> End.DT4 or End.DT6

```

The UE sends a packet destined to Z toward the gNB on a specific bearer for that session. The gNB, which is unmodified, encapsulates the packet into IPv6, UDP, and GTP headers. The IPv6 DA B, and the GTP TEID T are the ones received in the N2 interface.

The IPv6 address that was signaled over the N2 interface for that UE PDU Session, B, is now the IPv6 DA. B is an SRv6 Binding SID at the SRGW. Hence the packet is routed to the SRGW.

When the packet arrives at the SRGW, the SRGW identifies B as an End.M.GTP6.D Binding SID (see Section 6.3). Hence, the SRGW removes the IPv6, UDP, and GTP headers, and pushes an IPv6 header with its own SRH containing the SIDs bound to the SR policy associated with this BindingSID. There at least one instance of the End.M.GTP6.D SID per PDU type.

S1 and C1 perform their related Endpoint functionality and forward the packet.

When the packet arrives at UPF2, the active segment is (U2::T) which is bound to End.DT4/6. UPF2 then decapsulates (removing the outer IPv6 header with all its extension headers) and forwards the packet toward the data network.

#### 5.3.1.2. Packet flow - Downlink

The downlink packet flow is as follows:

```

UPF2_in : (Z,A)                                -> UPF2 maps the flow with
                                                <C1, S1, SRGW::TEID,gNB>
UPF2_out: (U2::1, C1)(gNB, SRGW::TEID, S1; SL=3)(Z,A) -> H.Encaps.Red
C1_out   : (U2::1, S1)(gNB, SRGW::TEID, S1; SL=2)(Z,A)
S1_out   : (U2::1, SRGW::TEID)(gNB, SRGW::TEID, S1, SL=1)(Z,A)
SRGW_out : (SRGW, gNB)(GTP: TEID=T)(Z,A)      -> SRGW/96 is End.M.GTP6.E
gNB_out  : (Z,A)

```

When a packet destined to A arrives at the UPF2, the UPF2 performs a lookup in the table associated to A and finds the SID list <C1, S1, SRGW::TEID, gNB>. The UPF2 performs an H.Encaps.Red operation, encapsulating the packet into a new IPv6 header with its corresponding SRH.

C1 and S1 perform their related Endpoint processing.

Once the packet arrives at the SRGW, the SRGW identifies the active SID as an End.M.GTP6.E function. The SRGW removes the IPv6 header and all its extensions headers. The SRGW generates new IPv6, UDP, and GTP headers. The new IPv6 DA is the gNB which is the last SID in the received SRH. The TEID in the generated GTP header is an argument of the received End.M.GTP6.E SID. The SRGW pushes the headers to the packet and forwards the packet toward the gNB. There is one instance of the End.M.GTP6.E SID per PDU type.

Once the packet arrives at the gNB, the packet is a regular IPv6/GTP packet. The gNB looks for the specific radio bearer for that TEID and forward it on the bearer. This gNB behavior is not modified from current and previous generations.

#### 5.3.1.3. Scalability

For the downlink traffic, the SRGW is stateless. All the state is in the SRH pushed by the UPF2. The UPF2 must have the UE states since it is the UE's session anchor point.

For the uplink traffic, the state at the SRGW does not necessarily need to be unique per PDU Session; the SR policy can be shared among UEs. This enables more scalable SRGW deployments compared to a solution holding millions of states, one or more per UE.

#### 5.3.2. Interworking with IPv4 GTP

In this interworking mode the gNB uses GTP over IPv4 in the N3 interface

Key points:

- \* The gNB is unchanged and encapsulates packets into GTP (the N3 interface is not modified).
- \* N2 signaling is not changed, though multiple UPF addresses need to be provided – one for each PDU Session Type.
- \* In the uplink, traffic is classified by SRGW's classification engine and steered into an SR policy. The SRGW may be implemented in a UPF or as a separate entity. How the classification engine rules are set up is outside the scope of this document, though one example is using BGP signaling from a Mobile User Plane Controller [I-D.mhkk-dmm-srv6mup-architecture].
- \* SRGW removes GTP, finds the SID list related to DA, and adds an SRH with the SID list.

An example topology is shown in Figure 6. In this mode the gNB is an unmodified gNB using IPv4/GTP. The UPFs are SR-aware. As before, the SRGW maps the IPv4/GTP traffic to SRv6.

S1 and C1 are two service segment endpoints. S1 represents a VNF in the network, and C1 represents a router configured for Traffic Engineering.

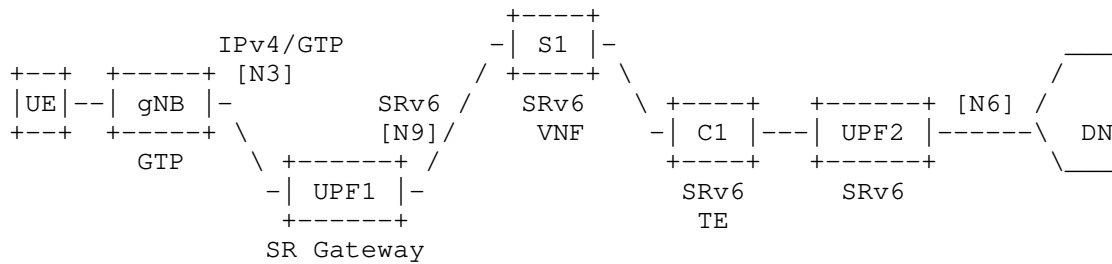


Figure 6: Enhanced mode with unchanged gNB IPv4/GTP behavior

## 5.3.2.1. Packet flow - Uplink

The uplink packet flow is as follows:

```

gNB_out : (gNB, B) (GTP: TEID T) (A, Z)          -> Interface N3
                                                unchanged IPv4/GTP
SRGW_out: (SRGW, S1) (U2::1, C1; SL=2) (A, Z)    -> H.M.GTP4.D function
S1_out  : (SRGW, C1) (U2::1, C1; SL=1) (A, Z)
C1_out  : (SRGW, U2::1) (A, Z)                   -> PSP
UPF2_out: (A, Z)                                 -> End.DT4 or End.DT6

```

The UE sends a packet destined to Z toward the gNB on a specific bearer for that session. The gNB, which is unmodified, encapsulates the packet into a new IPv4, UDP, and GTP headers. The IPv4 DA, B, and the GTP TEID are the ones received at the N2 interface.

When the packet arrives at the SRGW for UPF1, the SRGW has an classification engine rule for incoming traffic from the gNB, that steers the traffic into an SR policy by using the function H.M.GTP4.D. The SRGW removes the IPv4, UDP, and GTP headers and pushes an IPv6 header with its own SRH containing the SIDs related to the SR policy associated with this traffic. The SRGW forwards according to the new IPv6 DA.

S1 and C1 perform their related Endpoint functionality and forward the packet.

When the packet arrives at UPF2, the active segment is (U2::1) which is bound to End.DT4/6 which performs the decapsulation (removing the outer IPv6 header with all its extension headers) and forwards toward the data network.



Note that the interworking mechanisms for IPv4/GTP and IPv6/GTP differs. This is due to the fact that in IPv6/GTP we can leverage the remote steering capabilities provided by the Segment Routing BSID. In IPv4 this construct is not available, and building a similar mechanism would require a significant address consumption.

#### 5.3.2.2. Packet flow - Downlink

The downlink packet flow is as follows:

```

UPF2_in : (Z,A)                                -> UPF2 maps flow with SID
                                                <C1, S1,GW::SA:DA:TEID>
UPF2_out: (U2::1, C1) (GW::SA:DA:TEID, S1; SL=2) (Z,A) ->H.Encaps.Red
C1_out   : (U2::1, S1) (GW::SA:DA:TEID, S1; SL=1) (Z,A)
S1_out   : (U2::1, GW::SA:DA:TEID) (Z,A)
SRGW_out: (GW, gNB) (GTP: TEID=T) (Z,A)         -> End.M.GTP4.E
gNB_out  : (Z,A)

```

When a packet destined to A arrives at the UPF2, the UPF2 performs a lookup in the table associated to A and finds the SID list <C1, S1, SRGW::SA:DA:TEID>. The UPF2 performs a H.Encaps.Red operation, encapsulating the packet into a new IPv6 header with its corresponding SRH.

The nodes C1 and S1 perform their related Endpoint processing.

Once the packet arrives at the SRGW, the SRGW identifies the active SID as an End.M.GTP4.E function. The SRGW removes the IPv6 header and all its extensions headers. The SRGW generates an IPv4, UDP, and GTP headers. The IPv4 SA and DA are received as SID arguments. The TEID in the generated GTP header is also the arguments of the received End.M.GTP4.E SID. The SRGW pushes the headers to the packet and forwards the packet toward the gNB.

When the packet arrives at the gNB, the packet is a regular IPv4/GTP packet. The gNB looks for the specific radio bearer for that TEID and forwards it on the bearer. This gNB behavior is not modified from current and previous generations.

#### 5.3.2.3. Scalability

For the downlink traffic, the SRGW is stateless. All the state is in the SRH pushed by the UPF2. The UPF must have this UE-base state anyway (since it is its anchor point).

For the uplink traffic, the state at the SRGW is dedicated on a per UE/session basis according to a classification engine. There is state for steering the different sessions in the form of an SR Policy. However, SR policies are shared among several UE/sessions.

### 5.3.3. Extensions to the interworking mechanisms

In this section we presented two mechanisms for interworking with gNBs and UPFs that do not support SRv6. These mechanisms are used to support GTP over IPv4 and IPv6.

Even though we have presented these methods as an extension to the "Enhanced mode", it is straightforward in its applicability to the "Traditional mode".

### 5.4. SRv6 Drop-in Interworking

In this section we introduce another mode useful for legacy gNB and UPFs that still operate with GTP-U. This mode provides an SRv6-enabled user plane in between two GTP-U tunnel endpoints.

In this mode we employ two SRGWs that map GTP-U traffic to SRv6 and vice-versa.

Unlike other interworking modes, in this mode both of the mobility overlay endpoints use GTP-U. Two SRGWs are deployed in either N3 or N9 interface to realize an intermediate SR policy.

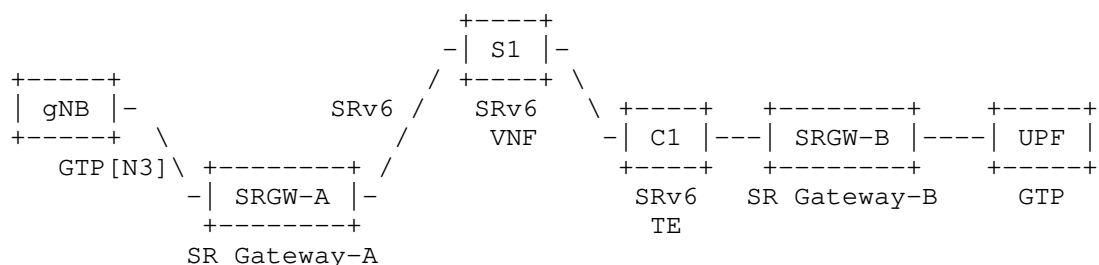


Figure 7: Example topology for SRv6 Drop-in mode

The packet flow of Figure 7 is as follows:

```

gNB_out : (gNB, U::1) (GTP: TEID T) (A,Z)
GW-A_out: (GW-A, S1) (U::1, SGB::TEID, C1; SL=3) (A,Z) ->U::1 is an
                                                    End.M.GTP6.D.Di
                                                    SID at SRGW-A
S1_out   : (GW-A, C1) (U::1, SGB::TEID, C1; SL=2) (A,Z)
C1_out   : (GW-A, SGB::TEID) (U::1, SGB::TEID, C1; SL=1) (A,Z)
GW-B_out: (GW-B, U::1) (GTP: TEID T) (A,Z) ->SGB::TEID is an
                                                    End.M.GTP6.E
                                                    SID at SRGW-B

UPF_out  : (A,Z)

```

When a packet destined to Z is sent to the gNB, which is unmodified (control-plane and user-plane remain GTP-U), gNB performs encapsulation into a new IP, UDP, and GTP headers. The IPv6 DA, U::1, and the GTP TEID are the ones received at the N2 interface.

The IPv6 address that was signaled over the N2 interface for that PDU Session, U::1, is now the IPv6 DA. U::1 is an SRv6 Binding SID at SRGW-A. Hence the packet is routed to the SRGW.

When the packet arrives at SRGW-A, the SRGW identifies U::1 as an End.M.GTP6.D.Di Binding SID (see Section 6.4). Hence, the SRGW removes the IPv6, UDP, and GTP headers, and pushes an IPv6 header with its own SRH containing the SIDs bound to the SR policy associated with this Binding SID. There is one instance of the End.M.GTP6.D.Di SID per PDU type.

S1 and C1 perform their related Endpoint functionality and forward the packet.

Once the packet arrives at SRGW-B, the SRGW identifies the active SID as an End.M.GTP6.E function. The SRGW removes the IPv6 header and all its extensions headers. The SRGW generates new IPv6, UDP, and GTP headers. The new IPv6 DA is U::1 which is the last SID in the received SRH. The TEID in the generated GTP header is an argument of the received End.M.GTP6.E SID. The SRGW pushes the headers to the packet and forwards the packet toward UPF. There is one instance of the End.M.GTP6.E SID per PDU type.

Once the packet arrives at UPF, the packet is a regular IPv6/GTP packet. The UPF looks for the specific rule for that TEID to forward the packet. This UPF behavior is not modified from current and previous generations.

## 6. SRv6 Segment Endpoint Mobility Behaviors

## 6.1. Args.Mob.Session

Args.Mob.Session provide per-session information for charging, buffering and lawful intercept (among others) required by some mobile nodes. The Args.Mob.Session argument format is used in combination with End.Map, End.DT4/End.DT6/End.DT46 and End.DX4/End.DX6/End.DX2 behaviors. Note that proposed format is applicable for 5G networks, while similar formats could be used for legacy networks.

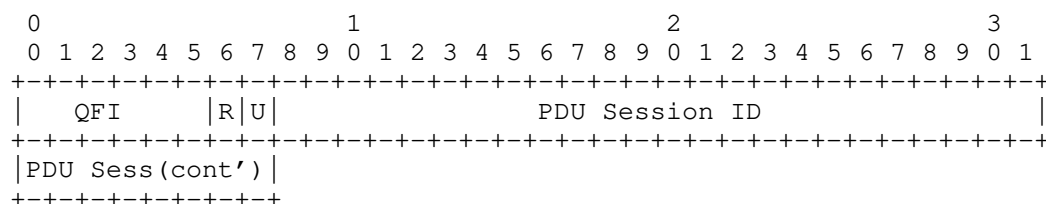


Figure 8: Args.Mob.Session format

- \* QFI: QoS Flow Identifier [TS.38415]
- \* R: Reflective QoS Indication [TS.23501]. This parameter indicates the activation of reflective QoS towards the UE for the transferred packet. Reflective QoS enables the UE to map UL User Plane traffic to QoS Flows without SMF provided QoS rules.
- \* U: Unused and for future use. MUST be 0 on transmission and ignored on receipt.
- \* PDU Session ID: Identifier of PDU Session. The GTP-U equivalent is TEID.

Arg.Mob.Session is required in case that one SID aggregates multiple PDU Sessions. Since the SRv6 SID is likely NOT to be instantiated per PDU session, Args.Mob.Session helps the UPF to perform the behaviors which require per QFI and/or per PDU Session granularity.

Note that the encoding of user-plane messages (e.g., Echo Request, Echo Reply, Error Indication and End Marker) is out of the scope of this draft. [I-D.murakami-dmm-user-plane-message-encoding] defines one possible encoding.

## 6.2. End.MAP

The "Endpoint behavior with SID mapping" behavior (End.MAP for short) is used in several scenarios. Particularly in mobility, End.MAP is used by the intermediate UPFs.

When node N receives a packet whose IPv6 DA is D and D is a local End.MAP SID, N does:

```
S01. If (IPv6 Hop Limit <= 1) {
S02.   Send an ICMP Time Exceeded message to the Source Address,
       Code 0 (Hop limit exceeded in transit),
       interrupt packet processing, and discard the packet.
S03. }
S04. Decrement IPv6 Hop Limit by 1
S05. Update the IPv6 DA with the new mapped SID
S06. Submit the packet to the egress IPv6 FIB lookup for
       transmission to the new destination
```

Notes: The SIDs in the SRH are not modified.

### 6.3. End.M.GTP6.D

The "Endpoint behavior with IPv6/GTP decapsulation into SR policy" behavior (End.M.GTP6.D for short) is used in interworking scenario for the uplink towards SRGW from the legacy gNB using IPv6/GTP. Any SID instance of this behavior is associated with an SR Policy B and an IPv6 Source Address S.

When the SR Gateway node N receives a packet destined to D and D is a local End.M.GTP6.D SID, N does:

```
S01. When an SRH is processed {
S02.   If (Segments Left != 0) {
S03.     Send an ICMP Parameter Problem to the Source Address,
         Code 0 (Erroneous header field encountered),
         Pointer set to the Segments Left field,
         interrupt packet processing, and discard the packet.
S04.   }
S05.   Proceed to process the next header in the packet
S06. }
```

When processing the Upper-layer header of a packet matching a FIB entry locally instantiated as an End.M.GTP6.D SID, N does:

```
S01. If (Next Header (NH) == UDP & UDP_Dest_port == GTP) {
S02.   Copy the GTP TEID and QFI to buffer memory
S03.   Pop the IPv6, UDP, and GTP Headers
S04.   Push a new IPv6 header with its own SRH containing B
S05.   Set the outer IPv6 SA to S
S06.   Set the outer IPv6 DA to the first SID of B
S07.   Set the outer Payload Length, Traffic Class, Flow Label,
       Hop Limit, and Next-Header (NH) fields
S08.   Write in the SRH[0] the Args.Mob.Session based on
       the information of buffer memory
S09.   Submit the packet to the egress IPv6 FIB lookup and
       transmission to the new destination
S10. } Else {
S11.   Process as per [RFC8986] Section 4.1.1
S12. }
```

Notes: S07. The NH is set based on the SID parameter. There is one instantiation of the End.M.GTP6.D SID per PDU Session Type, hence the NH is already known in advance. For the IPv4v6 PDU Session Type, in addition we inspect the first nibble of the PDU to know the NH value.

The last segment (S3 in above example) SHOULD be followed by an Arg.Mob.Session argument space which is used to provide the session identifiers.

#### 6.4. End.M.GTP6.D.Di

The "Endpoint behavior with IPv6/GTP decapsulation into SR policy for Drop-in Mode" behavior (End.M.GTP6.D.Di for short) is used in SRv6 drop-in interworking scenario described in Section 5.4. The difference between End.M.GTP6.D as another variant of IPv6/GTP decapsulation function is that the original IPv6 DA of GTP packet is preserved as the last SID in SRH.

Any SID instance of this behavior is associated with an SR Policy B and an IPv6 Source Address S.

When the SR Gateway node N receives a packet destined to D and D is a local End.M.GTP6.D.Di SID, N does:

```
S01. When an SRH is processed {
S02.   If (Segments Left != 0) {
S03.     Send an ICMP Parameter Problem to the Source Address,
        Code 0 (Erroneous header field encountered),
        Pointer set to the Segments Left field,
        interrupt packet processing, and discard the packet.
S04.   }
S05.   Proceed to process the next header in the packet
S06. }
```

When processing the Upper-layer header of a packet matching a FIB entry locally instantiated as an End.M.GTP6.Di SID, N does:

```
S01. If (Next Header = UDP & UDP_Dest_port = GTP) {
S02.   Copy D to buffer memory
S03.   Pop the IPv6, UDP, and GTP Headers
S04.   Push a new IPv6 header with its own SRH containing B
S05.   Set the outer IPv6 SA to S
S06.   Set the outer IPv6 DA to the first SID of B
S07.   Set the outer Payload Length, Traffic Class, Flow Label,
        Hop Limit, and Next-Header fields
S08.   Prepend D to the SRH (as SRH[0]) and set SL accordingly
S09.   Submit the packet to the egress IPv6 FIB lookup and
        transmission to the new destination
S10. } Else {
S11.   Process as per [RFC8986] Section 4.1.1
S12. }
```

Notes: S07. The NH is set based on the SID parameter. There is one instantiation of the End.M.GTP6.D SID per PDU Session Type, hence the NH is already known in advance. For the IPv4v6 PDU Session Type, in addition we inspect the first nibble of the PDU to know the NH value.

S SHOULD be an End.M.GTP6.E SID instantiated at the SR gateway.

#### 6.5. End.M.GTP6.E

The "Endpoint behavior with encapsulation for IPv6/GTP tunnel" behavior (End.M.GTP6.E for short) is used among others in the interworking scenario for the downlink toward the legacy gNB using IPv6/GTP.

The prefix of End.M.GTP6.E SID MUST be followed by the Arg.Mob.Session argument space which is used to provide the session identifiers.

When the SR Gateway node N receives a packet destined to D, and D is a local End.M.GTP6.E SID, N does the following:

```
S01. When an SRH is processed {
S02.   If (Segments Left != 1) {
S03.     Send an ICMP Parameter Problem to the Source Address,
        Code 0 (Erroneous header field encountered),
        Pointer set to the Segments Left field,
        interrupt packet processing, and discard the packet.
S04.   }
S05.   Proceed to process the next header in the packet
S06. }
```

When processing the Upper-layer header of a packet matching a FIB entry locally instantiated as an End.M.GTP6.E SID, N does:

```
S01.   Copy SRH[0] and D to buffer memory
S02.   Pop the IPv6 header and all its extension headers
S03.   Push a new IPv6 header with a UDP/GTP Header
S04.   Set the outer IPv6 SA to S
S05.   Set the outer IPv6 DA from buffer memory
S06.   Set the outer Payload Length, Traffic Class, Flow Label,
        Hop Limit, and Next-Header fields
S07.   Set the GTP TEID (from buffer memory)
S08.   Submit the packet to the egress IPv6 FIB lookup and
        transmission to the new destination
```

Notes: An End.M.GTP6.E SID MUST always be the penultimate SID. The TEID is extracted from the argument space of the current SID.

The source address S SHOULD be an End.M.GTP6.D SID instantiated at an SR gateway.

## 6.6. End.M.GTP4.E

The "Endpoint behavior with encapsulation for IPv4/GTP tunnel" behavior (End.M.GTP4.E for short) is used in the downlink when doing interworking with legacy gNB using IPv4/GTP.

When the SR Gateway node N receives a packet destined to S and S is a local End.M.GTP4.E SID, N does:

```
S01. When an SRH is processed {
S02.   If (Segments Left != 0) {
S03.     Send an ICMP Parameter Problem to the Source Address,
        Code 0 (Erroneous header field encountered),
        Pointer set to the Segments Left field,
        interrupt packet processing, and discard the packet.
S04.   }
S05.   Proceed to process the next header in the packet
S06. }
```



When processing the Upper-layer header of a packet matching a FIB entry locally instantiated as an End.M.GTP4.E SID, N does:

- S01. Store the IPv6 DA and SA in buffer memory
- S02. Pop the IPv6 header and all its extension headers
- S03. Push a new IPv4 header with a UDP/GTP Header
- S04. Set the outer IPv4 SA and DA (from buffer memory)
- S05. Set the outer Total Length, DSCP, Time To Live, and Next-Header fields
- S06. Set the GTP TEID (from buffer memory)
- S07. Submit the packet to the egress IPv6 FIB lookup and transmission to the new destination

Notes: The End.M.GTP4.E SID in S has the following format:

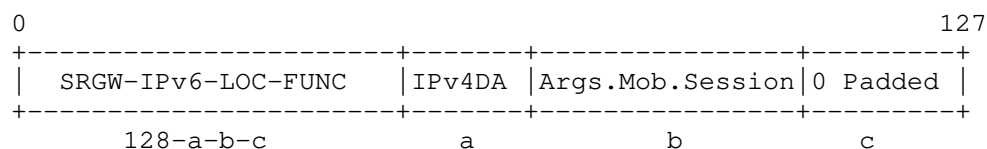


Figure 9: End.M.GTP4.E SID Encoding

The IPv6 Source Address has the following format:

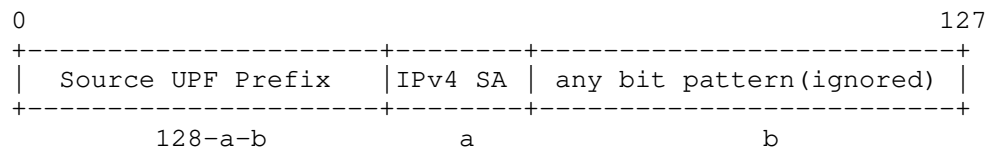


Figure 10: IPv6 SA Encoding for End.M.GTP4.E

#### 6.7. H.M.GTP4.D

The "SR Policy Headend with tunnel decapsulation and map to an SRv6 policy" behavior (H.M.GTP4.D for short) is used in the direction from legacy IPv4 user-plane to SRv6 user-plane network.

When the SR Gateway node N receives a packet destined to a IW-IPv4-Prefix, N does:

```

S01. IF Payload == UDP/GTP THEN
S02.   Pop the outer IPv4 header and UDP/GTP headers
S03.   Copy IPv4 DA, TEID to form SID B
S04.   Copy IPv4 SA to form IPv6 SA B'
S05.   Encapsulate the packet into a new IPv6 header   ;;Ref1
S06.   Set the IPv6 DA = B
S07.   Forward along the shortest path to B
S08. ELSE
S09.   Drop the packet

```

Ref1: The NH value is identified by inspecting the first nibble of the inner payload.

The SID B has the following format:

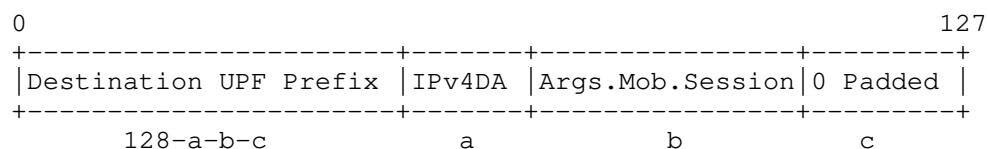


Figure 11: H.M.GTP4.D SID Encoding

The SID B MAY be an SRv6 Binding SID instantiated at the first UPF (U1) to bind an SR policy [I-D.ietf-spring-segment-routing-policy].

#### 6.8. End.Limit: Rate Limiting behavior

The mobile user-plane requires a rate-limit feature. For this purpose, we define a new behavior "End.Limit". The "End.Limit" behavior encodes in its arguments the rate limiting parameter that should be applied to this packet. Multiple flows of packets should have the same group identifier in the SID when those flows are in the same AMBR (Aggregate Maximum Bit Rate) group. The encoding format of the rate limit segment SID is as follows:

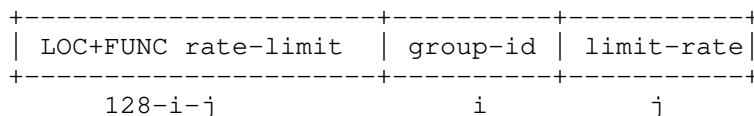


Figure 12: End.Limit: Rate limiting behavior argument format

If the limit-rate bits are set to zero, the node should not do rate limiting unless static configuration or control-plane sets the limit rate associated to the SID.

## 7. SRv6 supported 3GPP PDU session types

The 3GPP [TS.23501] defines the following PDU session types:

- \* IPv4
- \* IPv6
- \* IPv4v6
- \* Ethernet
- \* Unstructured

SRv6 supports the 3GPP PDU session types without any protocol overhead by using the corresponding SRv6 behaviors (End.DX4, End.DT4 for IPv4 PDU sessions; End.DX6, End.DT6, End.T for IPv6 PDU sessions; End.DT46 for IPv4v6 PDU sessions; End.DX2 for L2 and Unstructured PDU sessions).

## 8. Network Slicing Considerations

A mobile network may be required to implement "network slices", which logically separate network resources. User-plane behaviors represented as SRv6 segments would be part of a slice.

[I-D.ietf-spring-segment-routing-policy] describes a solution to build basic network slices with SR. Depending on the requirements, these slices can be further refined by adopting the mechanisms from:

- \* IGP Flex-Algo [I-D.ietf-lsr-flex-algo]
- \* Inter-Domain policies  
[I-D.ietf-spring-segment-routing-central-epe]

Furthermore, these can be combined with ODN/AS (On Demand Nexthop/ Automated Steering) [I-D.ietf-spring-segment-routing-policy] for automated slice provisioning and traffic steering.

Further details on how these tools can be used to create end to end network slices are documented in [I-D.ali-spring-network-slicing-building-blocks].

## 9. Control Plane Considerations

This document focuses on user-plane behavior and its independence from the control plane. While the SRv6 mobile user-plane behaviors may be utilized in emerging architectures, such as [I-D.gundavelli-dmm-mfa], [I-D.mhkk-dmm-srv6mup-architecture] for example, require control plane support for the user-plane, this document does not impose any change to the existent mobility control plane.

Section 11 allocates SRv6 Segment Endpoint Behavior codepoints for the new behaviors defined in this document.

## 10. Security Considerations

The security considerations for Segment Routing are discussed in [RFC8402]. More specifically for SRv6 the security considerations and the mechanisms for securing an SR domain are discussed in [RFC8754]. Together, they describe the required security mechanisms that allow establishment of an SR domain of trust to operate SRv6-based services for internal traffic while preventing any external traffic from accessing or exploiting the SRv6-based services.

The technology described in this document is applied to a mobile network that is within the SR Domain.

This document introduces new SRv6 Endpoint Behaviors. Those behaviors do not need any special security consideration given that it is deployed within that SR Domain.

## 11. IANA Considerations

The following values have been allocated within the "SRv6 Endpoint Behaviors" [RFC8986] sub-registry belonging to the top-level "Segment Routing Parameters" registry:

Value	Hex	Endpoint behavior	Reference
40	0x0028	End.MAP	[This.ID]
41	0x0029	End.Limit	[This.ID]
69	0x0045	End.M.GTP6.D	[This.ID]
70	0x0046	End.M.GTP6.Di	[This.ID]
71	0x0047	End.M.GTP6.E	[This.ID]
72	0x0048	End.M.GTP4.E	[This.ID]

Table 1: SRv6 Mobile User-plane Endpoint Behavior Types

## 12. Acknowledgements

The authors would like to thank Daisuke Yokota, Bart Peirens, Ryokichi Onishi, Kentaro Ebisawa, Peter Bosch, Darren Dukes, Francois Clad, Sri Gundavelli, Sridhar Bhaskaran, Arashmid Akhavain, Ravi Shekhar, Aeneas Dodd-Noble, Carlos Jesus Bernardos, Dirk v. Hugo and Jeffrey Zhang for their useful comments of this work.

## 13. Contributors

Kentaro Ebisawa Toyota Motor Corporation Japan

Email: [ebisawa@toyota-tokyo.tech](mailto:ebisawa@toyota-tokyo.tech)

Tetsuya Murakami Arrcus, Inc. United States of America

Email: [tetsuya.ietf@gmail.com](mailto:tetsuya.ietf@gmail.com)

## 14. References

### 14.1. Normative References

- [I-D.ietf-spring-segment-routing-policy]  
Filsfils, C., Talaulikar, K., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", Work in Progress, Internet-Draft, draft-ietf-spring-segment-routing-policy-22, 22 March 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-spring-segment-routing-policy-22>>.
- [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>>.
- [RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <<https://www.rfc-editor.org/info/rfc8754>>.

- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <<https://www.rfc-editor.org/info/rfc8986>>.
- [TS.23501] 3GPP, "System Architecture for the 5G System", 3GPP TS 23.501 15.0.0, November 2017.

#### 14.2. Informative References

- [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", Work in Progress, Internet-Draft, draft-ali-spring-network-slicing-building-blocks-04, 21 February 2021, <<https://datatracker.ietf.org/doc/html/draft-ali-spring-network-slicing-building-blocks-04>>.
- [I-D.camarilloelmalky-springdmm-srv6-mob-usecases]  
Garvia, P. C., Filsfils, C., Elmalky, H., Matsushima, S., Voyer, D., Cui, A., and B. Peirens, "SRv6 Mobility Use-Cases", Work in Progress, Internet-Draft, draft-camarilloelmalky-springdmm-srv6-mob-usecases-02, 15 August 2019, <<https://datatracker.ietf.org/doc/html/draft-camarilloelmalky-springdmm-srv6-mob-usecases-02>>.
- [I-D.gundavelli-dmm-mfa]  
Gundavelli, S., Liebsch, M., and S. Matsushima, "Mobility-aware Floating Anchor (MFA)", Work in Progress, Internet-Draft, draft-gundavelli-dmm-mfa-01, 19 September 2018, <<https://datatracker.ietf.org/doc/html/draft-gundavelli-dmm-mfa-01>>.
- [I-D.ietf-lsr-flex-algo]  
Psenak, P., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", Work in Progress, Internet-Draft, draft-ietf-lsr-flex-algo-19, 7 April 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-lsr-flex-algo-19>>.
- [I-D.ietf-spring-segment-routing-central-epe]  
Filsfils, C., Previdi, S., Dawra, G., Aries, E., and D. Afanasiev, "Segment Routing Centralized BGP Egress Peer Engineering", Work in Progress, Internet-Draft, draft-ietf-spring-segment-routing-central-epe-10, 21 December 2017, <<https://datatracker.ietf.org/doc/html/draft-ietf-spring-segment-routing-central-epe-10>>.

- [I-D.ietf-spring-sr-service-programming]  
Clad, F., Xu, X., Filsfils, C., Bernier, D., Li, C.,  
Decraene, B., Ma, S., Yadlapalli, C., Henderickx, W., and  
S. Salsano, "Service Programming with Segment Routing",  
Work in Progress, Internet-Draft, draft-ietf-spring-sr-  
service-programming-05, 10 September 2021,  
<<https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-service-programming-05>>.
- [I-D.kohno-dmm-srv6mob-arch]  
Kohno, M., Clad, F., Camarillo, P., and Z. Ali,  
"Architecture Discussion on SRv6 Mobile User plane", Work  
in Progress, Internet-Draft, draft-kohno-dmm-srv6mob-arch-  
05, 8 November 2021,  
<<https://datatracker.ietf.org/doc/html/draft-kohno-dmm-srv6mob-arch-05>>.
- [I-D.matsushima-spring-srv6-deployment-status]  
Matsushima, S., Filsfils, C., Ali, Z., Li, Z., Rajaraman,  
K., and A. Dhamija, "SRv6 Implementation and Deployment  
Status", Work in Progress, Internet-Draft, draft-  
matsushima-spring-srv6-deployment-status-15, 5 April 2022,  
<<https://datatracker.ietf.org/doc/html/draft-matsushima-spring-srv6-deployment-status-15>>.
- [I-D.mhkk-dmm-srv6mup-architecture]  
Matsushima, S., Horiba, K., Khan, A., Kawakami, Y.,  
Murakami, T., Patel, K., Kohno, M., Kamata, T., Garvia, P.  
C., Voyer, D., Zadok, S., Meilik, I., Agrawal, A.,  
Perumal, K., and J. Horn, "Segment Routing IPv6 Mobile  
User Plane Architecture for Distributed Mobility  
Management", Work in Progress, Internet-Draft, draft-mhkk-  
dmm-srv6mup-architecture-03, 20 March 2022,  
<<https://datatracker.ietf.org/doc/html/draft-mhkk-dmm-srv6mup-architecture-03>>.
- [I-D.murakami-dmm-user-plane-message-encoding]  
Murakami, T., Matsushima, S., Ebisawa, K., Camarillo, P.,  
and R. Shekhar, "User Plane Message Encoding", Work in  
Progress, Internet-Draft, draft-murakami-dmm-user-plane-  
message-encoding-05, 5 March 2022,  
<<https://datatracker.ietf.org/doc/html/draft-murakami-dmm-user-plane-message-encoding-05>>.
- [TS.29281] 3GPP, "General Packet Radio System (GPRS) Tunnelling  
Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 15.1.0,  
December 2017.

[TS.38415] 3GPP, "Draft Specification for 5GS container (TS 38.415)",  
3GPP R3-174510 0.0.0, August 2017.

## Appendix A. Implementations

This document introduces new SRv6 Endpoint Behaviors. These behaviors have an open-source P4 implementation available in <https://github.com/ebiken/p4srv6>.

Additionally, a full implementation of this document is available in Linux Foundation FD.io VPP project since release 20.05. More information available here: [https://docs.fd.io/vpp/20.05/d7/d3c/srv6\\_mobile\\_plugin\\_doc.html](https://docs.fd.io/vpp/20.05/d7/d3c/srv6_mobile_plugin_doc.html).

There are also experimental implementations in M-CORD NGIC and Open Air Interface (OAI).

## Authors' Addresses

Satoru Matsushima (editor)  
SoftBank  
Japan  
Email: [satoru.matsushima@g.softbank.co.jp](mailto:satoru.matsushima@g.softbank.co.jp)

Clarence Filsfils  
Cisco Systems, Inc.  
Belgium  
Email: [cf@cisco.com](mailto:cf@cisco.com)

Miya Kohno  
Cisco Systems, Inc.  
Japan  
Email: [mkohno@cisco.com](mailto:mkohno@cisco.com)

Pablo Camarillo Garvia (editor)  
Cisco Systems, Inc.  
Spain  
Email: [pcamaril@cisco.com](mailto:pcamaril@cisco.com)

Daniel Voyer  
Bell Canada  
Canada  
Email: [daniel.voyer@bell.ca](mailto:daniel.voyer@bell.ca)



Charles E. Perkins  
Lupin Lodge  
20600 Aldercroft Heights Rd.  
Los Gatos, CA 95033  
United States of America  
Email: charliep@computer.org

DMM Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 6, 2022

U. Chunduri, Ed.  
Intel Corporation  
J. Kaippallimalil, Ed.  
Futurewei  
S. Bhaskaran  
Altiostar  
J. Tantsura  
Microsoft  
P. Muley  
Nokia  
March 5, 2022

Mobility aware Transport Network Slicing for 5G  
draft-ietf-dmm-tn-aware-mobility-03

Abstract

This document specifies a framework and mapping of slices in 5G mobile systems to transport network slices in IP, Layer 2 or Layer 1 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 are mapped to transport network slice include bandwidth, latency and criteria such as isolation, directionality and disjoint routes. Mobile slice criteria are 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 a mobile network slice is mapped to a slice in IP or Layer 2 transport network between 3GPP provisioning end points. The same mapping mechanisms apply during initial UE session setup and following UE mobility. Applicability of this framework and underlying transport networks, which can enable different slice properties are 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

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 September 6, 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. IETF Network Slicing Terminology . . . . .	4
1.2. Problem Statement . . . . .	5
1.3. Solution Approach . . . . .	5
1.4. Acronyms . . . . .	5
2. Transport and Slice aware Mobility in 5G Networks . . . . .	7
2.1. Backhaul and Mid-Haul Transport Network . . . . .	8
2.1.1. IETF Network Slicing Applicability . . . . .	10
2.1.2. Fronthaul Transport Network . . . . .	10
2.2. Mobile Transport Network Context (MTNC) and Scalability .	10
2.3. Transport Network Function (TNF) . . . . .	11
2.4. Transport Provisioning . . . . .	12
2.5. MTNC-ID in the Data Packet . . . . .	13
2.6. Functionality for E2E Management . . . . .	15

3.	Transport Network Underlays . . . . .	16
3.1.	Applicability . . . . .	16
3.2.	Transport Network Technologies . . . . .	18
4.	Acknowledgements . . . . .	19
5.	IANA Considerations . . . . .	19
6.	Security Considerations . . . . .	19
7.	Contributing Authors . . . . .	19
8.	References . . . . .	19
8.1.	Normative References . . . . .	20
8.2.	Informative References . . . . .	20
Appendix A.	New Control Plane and User Planes . . . . .	22
A.1.	Slicing Framework and RAN Aspects . . . . .	22
A.2.	Slice aware Mobility: Discrete Approach . . . . .	23
Authors' Addresses	. . . . .	23

## 1. Introduction

The 3GPP architecture for 5GS defined in [TS.23.501-3GPP], [TS.23.502-3GPP] and [TS.23.503-3GPP] for 5GC (5G Core) and the NG-RAN architecture and procedures defined in [TS.38.300-3GPP] and [TS.38.401-3GPP] include procedures for setting up network slices in the 3GPP network.

3GPP has defined slice types to cover enhanced mobile broadband (eMBB) communications, ultra-reliable low latency communications (URLLC) and massive internet of things (mIoT) and may extend to include new slice types as needed. ATIS [ATIS075] has defined an additional slice type for V2X services. 3GPP slicing and RAN aspects are further described Appendix A.1.

3GPP slice types and multiple instances of a slice type satisfy various characteristics for 5G network resources. A slice in 3GPP is a logical chunk of 3GPP network resources that is dynamically created and may include core network control and user plane functions as well as access network functions. A slice instance that spans user plane network functions including the UPF (User Plane Function), gNB-CU (generalized Node-B Centralized Unit) and gNB-DU (generalized Node-B Distributed Unit) and its interfaces N3, N9, F1-U) are clearly defined, however:

- o 3GPP standards do not specify the underlying IP transport network capabilities or slices thereof.
- o Though 3GPP standards define how interfaces N3, N9, F1-U are reselected following mobility but do not specify the underlying transport network reselection aspects following mobility.

- o 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.

IP transport is used to interconnect the data forwarding entities UPFs, gNB-CU and gNB-DU in the 5GC and NG-RAN architecture but 3GPP specifications only define the interfaces (N3, N9, F1U etc.) and the 3GPP transport end points [TS.28.541-3GPP]. The architecture allows the flexibility to dynamically place Branching Point (BP) and Uplink Classifier (ULCL) UPFs closer to the access network (5G-AN). The 5G-AN can be a radio access network (NG-RAN) or any non-3GPP access network, for example, WLAN. The resources of gNB-CU and gNB-DU corresponding to a slice in a 5G radio access network (NG-RAN) may be interconnected using a Layer 2 or IP network transport.

A transport underlay across 3GPP interfaces N3, N9 and F1U may use multiple technologies or network providers on path and the slice in 3GPP domain should have a corresponding mapping in the transport domain. This document proposes to map a slice in the 3GPP domain to a transport domain slice. Key considerations including simplicity (e.g., use of L2 VLAN), routed networks on path (i.e., IP based mapping), efficiency of inspecting the slice mapping parameter and others are described in subsequent sections.

#### 1.1. IETF Network Slicing Terminology

[I-D.ietf-teas-ietf-network-slices] draft defines the 'IETF Network slice', its scope and characteristics. It lists use cases where IETF technologies can be used for slicing solutions, for various connectivity segments. Transport slice terminology as used in this document refers to the connectivity segment between various 5G systems (i.e. 5G-AN which includes NG-RAN, ULCL UPF, BP UPF and PSA UPF) and some of these segments are referred to as IETF Network slices.

[I-D.ietf-teas-ietf-network-slices] also defines a generic framework and how abstract requests to set up slices can be mapped to more specific technologies (e.g., VPN and traffic-engineering technologies). This document is aimed to be specific to 3GPP use case where many such connectivity segments are used in E2E slicing solutions. Some of the terminologies defined in these referred drafts and applicability to this document are further described in Section 2.1.1.

## 1.2. Problem Statement

- o The 5G System (5GS) as defined in 3GPP specifications, does not consider the resources and functionalities needed from the transport network for the path between UPF, gNB corresponding to the N3, N9 and F1-U interfaces. The lack of underlying Transport Network (TN) awareness in 3GPP 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).
- o Meeting the specific slice characteristics on the F1-U, N3 and N9 interfaces depends on the IP transport underlay providing these resources and capabilities. There should also be a means by which 3GPP slices are mapped to corresponding transport network slices and the means to carry this mapping in N3, N9, F1-U packets over the transport network. This is needed to meet SLAs for real-time, mission-critical or latency sensitive services.
- o 3GPP defines configuration for its transport end-points in [TS.28.541-3GPP]. These end-points may be for Layer 2 alternatives such as VLAN or L3/routed networks on the F1-U, N3 or N9 path based on desired capabilities. When L3/routed networks and IP transport are used, IP header fields like DSCP are not sufficient as they convey QoS but not the other aspects like isolation or protection. Other fields and extensions to carry a slice mapping, simplicity of lookup, implementation and scale are discussed in Section 2.

## 1.3. Solution Approach

This document specifies an approach to fulfil the needs of 5GS to transport user plane traffic from 5G-AN (including NG-RAN) to UPF in an optimized fashion. This is done by keeping establishment and mobility procedures aware of the 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.

## 1.4. 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 - User plane (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
NG-RAN	-	Next Generation Radio Access Network (i.e., gNB, NG-eNB - RAN functions which connect to 5GC)
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 (i.e 3GPP radio access network used synonymously with NG-RAN in this document)
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 and is provided here for information. The application of 5GS slices in transport network for backhaul, mid-haul and front haul are not explicitly covered in 3GPP and is the topic here. 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 the 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.

The figure shows the entities on path for 3GPP Network Functions (gNB-DU, gNB-CU, UPF) to obtain slice aware classification from an IP/L2 transport network.



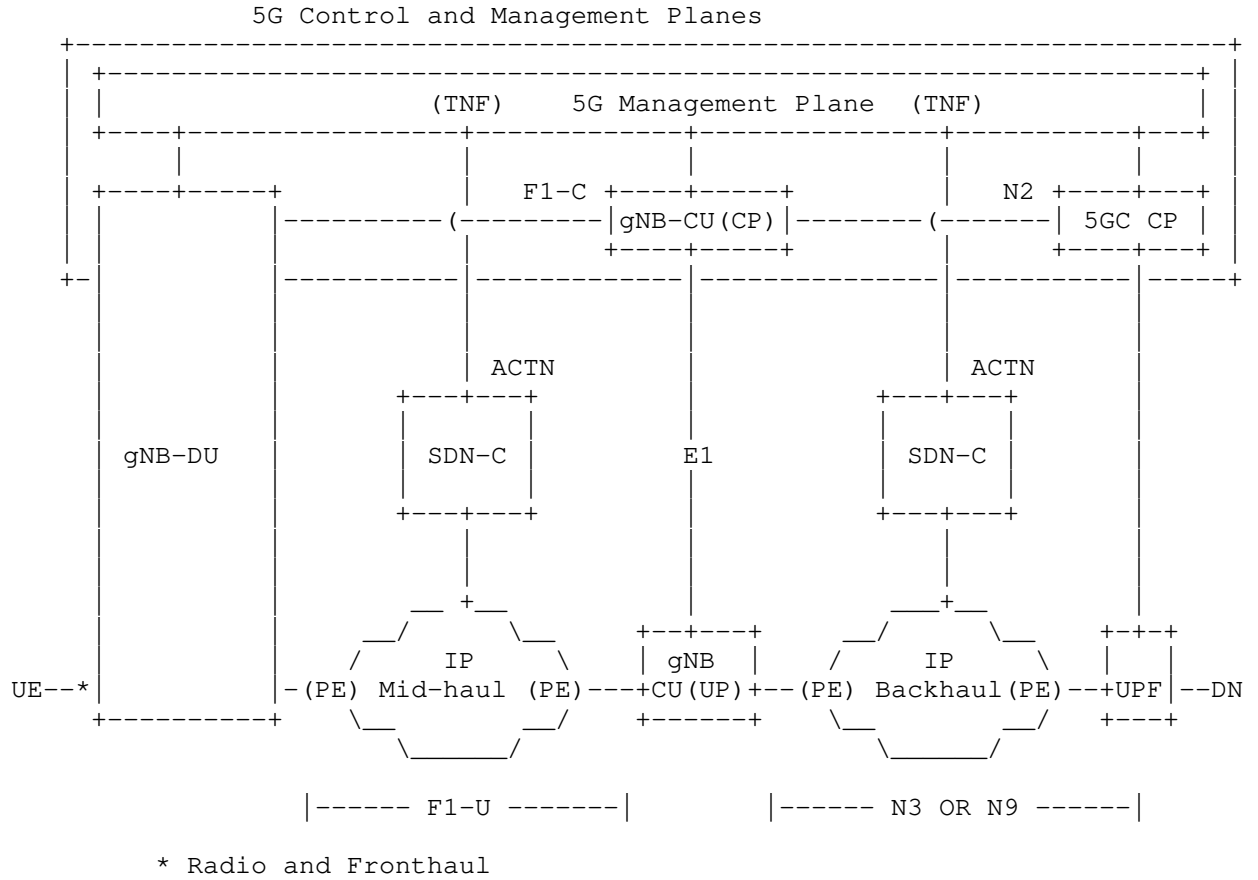


Figure 1: Backhaul and Mid-haul Transport Network for 5G

### 2.1. Backhaul and Mid-Haul Transport Network

Figure 1 depicts IP Xhaul network with SDN-C and PE (Provider Edge) routers providing 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 are estimated and provisioned by the functionality as specified in Section 2.3 (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 may be 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-U 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 2.1.2, 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-U 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 2.4.

#### 2.1.1. IETF Network Slicing Applicability

Some of the functional elements depicted in the Figure 1 can be mapped to the terminology set forth in the [I-D.ietf-teas-ietf-network-slices]. From 3GPP perspective, UE and UPF are the network slice endpoints and routers, gNB-DU, gNB-CU, switches, PE nodes are the slice realization endpoints. The TNF represented in the Figure 1 can be seen as IETF Network Slice Controller (NSC) functionality and SDN-C maps to Network Controller (NC). NSC-NBI interface is the interface from 3GPP Management plane (e.g., NSSF) and NSC-SBI interface is the interface between TNF and SDN-C. Various possibilities for implementation of these interfaces and the relation to ACTN are also further described in the [I-D.ietf-teas-ietf-network-slices].

#### 2.1.2. Fronthaul 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 can be 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 a UDP based fronthaul interface, the slice information can be 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.

#### 2.2. Mobile Transport Network Context (MTNC) and Scalability

The MTNC represents a slice of a transport path for a tenant between two 3GPP user plane functions. The Mobile-Transport Network Context Identifier (MTNC-ID) is generated by the TNF to be unique for each instance (for a tenant) and per traffic class (including QoS and slice aspects). Thus, there may be more than one MTNC-ID for the same QoS and instance if there is a need to provide isolation (slice)

of the traffic. It should be noted that MTNC are per class/instance and not per user session. The MTNC-IDs are configured by the TNF to be unique within a provisioning domain.

Since the MTNC-IDs are generated per instance / tenant, there is no need for unique MTNC-IDs per flow/session. In addition, since the traffic estimation is performed prior to UE's session establishment, there is no provisioning delay experienced by the UE during its session setup. For an instance/tenant, the MTNC-ID space scales roughly as a square of the number sites between which 3GPP user plane functions have paths. If there are T traffic classes and C Tenants, the number of MTNC-IDs in a fully meshed network is  $T * C$ . An MTNC-ID space of 16 bits (65K identifiers) can be expected to be sufficient.

### 2.3. 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 2.6 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.

#### 2.4. 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 instances 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.

## 2.5. 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. If the fronthaul, midhaul or backhaul IP path is bounded by an L2 network, one option maybe to use VLANs to carry the MTNC-ID. 3GPP specifications for management plane defines transport end-points configuration in [TS.28.541-3GPP]. However, Layer 2 alternatives such as VLAN will fail in L3/routed networks on the F1-U, N3 or N9 path. GTP-U (F1-U, N3, N9 encapsulation header) field extensions offer a possibility, however these extensions are not always easy 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.)

While IPv6 extension headers like SRv6 may be an option to carry the MTNC-ID that requires the end-to-end network to be IPv6 as well as the capability to lookup the extension header at line rate. To minimise the protocol changes 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. The UDP port information containing MTNC-ID is a simple extension that can be provisioned in 3GPP transport end-points defined in [TS.28.541-3GPP]. 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 the 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-U 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 on 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 Alliance 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 slices 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 2.1.2. On the UDP based fronthaul transport network, the UDP source port can be used to carry the MTNC-ID.

## 2.6. 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:

- o 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.
- o For transport slice assignment for various SSTs (eMBB, URLLC, MIIOT) corresponding underlay paths need to be created and monitored from each transport endpoint (CSR and PE@UPF).
- o 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.
- o 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.
- o Mapping of PDU session parameters to underlay SST paths need to be done. One way to do this is 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 2.4, Section 2.5 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 2.5.
- o 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.



- o Continuous monitoring of the underlying transport path characteristics should be enabled at the endpoints (technologies for monitoring depends on 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.
- o During UE mobility events 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 requires 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 a 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

- o 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 2.4) 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

- o 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.
- o Same set of TE Paths are created uniformly across all needed 5G-ANs and UPFs to allow various mobility scenarios.
- o 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.
- o 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 available, this section 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 provide TE benefits needed for 5G slices from a 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.

Richard Li  
Futurewei  
2330 Central Expressway  
Santa Clara  
CA 95050  
USA  
Email: richard.li@futurewei.com

Luis M. Contreras  
Telefonica  
Sur-3 building, 3rd floor  
Madrid 28050  
Spain  
Email: luismiguel.contrerasmurillo@telefonica.com

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-04 (work in progress), November 2020.
- [I-D.ietf-dmm-srv6-mobile-uplane] Matsushima, S., Filsfils, C., Kohno, M., Garvia, P. C., Voyer, D., and C. E. Perkins, "Segment Routing IPv6 for Mobile User Plane", draft-ietf-dmm-srv6-mobile-uplane-18 (work in progress), February 2022.
- [I-D.ietf-teas-ietf-network-slices] Farrel, A., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "Framework for IETF Network Slices", draft-ietf-teas-ietf-network-slices-07 (work in progress), March 2022.
- [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.28.541-3GPP]  
3rd Generation Partnership Project (3GPP), "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3 (Release 17)", June 2020.

[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)  
Intel Corporation  
2191 Laurelwood Rd  
Santa Clara, CA 95054  
USA

Email: [umac.ietf@gmail.com](mailto:umac.ietf@gmail.com)

John Kaippallimalil (editor)  
Futurewei

Email: [john.kaippallimalil@futurewei.com](mailto:john.kaippallimalil@futurewei.com)

Sridhar Bhaskaran  
Altiostar

Email: [sridharb@altistar.com](mailto:sridharb@altistar.com)

Jeff Tantsura  
Microsoft

Email: [jefftant.ietf@gmail.com](mailto:jefftant.ietf@gmail.com)

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

Email: [praveen.muley@nokia.com](mailto:praveen.muley@nokia.com)

Internet Engineering Task Force  
Internet-Draft  
Intended status: Standards Track  
Expires: 20 September 2022

S. Matsushima  
K. Horiba  
A. Khan  
Y. Kawakami  
SoftBank  
T. Murakami  
K. Patel  
Arrcus, Inc  
M. Kohno  
T. Kamata  
P. Camarillo  
Cisco Systems, Inc.  
D. Voyer  
Bell Canada  
S. Zadok  
I. Meilik  
Broadcom  
A. Agrawal  
K. Perumal  
Intel  
J. Horn  
Cisco Systems, Inc.  
19 March 2022

Segment Routing IPv6 Mobile User Plane Architecture for Distributed  
Mobility Management  
draft-mhkk-dmm-srv6mup-architecture-03

Abstract

This document defines the Segment Routing IPv6 Mobile User Plane (SRv6 MUP) architecture for Distributed Mobility Management. The requirements for Distributed Mobility Management described in [RFC7333] can be satisfied by routing fashion.

Mobile services are deployed over several parts of IP networks. A Segment Routing over IPv6 (SRv6) network can accommodate all, or part of those networks thanks to the large address space of IPv6 and the network programming capability described in [RFC8986].

Segment Routing IPv6 Mobile User Plane Architecture can incorporate existing session based mobile networks. By leveraging SRv6 network programmability, mobile user plane can be integrated into the SRv6 data plane. In that routing paradigm, session information between the entities of the mobile user plane is turned to routing information.

## 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 20 September 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	3
1.1. Requirements Language . . . . .	5
2. Terminology . . . . .	5
3. Architecture Overview . . . . .	5
4. Mobile User Plane Segment . . . . .	6
5. Distribution of Mobile User Plane Segment Information . . . . .	7
5.1. Direct Segment Discovery Route . . . . .	7
5.2. Interwork Segment Discovery Route . . . . .	8
6. Distribution of Session Transformed Route . . . . .	8
6.1. Type 1 Session Transformed Route . . . . .	9
6.2. Type 2 Session Transformed Route . . . . .	9
6.3. MUP Controller . . . . .	9
7. Illustration . . . . .	10
8. IANA Considerations . . . . .	15
9. Security Considerations . . . . .	16

10. References . . . . .	16
10.1. Normative References . . . . .	16
10.2. Informative References . . . . .	16
Authors' Addresses . . . . .	17

## 1. Introduction

Mobile services require IP connectivity for communication between the entities of mobile service architecture [RFC5213][TS.23501]. To provide the IP connectivity, Segment Routing (SR) [RFC8402] can be a candidate solution.

In PMIPv6 [RFC5213], IP connectivity between LMA and MAG can be provided over SR networks, as well as LMA and Internet. In 3GPP 5G [TS.23501], IP connectivity for N3 interface between gNodeB(es) and UPFs can also be provided by SR, as well as for N6 interface between UPFs and DNS (Data Network).

These IP connectivities may be covered by multiple SR networks, or just one SR network, depending on the size of the deployment. In the latter case, it is expected that the address space of the SR network should be large enough to cover a vast number of nodes, such as millions of base stations. For this reason, use of IPv6 for the SR dataplane looks sufficiently suitable.

SRv6 is an instantiation of SR over IPv6 dataplane in which a single network can accommodate all entities of mobile services thanks to the huge available address space and network programming capability described in [RFC8986].

Meanwhile, SRv6 network programmability enhances SRv6 dataplane to be integrated with mobile user plane [I-D.ietf-dmm-srv6-mobile-uplane]. It will make an entire SRv6 network support the user plane in a very efficient distributed routing fashion.

On the other hand, the requirements for Distributed Mobility Management (DMM) described in [RFC7333] can be satisfied by session management based solutions. [RFC8885] defines protocol extension to PMIPv6 for the DMM requirements. 3GPP 5G defines an architecture in which multiple session anchors can be added to one mobility session by the session management.

As a reminder, the user plane related requirements in [RFC7333] are reproduced here:

REQ1: Distributed mobility management  
IP mobility, network access solutions, and forwarding  
solutions provided by DMM MUST enable traffic to avoid

traversing a single mobility anchor far from the optimal route. It is noted that the requirement on distribution applies to the data plane only.

REQ3: IPv6 deployment

DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, particularly in situations where private IPv4 addresses and/or NATs are used.

REQ4: Existing mobility protocols

A DMM solution MUST first consider reusing and extending IETF standard protocols before specifying new protocols.

REQ5: Coexistence with deployed networks/hosts and operability across different networks

A DMM solution may require loose, tight, or no integration into existing mobility protocols and host IP stacks. Regardless of the integration level, DMM implementations MUST be able to coexist with existing network deployments, end hosts, and routers that may or may not implement existing mobility protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when the needed mobility management signaling, forwarding, and network access are allowed by the trust relationship between them.

This document defines the Segment Routing IPv6 Mobile User Plane (SRv6 MUP) architecture for Distributed Mobility Management. SRv6 MUP is not a mobility management system itself, but an architecture to integrate mobile user plane into the SRv6 data plane.

In this routing paradigm, session information from a mobility management system will be transformed to routing information. It means that mobile user plane specific nodes for the anchor or intermediate points are no longer required. The user plane anchor and intermediate functions can be supported by SR throughout an SR domain (REQ1), not to mention that SRv6 MUP will naturally be deployed over IPv6 networks (REQ3).

SRv6 MUP architecture is independent from the mobility management system. For the requirements (REQ4, 5), SRv6 MUP architecture is designed to be pluggable user plane part of existing mobile service architectures. Those existing architectures are for example defined in [RFC5213], [TS.23501], or if any.

The level of SRv6 MUP integration for mobile networks running based on the existing architecture will be varied and depending on the level of SRv6 awareness of the control and user plane entities.

Specifying how to modify the existing architecture to integrate SRv6 MUP is out of scope of this document. What this document provides for the existing architecture is an interface for SRv6 MUP which the existing or future architectures can easily integrate.

### 1.1. 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 RFC 2119 [RFC2119].

## 2. Terminology

MUP: Mobile User Plane

MUP Segment: Representation of mobile user plane segment

PE: Provider Edge node in an SR network

MUP Controller: Controller node for an SR network

UE: User Equipment, as per [TS.23501]

MN: Mobile Node, as per [RFC5213]

## 3. Architecture Overview

SRv6 MUP architecture defined in this document introduces new segment types of MUP segment called "Direct segment", and "Interwork Segment". An SR node of PE accommodates an Interwork Segment and/or a Direct Segment. Figure 1 depicts the overview.

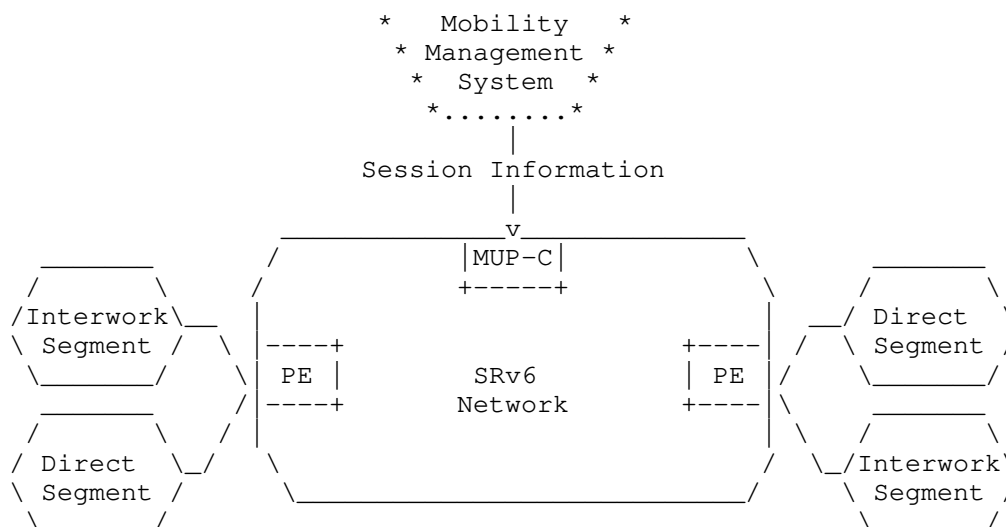


Figure 1: Overview of SRv6 MUP Architecture

This document also defines new routing information called "Segment Discovery route" and "Session Transformed route". To carry these new routing information, this architecture requires extending the existing routing protocols. Any routing protocol can be used to carry this information but this document recommends using BGP. Thus, this document describes extensions on BGP as an example.

#### 4. Mobile User Plane Segment

This document defines two new types of Mobile User Plane (MUP) segment. A MUP segment represents a network segment consisting of a mobile service. The MUP segment can be created by a PE which provides connectivity for the mobile user plane.

Direct Segment is a type of MUP segment that provides connectivity between MUP segments through the SRv6 network. Interwork Segment is another type of MUP segment. It provides connectivity between a user plane protocol of existing or future mobile service architecture and other MUP segments through the SRv6 networks.

An SRv6 SID (Segment Identifier) can represent a MUP segment. The SID can be any behavior defined in [RFC8986], [I-D.ietf-dmm-srv6-mobile-uplane], or any other extensions for further use cases. The behavior of the MUP segment will be chosen by the role of the representing MUP segment.

For example, in case of a PE interfaces to 5G user plane on the access side defined as "N3" in [TS.23501], the PE accommodates the N3 network as Interwork Segment in a routing instance and then the behavior of created segment SID by the PE will be "End.M.GTP4.E", or "End.M.GTP6.E". In this case, the PE may associate the SID to the routing instance for the N3 access network (N3RAN).

Another example here is that a PE interfaces to 5G DN on the core side defined as "N6" in [TS.23501], the PE accommodates the N6 network in a routing instance as Direct Segment and then the behavior of the created segment SID by the PE will be "End.DT4", "End.DT6", or "End.DT2". In this case, the PE may associate the SID to the routing instance for the N6 data network (N6DN).

## 5. Distribution of Mobile User Plane Segment Information

Distribution of MUP segment information can be done by advertising routing information with the MUP segment for mobile service. A PE distributes MUP segment information when a MUP segment is connected to the PE.

A MUP Segment Discovery route is routing information that associates the MUP segment with network reachability. This document defines the basic discovery route types, Direct Segment Discovery route, and Interwork Segment Discovery route. Other types of segment discovery route may be mobile service architecture specific. Defining the architecture specific network reachability is out of scope of this document and it will be specified in another document.

### 5.1. Direct Segment Discovery Route

When a PE accommodates a network through an interface or a routing instance as a Direct Segment, the PE advertises the corresponding Direct Segment Discovery route for the interface or the routing instance. The Direct Segment Discovery route includes an address of the PE in the network reachability information with an extended community indicating the corresponding Direct Segment, and SID of the routing instance to the SR domain.

For example in 3GPP 5G specific case, an PE may connect to N6 interface on a DN side, an MUP Segment Discovery route for the DN will be advertised with an address of the PE, corresponding SID and Direct Segment extended community to the routing instance for the DN from the PE.

When a PE receives a Direct Segment Discovery route from other PEs, the PE keeps the received Direct Segment Discovery route in the RIB. The PE uses the received Direct Segment Discovery route to resolve



Type 2 session transformed routes reachability, described in Section 6.2. If the Direct Segment Discovery route resolves reachability for the endpoints, and match the Direct Segment extended community of the Type 2 session transformed routes, the PE updates the FIB entry for the Type 2 session transformed route with the SID of the matched Direct Segment Discovery route.

## 5.2. Interwork Segment Discovery Route

When a PE accommodates a network through an interface or a routing instance for the user plane protocol of the mobile service architecture as an Interwork Segment, the PE advertises the corresponding Interwork Segment Discovery route with the prefixes of the Interwork Segment and the corresponding SID of the prefixes to the SR domain.

For example in 3GPP 5G specific case, an Interwork Segment Discovery route for N3 network accommodating RAN will be incorporated in an N3RAN segment discovery route associated with a RAN segment SID.

When a PE receives a Interwork Segment Discovery route, the PE keeps the received Interwork Segment Discovery routes in the RIB. The PE uses the received Interwork Segment Discovery routes to resolve the reachability for remote endpoint of Type 1 session transformed routes, described in Section 6.1. If the Interwork Segment Discovery route resolves the reachability for Type 1 session transformed routes, the PE updates the FIB entry for the prefix of Type 1 session transformed route with the SID of the matched MUP segment discovery route.

The received Interwork Segment Discovery routes MUST be used only to resolve reachability for the remote endpoints of Type 1 session transformed routes. The connectivity among the routing instances for Interwork Segments may be advertised as VPN routes. This is to avoid forwarding entries to the prefixes of Interwork Segment mingled in the other type of routing instance. A PE may discard the received Interwork segment discovery route if the Route Target extended communities of the route does not meet the PE's import policy.

## 6. Distribution of Session Transformed Route

SRv6 MUP architecture defines two types of session transformed route.

### 6.1. Type 1 Session Transformed Route

First type route, called Type 1 Session Transformed route, encodes IP prefix(es) for a UE or MN in a BGP MP-NLRI attribute with associated session information of the tunnel endpoint identifier on the access side. The MUP controller advertises the Type 1 Session Transformed route with the Route Target extended communities for the UE or MN to the SR domain.

A PE may receive the Type 1 Session Transformed routes from the MUP Controller in the SR domain. The PE may keep the received Type 1 Session Transformed routes advertised from the MUP Controller. The receiving PE will perform the importing of the received Type 1 Session Transformed routes in the configured routing instances based on the Route Target extended communities. A PE may discard the received Type 1 Session Transformed route if the PE fails to import the route based on the Route Target extended communities.

### 6.2. Type 2 Session Transformed Route

Second type route, called Type 2 Session Transformed route, encodes the tunnel endpoint identifier of the session on the core side in a BGP MP-NLRI attribute with the nature of tunnel decapsulation. Longest match algorithm for the prefix in this type of session transformed route should be applicable to aggregate the routes for scale. The MUP controller advertises the Type 2 Session Transformed route with the Route Target and Direct Segment extended communities for the endpoint to the SR domain.

A PE may receive the Type 2 Session Transformed routes from the MUP Controller in the SR domain. The PE may keep the received Type 2 Session Transformed routes advertised from the MUP Controller. The receiving PE will perform the importing of the received Type 2 Session Transformed routes in the configured routing instances based on the Route Target extended communities. A PE may discard the received Type 2 Session Transformed route if the PE fails to import the route based on the Route Target extended communities.

### 6.3. MUP Controller

A MUP controller provides a northbound API. A consumer of the API inputs session information for a UE or a MN from mobility management system. The MUP controller transforms the received session information to routing information and will advertise the session transformed routes with the corresponding extended communities to the SR domain.

The received session information is expected to include the UE or MN IP prefix(es), tunnel endpoint identifiers for both ends, and any other attributes for the mobile networks. For example in a 3GPP 5G specific case, the tunnel endpoint identifier will be a pair of the F-TEIDs on both the N3 access side (RAN) and core side (UPF).

## 7. Illustration

This section shows an illustration of SRv6 MUP deployment. The example deployment cases here is 3GPP 5G.

Before enabling SRv6 MUP, how SRv6 networks can accommodate existing mobile network service shown in Figure 2. The PE's of S1, S2, and S3 join an SR network. A routing instance is configured to each network of the mobile service. N6DN in S1 and S2 are supposed to provide connectivity to edge servers and the Internet respectively.

VRF (Virtual Routing Forwarding) is the routing instance to accommodate MUP segments in this section. All example cases in this section follow the typical routing policy control using the BGP extended community described in [RFC4360] and [RFC4684]

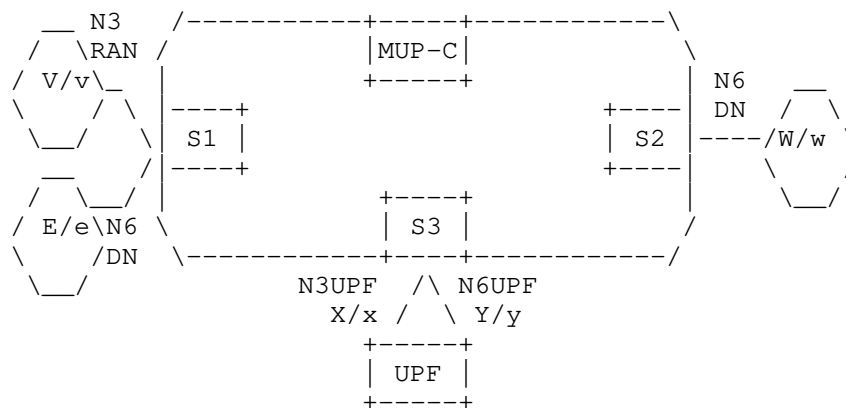


Figure 2

The following routing instances are configured:

- \* N3RAN in S1
  - export route V/v with route-target (RT) community C1
  - import routes which have route-target (RT) community C1 and C2
- \* N6DN in S1

- export route E/e with RT C4
- import routes which have RT C3 and C4
- \* N6DN in S2
  - export route W/w with RT C4
  - import routes which have RT C3 and C4
- \* N3UPF in S3
  - export route X/x with RT C2
  - import routes which have RT C1
- \* N6UPF in S3
  - export route Y/y with RT C3
  - import routes which have RT C4

Note: The above configurations are just to provide typical IP connectivity for 3GPP 5G. When the above configurations have been done, each endpoint in V/v and X/x can communicate through S1 and S3, but they can not communicate with nodes in E/e, W/w and Y/y.

Here, the PEs are configured to enable SRv6 MUP as following:

- \* S1
  - advertises Interwork type discovery route: V/v with SID S1::
  - set S1:: behavior End.M.GTP4.E or End.M.GTP6.E
- \* S1
  - advertise Direct type discovery route: MUP Direct Segment community D1 and SID S1:1::
  - set S1:1:: behavior End.DT4 or End.DT6 for the N6DN in S1
- \* S2
  - advertise Direct type route: MUP Direct Segment community D1 and SID S2::

- set S2:: behavior End.DT4 or End.DT6 for the N6DN in S2

S1 here adopts the local N6DN to prioritize closer segment for the same Direct Segment. Another PE may adopt D1 from S2, if the PE has no local N6DN for D1 and closer to S2 than S1.

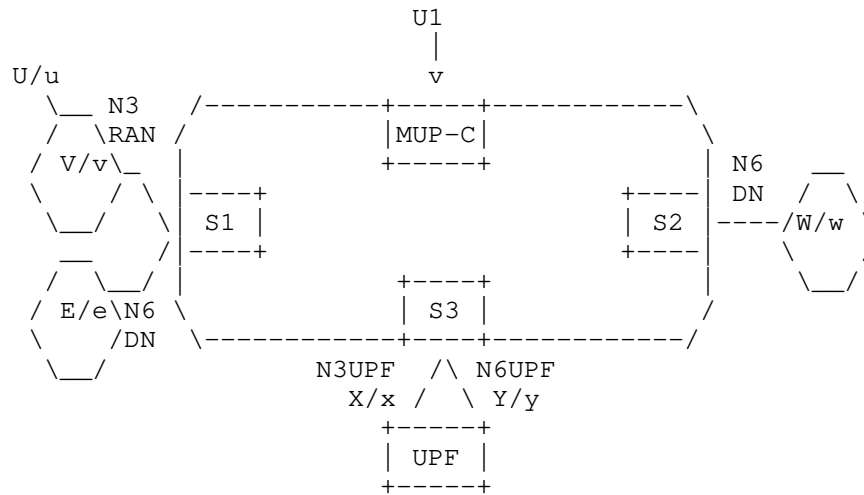


Figure 3

Now, session information U1 is put to a MUP Controller, MUP-C, and MUP-C is configured to transforms U1 to the routes as follows:

\* MUP-C

- attach the RT C3 to the DN in U1
- transforms UE's prefix U/u, the F-TEID on access side (gNB) and QFI in U1 to the Type 1 session transformed route for the prefix U/u with the F-TEID, the QFI, and RT C3
- transforms F-TEID on core side (UPF) X in U1 to the Type 2 session transformed route for X with MUP segment-ID D1 and RT C2

Then N3RAN and N6DN import route X and U/u respectively. S1 and S2 resolves U/u's remote endpoint with V/v and then install SID S1:: for U/u in FIB. S1:: will not be appeared in the packet from E/e to U/u over the wire.

As S1 adopts local N6DN for D1, N3RAN in S1 decapsulates GTP-U packets from V/v to X and then lookup the inner packets from U/u in N6DN after the decapsulation.

Note: When the above configurations have been done, SRv6 MUP is applied only to the packets from/to U/u. Each endpoint in U/u, W/w and E/e can communicate through S1 and S2. The rest of traffic from/to other UEs go through the usual 3GPP 5G user plane path using UPF via S3.

Another case shown in Figure 4 is that S4 joins the SR network and accommodates edge servers in the N6DN in S4.

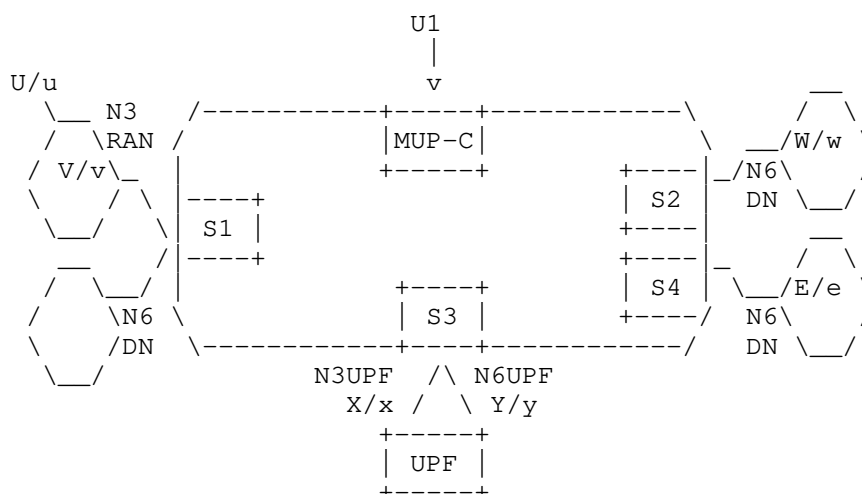


Figure 4

The following routing instances are configured:

- \* N3RAN in S1 (same with the previous case)
  - export route V/v with RT C1
  - import routes which have RT C1 and C2
- \* N6DN in S1
  - export no route
  - import routes which have RT C4
- \* N6DN in S2 (same with the previous case)

- export route W/w with RT C4
- import routes which have RT C3 and C4
- \* N3UPF in S3 (same with the previous case)
  - export route X/x with RT C2
  - import routes which have RT C1
- \* N6UPF in S3 (same with the previous case)
  - export route Y/y with RT C3
  - import routes which have RT C4
- \* N6DN in S4
  - export route E/e with RT C4
  - import routes which have RT C3 and C4

Here, the PEs are configured to enable SRv6 MUP as following:

- \* S1 (same with the previous case)
  - advertises Interwork type route: V/v with SID S1::
  - set S1:: behavior End.M.GTP4.E or End.M.GTP6.E
- \* S1
  - advertise Direct type route: MUP Direct Segment community D1 for the local N6DN
  - set S1:1:: behavior End.DT4 or End.DT6 for the N6DN in S1
- \* S2 (same with the previous case)
  - advertise Direct type route: MUP Direct Segment community D1 and SID S2::
  - set S2:: behavior End.DT4 or End.DT6 for the N6DN in S2
- \* S4
  - advertise Direct type route: MUP Direct Segment community D2 and SID S4::

- set S4:: behavior End.DT4 or End.DT6 for the N6DN in S4

As same as the previous case, S1 adopts the local N6DN for D1 as long as S1 prioritizes closer segment for the same MUP Direct Segment. The Direct type route from S4 for D2 with SID S4:: will be kept in S1.

\* MUP-C (same with the previous case)

- attach the RT C3 to the DN in U1
- transforms UE's prefix U/u, the F-TEID on access side (gNB) and QFI in U1 to the Type 1 session transformed route for the prefix U/u with the F-TEID, the QFI, and RT C3
- transforms F-TEID on core side (UPF) X in U1 to the Type 2 session transformed route for X with MUP Direct Segment community D1 and RT C2

Then N3RAN and N6DN import route X and U/u respectively. S2 and S4 resolve U/u's remote endpoint with V/v and then install SID S1:: for U/u in FIB.

As same as the previous case, S1 adopts local N6DN for D1, N3RAN in S1 decapsulates GTP-U packets from V/v to X and then lookup the inner packets from U/u in N6DN after the decapsulation.

For D2 on the other hand, no corresponding N6DN existed in S1. However E/e with RT C4 from S4 is imported into N6DN in S1 as a vpn route, E/e is reachable from U/u via N6DN for D1 in S1.

If a session U1' includes DN corresponding to D2, MUP-C advertises Type 2 session transformed route X' with MUP Direct Segment community D2, and then N3RAN in S1 instantiates H.M.GTP4.D or End.M.GTP6.D for X with S4:: as the last SID in the received Direct type route from S4.

Note: When the above configurations have been done, SRv6 MUP is applied only to the packets from/to U/u. Each endpoint in U/u, W/w and E/e can communicate through S1, S2 and S4. The rest of traffic from/to other UEs go through the usual 3GPP 5G user plane path using UPF via S3.

## 8. IANA Considerations

This memo includes no request to IANA.



## 9. Security Considerations

TBD.

## 10. References

### 10.1. Normative References

- [I-D.ietf-dmm-srv6-mobile-uplane]  
Matsushima, S., Filsfils, C., Kohno, M., Garvia, P. C., Voyer, D., and C. E. Perkins, "Segment Routing IPv6 for Mobile User Plane", Work in Progress, Internet-Draft, draft-ietf-dmm-srv6-mobile-uplane-18, 18 February 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-dmm-srv6-mobile-uplane-18>>.
- [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>>.
- [RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <<https://www.rfc-editor.org/info/rfc7333>>.
- [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>>.
- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <<https://www.rfc-editor.org/info/rfc8986>>.

### 10.2. Informative References

- [RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <<https://www.rfc-editor.org/info/rfc4360>>.

- [RFC4684] Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, DOI 10.17487/RFC4684, November 2006, <<https://www.rfc-editor.org/info/rfc4684>>.
- [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>>.
- [RFC8885] Bernardos, CJ., de la Oliva, A., Giust, F., Zúñiga, JC., and A. Mourad, "Proxy Mobile IPv6 Extensions for Distributed Mobility Management", RFC 8885, DOI 10.17487/RFC8885, October 2020, <<https://www.rfc-editor.org/info/rfc8885>>.
- [TS.23501] 3GPP, "System architecture for the 5G System (5GS)", 3GPP TS 23.501 17.2.0, 24 September 2021, <<http://www.3gpp.org/ftp/Specs/html-info/23501.htm>>.

## Authors' Addresses

Satoru Matsushima  
SoftBank  
Japan  
Email: [satoru.matsushima@g.softbank.co.jp](mailto:satoru.matsushima@g.softbank.co.jp)

Katsuhiro Horiba  
SoftBank  
Japan  
Email: [katsuhiro.horiba@g.softbank.co.jp](mailto:katsuhiro.horiba@g.softbank.co.jp)

Ashiq Khan  
SoftBank  
Japan  
Email: [ashiq.khan@g.softbank.co.jp](mailto:ashiq.khan@g.softbank.co.jp)

Yuya Kawakami  
SoftBank  
Japan  
Email: [yuya.kawakami01@g.softbank.co.jp](mailto:yuya.kawakami01@g.softbank.co.jp)

Tetsuya Murakami  
Arrcus, Inc.  
United States of America  
Email: tetsuya@arrcus.com

Keyur Patel  
Arrcus, Inc.  
United States of America  
Email: keyur@arrcus.com

Miya Kohno  
Cisco Systems, Inc.  
Japan  
Email: mkohno@cisco.com

Teppei Kamata  
Cisco Systems, Inc.  
Japan  
Email: tkamata@cisco.com

Pablo Camarillo Garvia  
Cisco Systems, Inc.  
Spain  
Email: pcamaril@cisco.com

Daniel Voyer  
Bell Canada  
Canada  
Email: daniel.voyer@bell.ca

Shay Zadok  
Broadcom  
Israel  
Email: shay.zadok@broadcom.com

Israel Meilik  
Broadcom  
Israel  
Email: israel.meilik@broadcom.com

Ashutosh Agrawal  
Intel  
United States of America  
Email: ashutosh.agrawal@intel.com

Kumaresh Perumal  
Intel  
United States of America  
Email: kumaresh.perumal@intel.com

Jakub Horn  
Cisco Systems, Inc.  
Czech Republic  
Email: jakuhorn@cisco.com