|  |  |
| --- | --- |
| 3GPP TR 29.892 V16.0.0 (2019-09) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  Study on User Plane Protocol in 5GC  (Release 16) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions, symbols and abbreviations 9

3.1 Definitions 9

3.2 Abbreviations 10

4 Introduction 10

5 User Plane Architecture in 5GC 10

5.1 Architectural Requirements for User Plane 10

5.1.1 General 10

5.1.2 User Plane Functionality 13

5.1.3 Support for Error Recovery and Restoration 13

5.2 Key Issues for User Plane Protocol 14

5.2.1 IP Connectivity for N9 and Network Slicing 14

5.2.1.1 Description of Key Issue 14

5.2.1.2 Considerations on Key Issue 14

5.2.2 <Key Issue 2> 15

5.2.x <Key Issue X> 15

5.2.y Summary of Key Issues 15

6 Candidate User Plane Protocols 15

6.1 GTP-U 15

6.1.1 Description 15

6.1.1.1 General 15

6.1.1.2 IP Transport for GTP-U 15

6.1.1.3 Path/Tunnel Management functions 15

6.1.1.4 Load Balancing 16

6.1.1.5 Multicast 16

6.1.2 Analysis of IETF RFC 8200 Impacts 16

6.1.3 Solutions for Impacts due to IETF RFC 8200 20

6.1.3.1 General 20

6.1.3.2 Addressing UDP Zero Checksum Issue 20

6.1.3.2.1 Solution Description 20

6.1.3.2.2 Identified Impacts 21

6.1.4 System Impacts 21

6.2 Segment Routing IPv6 (SRv6) 21

6.2.1 General SRv6 Description 21

6.2.1.1 General 21

6.2.1.2 Packet Processing 22

6.2.1.3 Network Programmability 23

6.2.2 Description of SRv6 solution in 5GC 23

6.2.2.1 General 23

6.2.2.2 Principles 23

6.2.2.3 SRv6 SID Encoding 24

6.2.2.3.1 General 24

6.2.2.3.2 Discussion 24

6.2.2.4 User Plane packet flow 25

6.2.2.4.1 SRv6 in Traditional Mode 25

6.2.2.4.2 SRv6 in Enhanced mode 26

6.2.2.4.2.1 Uplink 27

6.2.2.4.2.2 Downlink 28

6.2.2.4.3 Hand-over 28

6.2.2.5 Discovery of SRv6 supported UPF 29

6.2.2.5.1 General 29

6.2.2.5.2 Use PFCP protocol at N4 to pass SRv6 Capability 29

6.2.2.5.3 Use Local Configuration at SMF 30

6.2.2.5.4 Discovery of UPF using NRF 30

6.2.2.6 IPv4 Transport Support for SRv6 User Plane 30

6.2.2.6.1 General 30

6.2.2.6.2 IPv4 Encapsulation and Decapsulation for IPv6 packet 30

6.2.2.6.3 Routing IPv6 packet over IPv4 Transport Network 30

6.2.2.6.4 Mapping SRv6 User Plane IP Resource to IPv4 Transport 31

6.2.2.7 Security Considerations for SRv6 31

6.2.2.8 Using SRH for User Plane Messages 31

6.2.2.8.1 General 31

6.2.2.8.2 Tag Encoding 31

6.2.2.9 Packet forwarding between SMF and UPF 32

6.2.2.10 Roaming Support 32

6.2.2.11 Failure Detection and Recovery 32

6.2.2.11.1 General 32

6.2.2.11.2 Failure Detection 32

6.2.2.11.2.1 Loss of SRv6 SID contexts 32

6.2.2.11.2.2 User Plane Path Failure 32

6.2.2.11.3 Restoration Procedure 32

6.2.2.11.3.1 SRv6 Error Indication received by another UPF 32

6.2.2.11.3.2 Restoration Procedures upon User Plane Path Failure 33

6.2.2.11.4 Restoration Procedure for User Plane Related Entities 33

6.2.2.12 SRv6 Guaranteed Packet Delivery 33

6.2.2.12.1 General 33

6.2.2.12.2 Redundant packet transmission for downlink traffic 33

6.2.2.12.3 Removal of Redundant packet for uplink traffic 34

6.2.2.13 SRv6 extensibility using SRH TLVs 35

6.2.3 System Impacts 35

6.2.3.1 General 35

6.2.3.2 Common System Impacts of SRv6 35

6.2.3.2.1 System Impact on N4 interface 35

6.2.3.2.1.1 General 35

6.2.3.2.1.2 Impact on PFCP procedure 35

6.2.3.2.1.3 Impact on PFCP IEs 36

6.2.3.2.2 System Impact on N16/N16a/N38 interfaces 36

6.2.3.3 System Impacts of Traditional Mode 37

6.2.3.4 System Impacts of Enhanced Mode 37

7 Evaluations and Comparison 37

7.1 Evaluation 37

7.1.1 Evaluation Points 37

7.1.2 GTP-U 37

7.1.2.1 General 37

7.1.2.2 Architectural requirements for User Plane 37

7.1.2.3 Key issues 37

7.1.2.4 System impacts 38

7.1.3 SRv6 38

7.1.3.1 Traditional Mode 38

7.1.3.1.1 General 38

7.1.3.1.2 Architectural requirements for User Plane 38

7.1.3.1.3 Key issues 38

7.1.3.1.4 System impacts 38

7.1.3.2 Enhanced Mode 39

7.1.3.2.1 General 39

7.1.3.2.2 Architectural requirements for User Plane 40

7.1.3.2.3 Key issues 40

7.1.3.2.4 System impacts 40

7.2 Additional Considerations 40

7.2.1 Consideration Points 40

7.2.2 GTP-U 42

7.2.3 SRv6 44

7.3 Comparison 47

8 Conclusion 48

8.1 General 48

8.2 GTP-U over IP-based transport (including SRv6) 48

8.3 SRv6 user plane protocol (without GTP-U) 49

Annex A: Change history 50

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, certain modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

NOTE 1: The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

NOTE 2: The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

NOTE 3: The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

NOTE 4: The constructions "can" and "cannot" shall not to be used as substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

NOTE 5: The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document studies possible candidate protocols for the user plane in 5GC based on Rel-16 stage 2 requirements.

This technical report covers the following analysis:

- List architectural requirements and key issues;

- Identify the possible candidate protocols for user-plane including GTP-U as existing protocol, specified for Rel-15;

- Define a list of evaluation criteria based on Rel-16 stage 2 architecture and procedures to evaluate the candidate protocols;

- Evaluate the candidate solutions against the list of requirements and the potential benefits against the existing user plane solution in 5GS.

The N3 and N6 user plane interfaces are out of the scope of this study. N3 uses GTP-U (see clause 4.3.1 of 3GPP TS 38.300 [12]).

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[3] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[4] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[5] IETF RFC 8402: "Segment Routing Architecture".

[6] IETF draft-ietf-6man-segment-routing-header-18: "IPv6 Segment Routing Header (SRH)".

[7] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[8] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[9] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes; Stage 3".

[10] 3GPP TS 38.415: "NG-RAN; PDU Session User Plane Protocol".

[11] 3GPP TS 23.527: "5G System; Restoration Procedures".

[12] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[13] IETF RFC 6437: "IPv6 Flow Label Specification".

[14] IETF draft-ali-spring-srv6-oam-01: "Operations, Administration, and Maintenance (OAM) in SRv6".

[15] IETF RFC 1027: "Using ARP to Implement Transparent Subnet Gateways".

[16] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[17] 3GPP TS 29.060: "GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[18] IETF RFC 2401: "Security Architecture for the Internet Protocol".

[19] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[20] IETF RFC 6935: "IPv6 and UDP Checksums for Tunneled Packets".

[21] IETF RFC 6936: "Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums".

[22] 3GPP TR 23.725: "Study on enhancement of Ultra-Reliable Low-Latency Communication (URLLC) support in the 5G Core network (5GC)".

[23] 3GPP TR 23.726: " Study on Enhancing Topology of SMF and UPF in 5G Networks".

[24] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".

[25] 3GPP TS 29.510: "Network Function Repository Services, Stage 3".

[26] IETF RFC 4213: "Basic Transition Mechanisms for IPv6 Hosts and Routers".

[27] IETF RFC 5969: "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) Protocol Specification".

[28] IETF draft-geng-detnet-dp-sol-srv6-00: "DetNet SRv6 Data Plane Encapsulation".

[29] 3GPP TS 29.502: "Session Management Services, Stage 3".

[30] IETF draft-ietf-spring-segment-routing-policy-02: "Segment Routing Policy Architecture".

[31] IETF RFC 6438: "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Core network service slice:** network slice created within the 5GC as defined in TS 23.501 [7]. This does not refer to any slice in the transport network.

**Forwarding Entity:** Any entity that is explicitly encoded in the user plane packet header to process and forward the packet. Transport layer entities that are agnostic to the user plane protocol being used in a 3GPP network are not considered as forwarding entity within the scope of this TR.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

BP Branching Point

I-UPF Intermediate UPF

I-SMF Intermediate SMF

SR Segment Routing

SRv6 Segment Routing IPv6

SRH Segment Routing Header

SID Segment ID

DA Destination Address

NPU Network Processing Unit

PSA PDU Session Anchor

UL CL Uplink Classifier

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

VM Virtual Machine

# 4 Introduction

# 5 User Plane Architecture in 5GC

## 5.1 Architectural Requirements for User Plane

### 5.1.1 General

The system architecture requirements specified in TS 23.501 [7] and TS 23.502 [8] shall apply.

Editor's Note: the stage 2 work for Rel-16 is on-going in 3GPP SA2. The following requirements are derived from the Rel-15 stage 2 specifications and the Rel-16 stage 2 requirements that are currently available. More requirements may be captured in this clause based on the outcomes of the Rel-16 stage 2 work.

Figure 5.1.1-1 depicts the 5G System architecture, where N3, N6 and N9 are user plane interfaces, and N4 is the control plane interface to control the user plane functionalities in the UPF.



Figure 5.1.1-1: 5G System architecture

Figure 5.1.1-2 depicts the 5G System architecture (non-roaming architecture) with the insertion of an I-SMF and UL-CL/BP, for PDU sessions where the SMF cannot control the UPF terminating the N3 interface and communicate via the N16a interface with an I-SMF that is inserted to control the UPF(s) that the SMF cannot directly control.



Figure 5.1.1-2: 5G System architecture with I-SMF insertion and UL-CL/BP.

The following architectural requirements apply to the user plane:

1) IPv4, IPv6, IPv4v6, Ethernet and Unstructured PDU sessions shall be supported.

2) The User Plane protocol shall be able to run over IPv4 and IPv6.

3) 3GPP specifications support deployments with a single UPF or multiple UPFs for a given PDU session.

4) A UPF that terminates a N6 interface is said to support a PDU Session Anchor (PSA) functionality. A PDU session may support one or multiple PSAs.

5) A UPF may be inserted to support the UL Classifier (UL CL) functionality (see clause 5.6.4.2 of TS 23.501 [7]) or the Branching Point functionality (see clause 5.6.4.3 of TS 23.501 [7]) to forward the traffic of the PDU session to/from different PSAs. It is possible for a UPF to support both the UL CL or Branching Point functionalities and PSA functionalities.

6) The SMF shall control the user plane functionalities in the UPF using the N4 reference point. This includes controlling all the functionalities specified in clause 5.8 of TS 23.501 [7] and in TS 29.244 [9], e.g.

- Establishing and releasing user plane tunnels;

- Detecting, forwarding, buffering, duplicating (for Lawful Interception) or dropping user plane packets;

- Enforcing PCC and QoS policies (e.g. gating control, QoS control, packet marking, traffic steering);

- Detecting and reporting user plane events (e.g. receipt of DL packets for a PDU session without user plane connectivity in 5G-AN, application start/stop, user plane inactivity);

- Measuring and reporting traffic counts for PCC or charging;

- Other functionalities (e.g. tracing, framed routing).

7) End Marker user plane packets shall be supported to assist packets reordering in the target RAN during mobility scenarios (see Annex A of TS 29.281 [2]), e.g. handovers, QoS flows mobility with dual connectivity. End markers may be generated in the SMF or in the UPF. End Marker user plane packets origination from an Intermediate UPF (I-UPF) and from the PSA UPF shall be supported. Transfer of End Marker user plane packets by an I-UPF shall be supported.

8) The PDU Session User Plane Protocol (see TS 38.415 [10]) shall be supported to transfer 5GS information over N3 and N9 (e.g. QoS Flow Identifier, Reflective QoS Indicator, Paging Policy Indicator) together with user plane packets.

9) It shall be possible to detect and handle user plane path failures as specified in clause 5 of TS 23.527 [11].

10) The user plane protocol shall be applicable to home routed roaming scenarios as well.

11) It shall be possible to detect and handle the loss of a user plane context in a peer UPF as specified in clause 5 of TS 23.527 [11].

NOTE: Other user plane requirements need to be supported in the RAN, e.g. to transport PDCP PDU Number or RAN Containers, but this is out of scope of this study.

12) When multiple UPFs are chained, the change in RAN node shall only create N4 signaling towards its immediate next hop UPF (in scenarios where the I-UPF with the N9 interface with the PSA does not need to be changed). The anchor UPF shall not be aware of the change of RAN node.

13) In the case of home routed roaming, the PSA UPF in HPLMN shall not be aware of the topology of the VPLMN. In other words, the IP addresses of the RAN nodes in the VPLMN are not known to the HPLMN.

14) If the user plane protocol on N9 is different from the user plane protocol on N3, then interworking of user plane packets from one protocol to the other shall be well specified and have the least processing impacts.

15) Data forwarding shall be supported between the SMF and UPF, see clause 5.3 of TS 29.244 [9].

16) For non-roaming or LBO roaming cases, and PDU sessions not using SSC mode 2 or 3, an I-SMF may be inserted to control the UPF terminating the N3 interface. Based on PCC rules received from PCF and DNAI list reported by the I-SMF, the SMF provides the I-SMF with information that allows the I-SMF to make traffic routing related decisions and I-UPF selection decisions (among others), e.g. to add, replace or remove a UPF in the data path. See TR 23.726 [23].

17) Redundant transmission may be supported on N9 (and N3) via two independent tunnels associated with a single PDU session, for Ultra Reliable Low Latency Communications (URLLC). See TR 23.725 [22]. If the SMF decides to perform redundant transmission for one or more Qos flows of a PDU session, the SMF allocates two CN tunnels and indicates the UPF to perform redundant transmission of packets of the QoS flow(s) in the downlink direction, or to eliminate duplicate packets for the Qos flow(s) in the uplink direction, via the N4 interface.

Two Intermediate UPFs (I-UPFs) between the PSA UPF and the NG-RAN may be used to support the redundant transmission based on two N3 and N9 tunnels between a single NG-RAN mode and the UPF.



Figure 5.1.1-3: Two N3 and N9 tunnels between NG-RAN and UPF for redundant transmission

The PSA UPF duplicates the downlink packet of the QoS Flow from the DN and assigns the same GTP-U sequence number to them. These duplicated packets are transmitted to I-UPF1 and I-UPF2 via N9 Tunnel 1 and N9 Tunnel 2 separately. Each I-UPF forwards the packet with the same GTP-U sequence number as received from the UPF to NG-RAN via N3 Tunnel 1 and N3 Tunnel 2 respectively. The NG-RAN eliminates the duplicated packet based on the GTP-U sequence number. For uplink traffic, the NG-RAN duplicates the packet of the QoS Flow for the UE and the UPF eliminates the duplicated packet based on the GTP-U sequence number.

### 5.1.2 User Plane Functionality

This clause lists the main UP functionalities required to be supported by UPF as per stage 2 specified in clause 6.2.3 of TS 23.501 [7] as following:

- Anchor point for Intra-/Inter-RAT mobility (when applicable);

- External PDU Session point of interconnect to Data Network;

- Packet routing & forwarding (e.g. support of Uplink classifier to route traffic flows to an instance of a data network, support of Branching point to support multi-homed PDU Session);

- Packet inspection (e.g. Application detection based on service data flow template and the optional PFDs received from the SMF in addition);

- User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering);

- Lawful intercept (UP collection);

- Traffic usage reporting;

- QoS handling for user plane, e.g. UL/DL rate enforcement, Reflective QoS marking in DL;

- Uplink Traffic verification (SDF to QoS Flow mapping);

- Transport level packet marking in the uplink and downlink;

- Downlink packet buffering and downlink data notification triggering;

- Sending and forwarding of one or more "end marker" to the source NG-RAN node;

- ARP proxying as specified in IETF RFC 1027 [15] and / or IPv6 Neighbour Solicitation Proxying as specified in IETF RFC 4861 [16] functionality for the Ethernet PDUs. The UPF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request;

- Packet duplication in downlink direction and elimination in uplink direction by the UP protocol.

NOTE: Not all of the UPF functionalities are required to be supported in an instance of user plane function of a Network Slice.

### 5.1.3 Support for Error Recovery and Restoration

As per the 5GC architecture specified in TS 23.501 [7] and TS 23.502 [8], the packet detection and forwarding rules at the UPF are installed and controlled on a per PDU session basis over the N4 interface. This results in the creation of packet detection and forwarding state on a per PDU session basis at the UPF. 3GPP currently specifies the path failure detection, error detection and recovery mechanism when GTPU is used as the user plane protocol, in TS 23.527 [11].

Any user plane protocol to be used for 5GC shall then correspondingly have:

- Mechanisms for the detection of loss of "packet forwarding state" associated with a user plane packet at the receiving UPF;

- Mechanisms for detecting loss of connectivity towards a destination UPF;

- Mechanisms for detection of loss of connectivity towards transport layer forwarding entities, if the user plane protocol explicitly encodes the transport path;

- Mechanisms for the recovery of packet detection and forwarding state after the failure of a forwarding entity that is explicitly encoded in the user plane protocol to process the packet.

## 5.2 Key Issues for User Plane Protocol

This clause will identify key issues which the candidate protocols can solve, or could be improved.

### 5.2.1 IP Connectivity for N9 and Network Slicing

#### 5.2.1.1 Description of Key Issue

The N9 interface requires IP connectivity between UPFs. IP networking issues may affect the user plane of 3GPP system. The data path between UPFs may consist of various links and IP routing nodes so that multiple paths may be available for the N9 interface. The bandwidth, latency and reliability of those paths may differ.

The 5GC supports the concept of network slicing. The Network Instance ID supported over N4 enables to provide information to the UPF about the network slice of the PDU session (see clause 5.6.12 of 3GPP TS 23.501 [7], which indicates that the Network Instance ID can be selected based on the S-NSSAI of the PDU session). The UPFs need to have information on the transport network slice to allow the user plane packet of PDU sessions of 5GC network slices to be sent via appropriate transport networks. There is no one to one mapping between 5GC slices and transport network slices, i.e. several 5GC slices may use the same transport network slice.

NOTE: How network slicing is supported in transport networks is out of scope of 3GPP.

It is proposed to study the following aspects:

- whether there is a requirement to pass information about the network slice or the required QoS for the data path in the user plane packets.

#### 5.2.1.2 Considerations on Key Issue

This clause provides considerations for the Key Issue documented in clause 5.2.1.1 on whether there is a requirement to pass information about the network slice or the required QoS for the data path in user plane packets.

The following considerations apply:

1) 3GPP UP entities (UPFs for the N9 interface) get information about the core network service slice of the PDU session, via the Network Instance ID received from the SMF over N4 for UPFs, as specified in clause 5.2.1; there is thus no need to carry service slice information in UP packets, for 3GPP UP entities of the core network;

2) To support network slicing, 3GPP UP entities (UPFs for the N9 interface) are expected to be configured with local information to map core network service slices (Network Instance IDs) to transport links or VPNs (or "transport slices");

3) There is no one to one mapping between core network service slices and transport slices, i.e. several service slices may use the same transport slice.

4) How network slicing is supported in transport networks to support QoS and traffic segregation is out of scope of 3GPP. It is expected that transport slicing can be implemented with any existing technologies, e.g. using different types of L2 or L3 VPNs, MPLS-based services or segment routing, relying on service level agreement with the transport network operator.

NOTE: This is consistent with earlier conclusion at TSG SA#75 not to do any work on transport aspects, see TSG SA Reply LS ([SP-170276](ftp://ftp.3gpp.org/tsg_sa/TSG_SA/TSGS_75/Docs/SP-170276.zip)) to SA5 LS ([SP-170173](ftp://ftp.3gpp.org/tsg_sa/TSG_SA/TSGS_75/Docs/SP-170173.zip)) and RAN3 LS ([SP-170299](ftp://ftp.3gpp.org/tsg_sa/TSG_SA/TSGS_76/Docs/SP-170299.zip)).

5) Network slicing is already supported in 3GPP Rel-15, without any newly defined service slice or transport slice information in the user plane and relying on existing means to identify transport slices in the user plane such as VLAN tags or MPLS service labels and IP addresses.

There is no existing 3GPP requirement to:

- pass any new information about the service slice in UP packets;

- define and pass any new identifier in UP packets to identify transport slices or the required QoS for the data path.

### 5.2.2 <Key Issue 2>

### 5.2.x <Key Issue X>

### 5.2.y Summary of Key Issues

# 6 Candidate User Plane Protocols

This clause will describe each candidate protocol.

## 6.1 GTP-U

### 6.1.1 Description

#### 6.1.1.1 General

GTP-U is a tunneling protocol between given a pair of GTP-U tunnel endpoints. A Tunnel Endpoint ID (TEID) value allocated on each end point indicates which tunnel a particular T-PDU belongs to. That is described in clause 4.2.1 of TS 29.281 [2].

The receiving endpoint individually allocates the TEID and the sender tunnel endpoint encapsulates the packet from/to the UE with the TEID at the receiving endpoint in GTP-U header on top of UDP and IPv4 or IPv6.

#### 6.1.1.2 IP Transport for GTP-U

GTP-U supports both IPv4 and IPv6 as underlying transport layer protocol. As for IPv6, GTP-U specification refers to IETF RFC 2460 [3], which is described in clause 4.2.3 of TS 29.281 [2]. An analysis of the differences in the latest IETF RFC 8200 [4] for IPv6 and their impact on GTPU protocol is specified in clause 6.1.2.

UDP is utilized for GTP-U encapsulation and UDP destination port is 2152 which is assigned by IANA. Allocation of UDP source port depends on sender tunnel endpoint node.

GTP-U can be transported using transport technologies, such as L2 or L3 VPNs, MPLS-based services or segment routing (SR-MPLS or SRv6), as described in clause 5.2.1.2.

For some specific transport protocols of GTP-U (e.g. SR-MPLS or SRv6), the intended path in the transport networks is encoded in the transport protocol header corresponding to Network Instance.

UDP checksum can be used to detect packet corruptions, if required.

#### 6.1.1.3 Path/Tunnel Management functions

GTP-U supports in-band signaling for path and tunnel management. Currently GTP-U supports the following messages:

- Echo Request;

- Echo Response;

- Supported Extension Headers Notification;

- Error Indication;

- End Marker.

A GTP-U tunnel endpoint node sends an Echo Request message to another node for keep-alive and the receiving node sends an Echo Response message to sender node as acknowledgment. Echo Request message and Echo Response message are described in clause 7.2.1 and clause 7.2.2 of TS 29.281 [2] respectively.

The Supported Extension Headers Notification message indicates supported extension header by the tunnel endpoint node. This message is sent only in case a tunnel endpoint node receives GTP-U packet with unsupported extension header.

GTP-U has the Error Indication message to notify the sending endpoint that the receiving endpoint has discarded packets for which no session exists. The Error Indication message is described in clause 7.3.1 of TS 29.281 [2].

GTP-U has End Marker message to indicate the end of the payload stream that needs to be sent on a GTP-U tunnel. End Marker message is described in clause 7.3.2 of TS 29.281 [2].

#### 6.1.1.4 Load Balancing

A GTP-U tunnel endpoint node can utilize UDP source port for load balancing purpose. The specification of this dynamic allocation is described in clause 4.4.2.0 of TS 29.281 [2]. The logic of source port number calculation is not described in the document and it depends on the implementation of GTP-U tunnel endpoint node.

#### 6.1.1.5 Multicast

GTP-U allows one tunnel endpoint node to send out a G-PDU to be received at multiple tunnel endpoints by utilizing IP multicast capability of underlay IP networks. It is used for MBMS (Multimedia Broadcast Multicast Service) through GTP-U tunnel that is described in clause 4.2.6 of TS 29.281 [2]. It means that GTP-U has Point-to-Multipoint (P2MP) tunneling capability.

### 6.1.2 Analysis of IETF RFC 8200 Impacts

IETF RFC 8200 [4], Appendix B specifies the changes in IPv6 protocol since IETF RFC 2460 [3]. Table 6.1.2-1 provides an analysis of the impact of each of these specified changes on the GTPU protocol.

Table 6.1.2-1 Analysis of Impacts on GTPU due to IETF RFC 8200 [4]

|  |  |  |
| --- | --- | --- |
| Sl.No | Change in IETF RFC 8200 [4] from IETF RFC 2460 [3] | Impact on GTPU |
| 1 | Removed IP Next Generation from the Abstract. | Editorial correction. No impact on GTPU. |
| 2 | Added text in Clause 1 that the data transmission order is the same as IPv4 as defined in RFC 791 | This is just a clarification to resolve ambiguity. 3GPP TS 29.281 [2], clause 4.5 refers to 3GPP TS 29.060 [17], clause 5 which describes the transmission order as network byte order starting from octet 1. Hence GTPU specifications are already aligned with this clarification. |
| 3 | Clarified the text in Clause 3 about decrementing the Hop Limit. | In IETF RFC 2460 [3] clause 3, the text read as:  *"Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero."*  In IETF RFC 8200 [4] this was clarified as:  *"Decremented by 1 by each node that forwards the packet. When forwarding, the packet is discarded if Hop Limit was zero when received or is decremented to zero. A node that is the destination of a packet should not discard a packet with Hop Limit equal to zero; it should process the packet normally."*  Even if a legacy GTPU entity interpreted IETF RFC 2460 [3] verbatim and had dropped packets that had a hop limit of 0, upgrading that entity to support IETF RFC 8200 [4] could only make sure unnecessary packet drops are not done and would improve the overall KPI / performance of the system. Upgrading to IETF RFC 8200 [4] does not cause any specific interoperability issue with respect to this specific hop limit clarification.  Hence it is safe to update the behaviour of a GTPU entity to align with IETF RFC 8200 [4] with respect to hop limit interpretation. |
| 4 | Clarified that extension headers (except for the Hop-by-Hop Options header) are not processed, inserted, or deleted by any node along a packet's delivery path. | 3GPP TS 29.281 [2] does not specify insertion IPv6 extension headers by GTPU entities. Hence this does not impact GTPU. |
| 5 | Changed requirement for the Hop-by-Hop Options header to a "may", and added a note to indicate what is expected regarding the Hop-by-Hop Options header. | IETF RFC 2460 [3] required that all nodes must examine and process the Hop-by-Hop Options header. But IETF RFC 8200 [4] specifies that nodes along a packet's delivery path only examine and process the Hop-by-Hop Options header if explicitly configured to do so.  The hop-by-hop headers are a IPv6 level information. As mentioned above GTPU does not expect any hop by hop headers. So this change in the RFC does not impact the GTPU protocol specification. |
| 6 | Added a paragraph to Clause 4 to clarify how extension headers are numbered and which are upper-layer headers. | GTPU does not use any IPv6 extension header and this clarification has no impact to GTPU. |
| 7 | Added a reference to the end of Clause 4 to the "IPv6 Extension Header Types" IANA registry. | GTPU does not use any IPv6 extension header and this clarification has no impact to GTPU. |
| 8 | Incorporated the updates from RFCs 5095 and 5871 to remove the description of RH0, that the allocations guidelines for routing headers are specified in RFC 5871, and removed RH0 from the list of required extension headers. | GTPU does not use any IPv6 extension header and this clarification has no impact to GTPU. |
| 9 | Revised Clause 4.5 on IPv6 fragmentation based on updates from RFCs 5722, 6946, 7112, and 8021. See rows below for the specific changes made. | See below. |
| 10 | Revised the text to handle the case of fragments that are whole datagrams (i.e., both the Fragment Offset field and the M flag are zero). If received, they should be processed as a reassembled packet. Any other fragments that match should be processed independently. The revised Fragment creation process was modified to not create whole datagram fragments (Fragment Offset field and the M flag are zero). | This is a clarification to the IPv6 layer of the stack on how to do the fragmentation. This does not impact GTPU protocol. |
| 11 | Changed the text to require that IPv6 nodes must not create overlapping fragments. Also, when reassembling an IPv6 datagram, if one or more its constituent fragments is determined to be an overlapping fragment, the entire datagram (and any constituent fragments) must be silently discarded. Includes a clarification that no ICMP error message should be sent if overlapping fragments are received. | This is a clarification to the IPv6 layer of the stack on how to do the fragmentation. This does not impact GTPU protocol. |
| 12 | Revised the text to require that all headers through the first Upper-Layer header are in the first fragment. This changed the text describing how packets are fragmented and reassembled and added a new error case. | The new error case added is about the silent discarding of overlapping fragments during re-assembly. This is a clarification to the IPv6 layer of the stack on how to do the reassembly. This does not impact GTPU protocol. |
| 13 | Added text to the Fragment header process on handling exact duplicate fragments. | The clarification added is:  "It should be noted that fragments may be duplicated in the network. Instead of treating these exact duplicate fragments as overlapping fragments, an implementation may choose to detect this case and drop exact duplicate fragments while keeping the other fragments belonging to the same packet."  This is an IPv6 level clarification for implementation. This does not impact GTPU protocol. |
| 14 | Updated the Fragmentation header text to correct the inclusion of an Authentication Header (AH) and noted No Next Header case. | No impact to GTPU. |
| 15 | Changed terminology in the Fragment header clause from "Unfragmentable Headers" to "Per-Fragment headers". | No impact to GTPU. |
| 16 | Removed the paragraph in Clause 5 that required including a Fragment header to outgoing packets if an ICMP Packet Too Big message reports a Next-Hop MTU less than 1280. | No impact to GTPU. |
| 17 | Changed the text to clarify MTU restriction and 8-byte restrictions, and noted the restriction on headers in the first fragment. | No impact to GTPU. |
| 18 | In Clause 4.5, added clarification noting that some fields in the IPv6 header may also vary across the fragments being reassembled, and that other specifications may provide additional instructions for how they should be reassembled. See, for example, Clause 5.3 of [RFC3168]. | No impact to GTPU. |
| 19 | Incorporated the update from RFC 6564 to add a new Clause 4.8 that describes recommendations for defining new extension headers and options. | No impact to GTPU. |
| 20 | Added text to Clause 5 to define "IPv6 minimum link MTU". | This is just a clarification. No impact to GTPU. |
| 21 | Simplified the text in Clause 6 about Flow Labels and removed what was Appendix A ("Semantics and Usage of the Flow Label Field"); instead, pointed to the current specifications of the IPv6 Flow Label field in [RFC6437] and the Traffic Class field in [RFC2474] and [RFC3168]. | IETF RFC 2460 [3], Appendix A specified the semantics and usage of the flow label field. Current implementations of GTPU entities rely on this. This did not specify any behaviour for the IPv6 forwarding nodes on whether they are permitted to modify the flow label if it was set to zero by the source of the IPv6 packet.  However, IETF RFC 8200 [4] removed this Appendix and instead is referring to IETF RFC 6437 [13] which specifies in clause 3:  *A node that forwards a flow whose flow label value in arriving packets is zero MAY change the flow label value. In that case, it is RECOMMENDED that the forwarding node sets the flow label field for a flow to a uniformly distributed value as just described for source nodes.*  providing the flexibility for GTPU entities that forward user plane packets to set the flow label if the incoming packet has a zero value for the flow label.  If 3GPP TS 29.281 [2] is updated to refer to IETF RFC 8200 [4] then new implementations of GTPU entities may use this flexibility at the IPv6 level even though it does not impact GTPU protocol specification as such. |
| 22 | Incorporated the update made by IETF RFC 6935 [20] ("IPv6 and UDP Checksums for Tunneled Packets") in Clause 8. Added an exception to the default behavior for the handling of UDP packets with zero checksums for tunnels. | IETF RFC 2460 [3], clause 8.1 specifies  *Unlike IPv4, when UDP packets are originated by an IPv6 node, the UDP checksum is not optional. That is, whenever originating a UDP packet, an IPv6 node must compute a UDP checksum over the packet and the pseudo-header, and, if that computation yields a result of zero, it must be changed to hex FFFF for placement in the UDP header. IPv6 receivers must discard UDP packets containing a zero checksum, and should log the error.*  IETF RFC 8200 [4] refers to IETF RFC 6936 [21] which in turn refers to IETF RFC 6935 [20] and allows the following exceptions to the above rule:  - Allows tunneling protocol entities (e.g. GTPU entities) to use UDP zero checksum;  - Allows a receiving IPv6 tunneling protocol entity (e.g. GTPU entity) not to discard a packet with a zero UDP checksum.  Due to the addition of these exceptions, if 3GPP TS 29.281 [2] is updated to refer to IETF RFC 8200 [4] then it is possible that a IETF RFC 8200 [4] compliant GTPU entity includes UDP zero checksum while a receiving IETF RFC 8200 [4] non-compliant GTPU entity will keep rejecting the packets.  In order to avoid such inter-operability issues, a solution shall be identified to negotiate the GTPU entity's capabilities via the 3GPP control plane protocol.  Also the requirements on the usage of the zero UDP checksum specified in clause 5 of IETF RFC 6936 [21] needs to be taken into account. |
| 23 | Added instruction to Clause 9, "IANA Considerations", to change references to IETF RFC 2460 [3] to this document. | No impact to GTPU. |
| 24 | Revised and expanded Clause 10, "Security Considerations". | IETF RFC 2460 [3] referred to IETF RFC 2401 [18] whereas IETF RFC 8200 [4] refers to IETF RFC 4301 [19] which has updated a number of security considerations for IPSec use over IPv6. Hence if 3GPP TS 29.281 [2] is updated to refer to IETF RFC 8200 [4] then the requirements in IETF RFC 4301 [19] would apply. However this does not bring any change to the GTPU protocol specification as such. |
| 25 | Added a paragraph to the Acknowledgments clause acknowledging the authors of the updating documents. | Editorial. No impact to GTPU. |
| 26 | Updated references to current versions and assigned references to normative and informative. | Editorial. No impact to GTPU. |

### 6.1.3 Solutions for Impacts due to IETF RFC 8200

#### 6.1.3.1 General

This clause addresses solutions for the impacts to GTP-U identified in clause 6.1.2 due to IETF RFC 8200 [4].

#### 6.1.3.2 Addressing UDP Zero Checksum Issue

##### 6.1.3.2.1 Solution Description

When a GTP-U entity is upgraded to support IETF RFC 8200 [4], then in order to use the UDP Zero Checksum capability, it has to be ensured that the path from the GTP-U entity to its peer GTP-U entity supports this capability, i.e all the on path IPv6 middleboxes should also be supporting UDP zero checksum (see IETF RFC 6936 [21]). In order to ensure that the following building block information is needed

- When a GTP-U tunnel over IPv6 is setup between two GTP-U entities, via 3GPP control plane signaling, the 3GPP control plane entities shall signal each other that a UDP zero checksum handling capable path that ensures integrity of the packet, is available for the GTP-U tunnel over IPv6.

The following steps provide the mechanism for a GTP-U entity to know the support for UDP zero checksum capable path towards a peer GTP-U entity.

1. Before a GTP-U tunnel is established between two GTP-U entities, the control plane function will get to know the peer GTP-U endpoint FTEID as part of control plane signalling. It is proposed that as part of this FTEID exchange over control plane, the following information is also exchanged between the control plane entities:

- Based on operator policies, whether a UDP zero checksum over IPv6 capable path that ensures integrity of the packet exists between the peer GTP-U entities.

NOTE: Whether this requires signalling 2 information over N4 - the UDP zero checksum support capability by peer GTP-U entities and the allowance to use the same based on operator policies as separate IEs or whether they can be combined into a single IE / bit can be determined during the normative phase.

2. For example, during PDU session establishment scenario, when the SMF establishes the N4 session in step 10 of the call flow specified in clause 4.3.2.2.1 of TS 23.502 [8],

- Either the UPF shall signal to the SMF, the availability of a UDP zero checksum support capable path that ensures the integrity of the packet, from a particular outbound network interface, based on operator policies; or

- The UPF shall signal to the SMF its UDP zero checksum support capability during the PFCP Association Setup Request / Response, and the SMF, based on operator policies, determines if a UDP zero checksum over IPv6 capable path that ensures the integrity of the packet, exists between the UPF and the peer GTP-U entity.

Then when the SMF initiates the N2 PDU session request towards the 5G-AN via the AMF in step 11, it shall include the information about the availability of a UDP zero checksum over IPv6 capable path between the UPF and the 5G-AN. This enables the 5G-AN to decide whether to send GTP-U packets with UDP zero checksum or not towards the UPF in the uplink direction.

3. When the 5G-AN responds to the N2 request, it shall include the information about the availability of UDP zero checksum over IPv6 capable path that ensures the integrity of the packet, between the 5G-AN and the UPF, based on operator policies at the 5G-AN. The SMF will get to know of this in step 15 and will inform it to UPF in step 16. This enables the UPF to decide whether to send GTP-U packets with UDP zero checksum or not towards the 5G-AN in the downlink direction.

4. Similarly the UDP zero checksum support capability can be signalled between the NG-RAN nodes for the use of GTP-U on the Xn and F1-U interfaces as well.

5. Once a UP function entity is informed that UDP zero checksum can be used e.g. when it is allowed by operator policies and when the peer GTP-U entity supports UDP zero checksum, it should send an Echo Request to the GTP-U peer periodically in order to check the aliveness of the GTP-U path with UDP zero checksum, as specified in IETF RFC 6935 [20].

6. The support for IETF RFC 8200 [4] and consequently the support for UDP zero checksum may be restricted to 5G UP functions only in order to avoid signalling protocol changes to EUTRA and EPC entities.

The interfaces carrying GTP-U traffic may be protected by NDS / Physical security and hence any packet corruption can be detected. Also the use of UDP zero checksum for GTP-U is controlled by operator policy and the operators can enable it, e.g. if it is known that packet corruptions between the two GTP-U entities are not possible. Correspondingly it is not required to address the requirements specified in clause 5 of IETF RFC 6936 [21] natively in GTP-U when UDP zero checksum over IPv6 is used. If NDS / Physical security is not used for the interfaces carrying GTP-U traffic and packet corruptions may occur, then the use of UDP zero checksum over IPv6 should not be enabled in the operator policy.

##### 6.1.3.2.2 Identified Impacts

The following are the impacts identified due to the solution proposed in clause 6.1.3.2.1.

- Potential addition of a UDP Zero Checksum for IPv6 support bit in UP Function Features IE of TS 29.244 [9].

- Addition of a "UDP Zero Checksum for IPv6 IE" in PFCP Session Establishment Request and PFCP Session Modification Request messages of TS 29.244 [9].

- Addition of UDP Zero Checksum for IPv6 IE in N2 SM information exchanged between SMF and 5G-AN.

- Addition of UDP Zero Checksum for IPv6 IE in Nsmf\_PDUSession\_Create / Update request and response over N16 (between V-SMF and H-SMF) and over N16a (between I-SMF and SMF).

- Addition of UDP Zero Checksum for IPv6 IE in Xn, F1 and E1 signalling messages to indicate the support of the corresponding UP function in the NG-RAN for the UDP zero checksum capability and its use as per operator policies. This will require liaising with RAN3.

- Changes to TS 29.281 [2] to add reference to IETF RFC 8200 [4] and to specify that periodic echo request should be done to check the aliveness of the path when sending UDP zero checksum over IPv6.

### 6.1.4 System Impacts

GTP-U is already supported in the 5G System.

No impacts are identified, other than those listed in clause 6.1.3.2.2 for the optional support of UDP zero checksum for GTP-U over IPv6.

## 6.2 Segment Routing IPv6 (SRv6)

### 6.2.1 General SRv6 Description

#### 6.2.1.1 General

SRv6 is the IPv6 dataplane instantiation of Segment Routing, defined in IETF RFC 8402 [5]. Segment Routing is a network architecture based on source-routing. Thus confining flow states to the ingress nodes in the SR domain.

The SRv6 dataplane consists on leveraging the IPv6 extension headers, defined in IETF RFC 8200 [4], to include in the IPv6 header a new routing extension header called "Segment Routing Header" (SRH), defined in IETF draft-ietf-6man-segment-routing-header-15 [6].

SRv6 has support for IPv4, IPv6, IPv4v6, Ethernet and Unstructured PDUs.

#### 6.2.1.2 Packet Processing

SRv6 encodes segments (SIDs) as IPv6 addresses in the Segment List of SRH. Source SR node of the SR domain creates SRH in the outer encapsulating IPv6 packet. Figure 6.2.1.2-1 shows SRH format, defined in IETF draft-ietf-6man-segment-routing-header-15 [6]. The Segment Left in the SRH points an index number of the Segment List that specifies the active segment. The IPv6 Destination Address (DA) is updated with the IPv6 address of the active segment so that the packet is routed to the node which has the active segment along the shortest path in the network.

Once the packet has reached the node, called SR Segment Endpoint Node decrements Segment Left and updates IPv6 DA with the active segment indicated by the updated Segment Left. Then the node forwards the packet along the updated DA. When the packet reaches the last segment of the Segment List, which means Segment Left becomes zero, the node pops out the SRH and forward the packet along the last segment.

The nodes between Source SR node and SR Endpoint Nodes, called Transit Nodes, neither inspect the SRH nor process it. Thus Transit Nodes only need to be IPv6 routing and forwarding capable.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octets |  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 |  | Next Header | | | | | | | |
| 2 |  | Header Extension Length = n | | | | | | | |
| 3 |  | Routing Type = 0x04 | | | | | | | |
| 4 |  | Segment Left | | | | | | | |
| 5 |  | Last Entry = m | | | | | | | |
| 6 |  | Flags | | | | | | | |
| 7 |  | Tag (1st Octet) | | | | | | | |
| 8 |  | Tag (2nd Octet) | | | | | | | |
| p to (p+15) |  | Segment List [0] (128 bits IPv6 Address) | | | | | | | |
| ... |  | ... | | | | | | | |
| q to (q+15) |  | Segment List [m] (128 bits IPv6 Address) | | | | | | | |
| (q+16) to (8n+8) |  | Optional Type Length Value objects (variable) | | | | | | | |

Figure 6.2.1.2-1: IPv6 Segment Routing Extension Header Format

where:

- Next Header: 8-bit selector. Identifies the type of header immediately following the Routing header, defined in IETF RFC 8200 [4];

- Header Extension Length: 8-bit unsigned integer. Length of the Routing header in 8-octet units, not including the first 8 octets, defined in IETF RFC 8200 [4];

- Routing Type: 8-bit identifier of a particular Routing header variant. 0x04 is suggested value for Segment Routing Header;

- Segments Left: 8-bit unsigned integer. Number of route segments remaining, i.e., number of explicitly listed intermediate nodes still to be visited before reaching the final destination, defined in IETF RFC 8200 [4];

- Last Entry: contains the index (zero based), in the Segment List, of the last element of the Segment List;

- Flags: 8 bits of flags. Currently no flags are defined;

- Tag: tag a packet as part of a class or group of packets, e.g., packets sharing the same set of properties. When tag is not used at source it MUST be set to zero on transmission. When tag is not used during SRH Processing it SHOULD be ignored. Tag is not used when processing the SID as defined in Clause 4.3.1 of IETF draft-ietf-6man-segment-routing-header-18 [6], which means the Tag value will not be touched by intermediate routers in SRv6 Enhanced mode solution;

- Segment List[n]: 128 bit IPv6 addresses representing the nth segment in the Segment List. The Segment List is encoded starting from the last segment of the SR Policy. i.e., the first element of the segment list (Segment List [0]) contains the last segment of the SR Policy, the second element contains the penultimate segment of the SR Policy and so on;

- Type Length Value (TLV) objects are optional and are described in IETF draft-ietf-6man-segment-routing-header-15 [6].

#### 6.2.1.3 Network Programmability

SRv6 introduces the concept of Network Programming. This implies that an SRv6 segment can be bound to any function/service in a router or compute instance.

An SRv6 segment is an IPv6 address, which is divided into Locator:Function:Arguments.  
The Locator routes the packet up to a given node in the network. Once the packet has arrived to this node, the Function is executed. The function might or might not take additional arguments specific to that function.

The 128 bit SRv6 SID consist of following components:

- Locator: routed to the node performing the function;

- Function: any possible function, either local to Network Processing Unit (NPU) or applications in Virtual Machine (VM)/Container;

- Arguments: optional argument bits to be used only by that SID.



Figure 6.2.1.3-1: SRv6 SID Structure

Editor's Note: How Network Programmability applies for 5GS is FFS.

### 6.2.2 Description of SRv6 solution in 5GC

#### 6.2.2.1 General

This clause studies SRv6 for User Plane in 3GPP 5GC.

It requires UPFs in 5GC to support SRv6.

#### 6.2.2.2 Principles

To derive the principle for SRv6 User Plane in 5GC, the following considerations apply:

- As 128-bits IPv6 address and the capability to accumulate it in SRH, all information user plane needs could only use IPv6 header, or IPv6 with SRH. It enables IP layer only user plane (i.e, w/o UDP/GTP-U);

- The UP function follows the forwarding model defined in TS 23.214 [24];

- The SMF controls each UPF for the user plane path per PDU Session.

The following principles are proposed:

1) No additional header other than IPv6 (Traditional mode), or IPv6 with SRH (Enhanced mode) to encapsulate all type of PDU session packet and user plane messages required to N9 interface (Traditional and Enhanced modes).

2) A SID of Locator:Function (see clause 6.2.1.3) shall consist of a IPv6 prefix assigned to user plane IP resource of UPF, and the Argument shall encode the identifiers of tunnel and QoS. (e.g; TEID, QFI and RQI)

In 5GC, there is only one function defined as the UP function which all instructions shall be configured through N4.

3) UPF shall lookup N4 session based on active SID as the destination address in the IPv6 header of receiving user plane packet.

4) SMF or UPF shall allocate a SID which enables UPF to be able to lookup the corresponding N4 session for each uplink and/or downlink.

5) N4 interface shall enable SMF to configure incoming and outgoing SID for a N4 session in each N9 UPF.

6) N4 interface shall enable UPF to notify SRv6 User Plane capability to SMF.

7) UPF shall be allowed to encapsulate T-PDU without SRH (i.e; Traditional mode).

8) UPF shall be allowed to add SIDs mapping to corresponding Network Instance into a SRH to encapsulate T-PDU (i.e; Enhanced mode).

9) N16/N16a/N38 interfaces shall enable V-SMF, H-SMF, I-SMF and SMF to negotiate the use of SRv6 and notify the capability of SRv6 in N9 with a SID for each corresponding PDU session.

#### 6.2.2.3 SRv6 SID Encoding

##### 6.2.2.3.1 General

In 5GC, SRv6 128-bits SID encoding shall follow the principle 2. This clause discusses what SID encoding looks like for user plane in 3GPP 5G System.

##### 6.2.2.3.2 Discussion

SRv6 takes SID in the format of "Locator:Funcition:Argument" in IPv6 address as described in clause 6.2.1.3. In 5GC architecture, one UP Function has been defined while multiple user plane IP resources will be available on a UPF. To follow the 5GC architecture, the Locator:Function part can turn out to be IPv6 prefix assigned to user plane IP resource of UPF.

The Argument bits consist of TEID, QFI and RQI bits. These bits help UPF to lookup N4 session by the active SID as the destination IP address in the IPv6 header of the receiving user plane packet.

The argument of which those bits embedded (TEID/QFI/RQI) requires at least 39-bits in total.

Figure 6.2.2.3.2-1 illustrates an example of SRv6 SID encoding. An IPv6 Prefix of the user plane IP resource consists of the IPv6 Prefix allocated to the UPF and some bits allocated to the IP resource. For example, an UPF allocated a prefix of 2001:db8::/32 assigns 0x39bb from 16-bits space from the user plane IP resources, 2001:db8:39:bb::/48 shall be the prefix for the IP resource.

The length of the IPv6 Prefix for the user plane IP resource shall be shorter than (128-39) bits. And the argument may be required that would be placed right after the IP resource prefix. In case that the total length of the all IPv6 Prefix and the argument shorter than 128 bits, the SID shall be right padded.

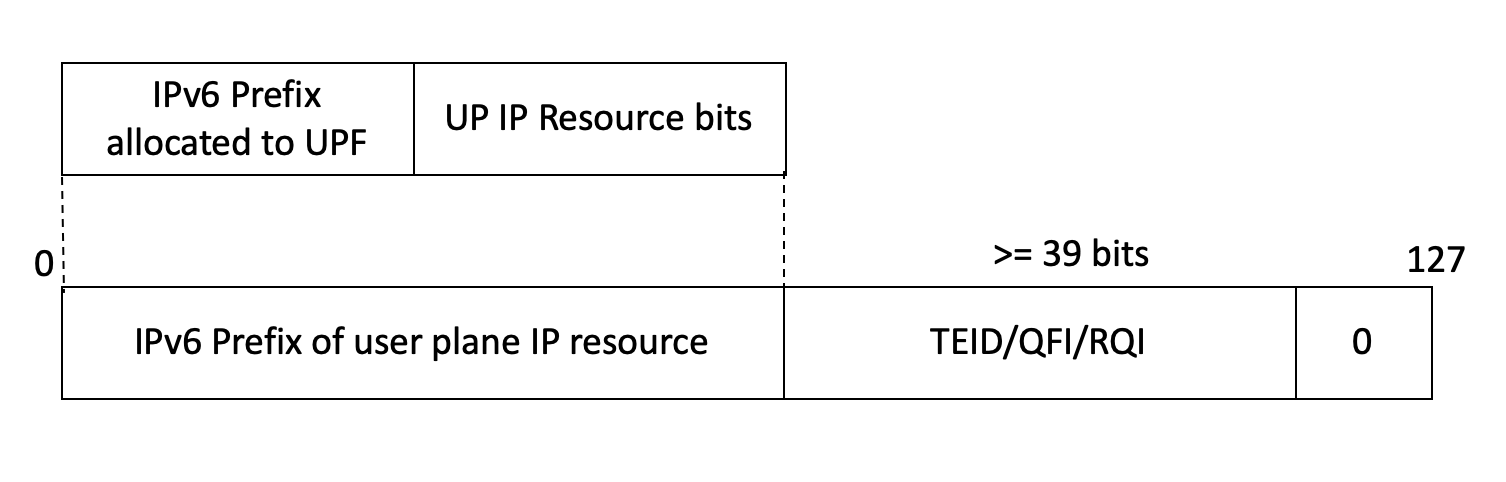


Figure 6.2.2.3.2-1: An example of SRv6 SID Encoding for 5GC

Editor's Note: More detail SID encoding for 5GC is FFS.

Editor's Note: The argument is encoded in a limited number of bits. Future extensibility to support more UP features in future release is FFS.

#### 6.2.2.4 User Plane packet flow

##### 6.2.2.4.1 SRv6 in Traditional Mode

SRv6 in traditional mode for 3GPP System works with a hop by hop model over N9 as follows:

- UPFs over N9 are SRv6 capable;

- when sending a packet on one N9 hop, the UPF creates one single SID in the destination address of the outer IPv6 header, that is set to the IP address of the next UPF and the SID identifying the PDU N4 session at the next UPF, and forwards the packet. No SRH header is included to encapsulate T-PDU;

- the UPF receiving the packet on the N9 hop identifies the PDU N4 session using the SID received in the Destination Address;

- packet processing functions in each UPF are controlled by the SMF provisioning packet processing rules (PDR/FAR/QER/URR) to the UPF over N4, using existing PFCP protocol;

- for End Marker and Error Indications the SRH header will contain a single segment that is the DA.

The Figure 6.2.2.4.1-1 shows how SRv6 in traditional mode could be used as user plane protocol over N9 with the current 5G System Architecture.

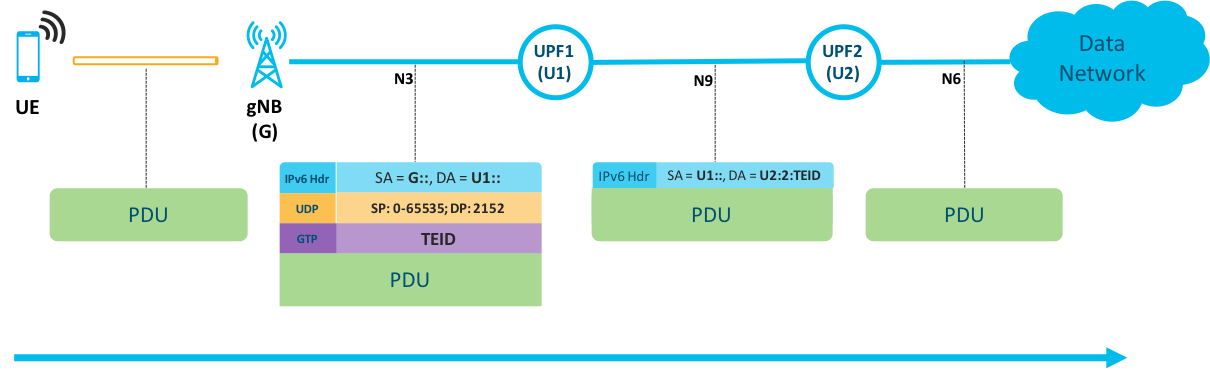


Figure 6.2.2.4.1-1: Uplink packet flow in SRv6 Traditional Mode

NOTE 1: UPF2 in the figure is PSA and UPF1 is I-UPF.

The PDU arrives from the gNB in GTP-U encapsulation at UPF1. The UPF1 removes the GTP-U header and encapsulates the PDU with an outer IPv6 header and then send out the packet to UPF2, based on the rules (PDR/FAR) associated to the corresponding N4 session provisioned by the SMF in UPF1 over N4. The IPv6 Source address will be set to the U1 of UPF1 address and the IPv6 Destination Address will be set to the U2 of UPF2.

The IPv6 Flow Label is computed as per IETF RFC 6437 [13].

All the PDU session types defined by TS 23.501 [7] are supported, since the original packet is encapsulated with a new IPv6 header.

Once the packet arrives at U2, the UP functions (e.g. packet forwarding) are executed by UPF2, based on the rules (PDR/FAR/QER/URR) associated to the corresponding N4 session provisioned by the SMF in UPF2 over N4. As UPF2 behaves as PSA, the PDU is decapsulated and forwarded over the N6 interface.

Note that the downlink packet flow is the similar, except for a simple reversal of the source for the destination IP addresses. This is shown in the Figure 6.2.2.4.1-2.

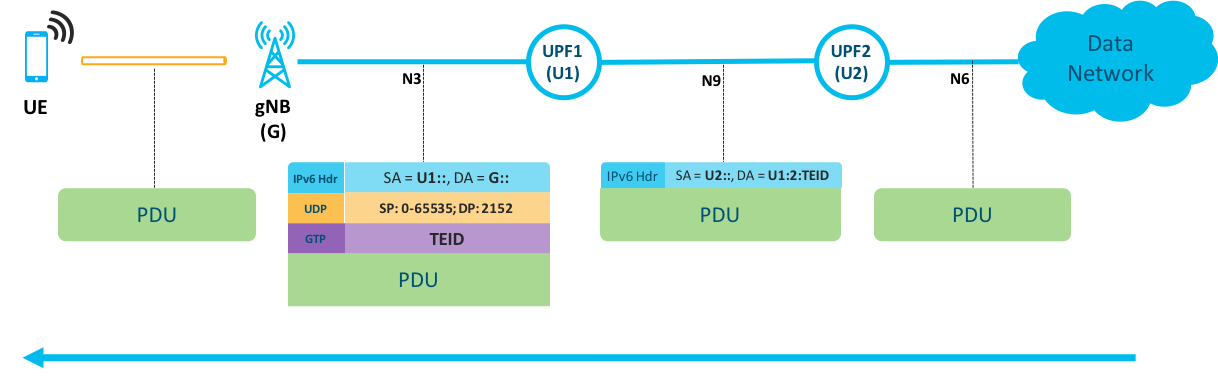


Figure 6.2.2.4.1-2: Downlink Packet Flow in the SRv6 Traditional Mode

NOTE 2: UPF2 in the figure is PSA and UPF1 is I-UPF.

##### 6.2.2.4.2 SRv6 in Enhanced mode

SRv6 in enhanced mode works over N9 as follows:

- UPFs over N9 are SRv6 capable;

- the N9 path may integrate transport slice of underlay network mapping to Network Instance based on local information;

- when sending a packet on N9, the UPF processes Network Instance that the packet created after FAR processing to insert one or multiple SIDs in a SRH between IPv6 header and to encapsulate T-PDU. Both packet processing are as following:

a. During FAR processing, the IPv6 Destination Address is set as the next hop UPF address with the arguments part carrying the TEID.

b. During Network Instance processing, the IPv6 Destination Address set by FAR is moved as the last SID in the SID list and the topmost SID in the list configured for the Network Instance is copied to the IPv6 Destination Address.  
  
What those SIDs represent is out of scope of 3GPP. The last SID contains the IPv6 address of the next UPF and the TEID encoded as argument identifying the PDU N4 session at the next UPF;

- the UPF receiving the packet on the N9 hop identifies the PDU N4 session using the IPv6 address received in the Destination Address.

- as same as Traditional mode, packet processing functions in each UPF are controlled by the SMF provisioning packet processing rules (PDR/FAR/QER/URR) to the UPF over N4, using existing PFCP protocol.

- For End Marker and Error Indications an additional outer SRH header with the SIDs will be added by UPF after the processing by network instance.

###### 6.2.2.4.2.1 Uplink

The Figure 6.2.2.4.2.1-1 shows how SRv6 in Enhanced mode can be used as a user plane protocol over N9 uplink in the current 5G System Architecture with an end-to-end transport network slice (and an associated ultra-low-latency SLA).

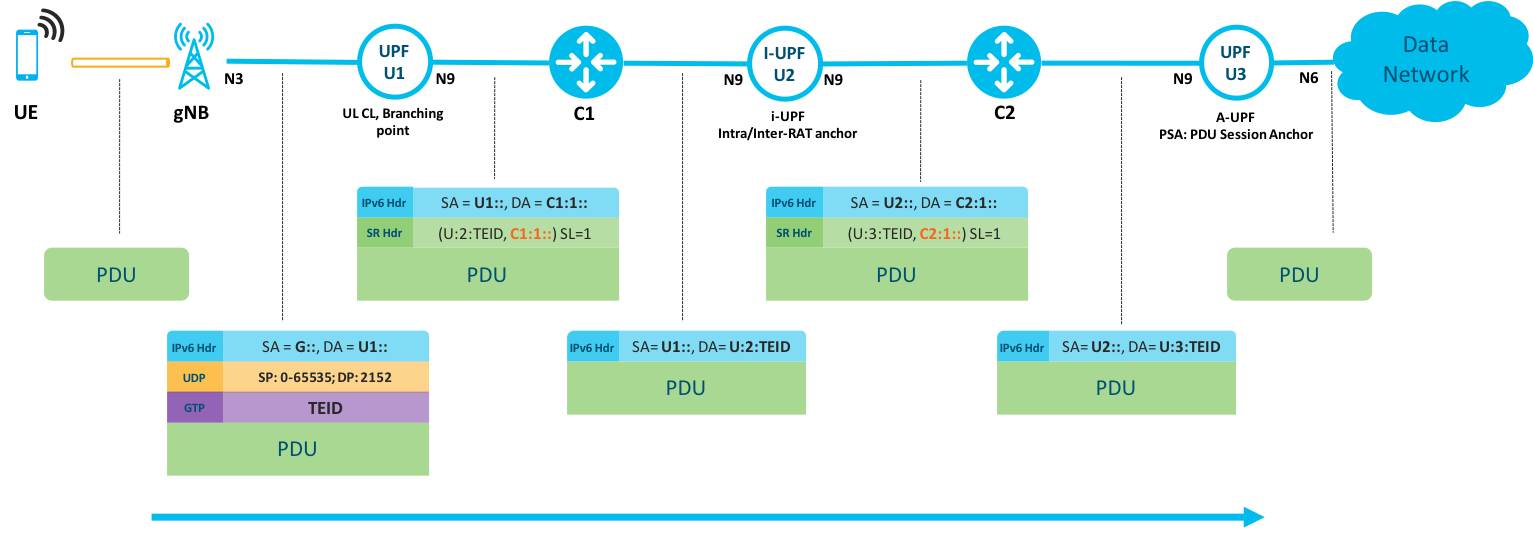


Figure 6.2.2.4.2.1-1: Uplink Packet flow using SRv6 Enhanced Mode

Note: C1 and C2 in the diagram are non-3GPP functions/entities.

The PDU arrives from the UE. The gNB encapsulates the PDU, adding an IPv6, UDP and GTP-U headers. The packet is destined towards the UPF U1.

Upon packet arrival, the UPF U1 processes the packet, removing the IPv6, UDP and GTP headers and it will then re-encapsulate it with an outer IPv6 header based on the rules (PDR/FAR) with an SRH mapping to the Network Instance in the rules associated to the corresponding N4 session provisioned by the SMF in UPF1 over N4.

The SRH contains the set of SIDs mapping to the provisioned Network Instance in the FAR based on local information. The last SID in the SRH shall be the SID identifying the N4 session at the next UPF, I-UPF U2.

The IPv6 Source address will be set to the UPF U1 IP address. The IPv6 Destination Address will be set to the first SRv6 segment. The IPv6 Flow Label is computed as per IETF RFC 6437 [13].

One simple transport slice example here is used as an example to explain the packet flow. The packet leaves the UPF1 and is forwarded on the N9 interface up to the node C1. Once the packet arrives to C1, the function 1 is going to be executed, which is fundamental SRv6 endpoint function described in clause 6.2.1.2. The IPv6 Destination Address is updated to the next segment, U:2:TEID, the last SID in the SRH. The SRH Segment Left value is decremented, and since now the value is at zero the router pops the SRH.

The packet is forwarded through the intended path up to the next segment U:2:TEID, which identifies the N4 session on the I-UPF U2. Once the packet arrives at U2, the UP functions are executed by U2, based on the rules (PDR/FAR/QER/URR) associated to the corresponding N4 session provisioned by the SMF in U2 over N4. Note that the I-UPF behaves as an *Intra/Inter-RAT anchor point.*

The I-UPF U2, after packet processing based on the provisioned rules, will insert again an SRH that will contain the set of SIDs mapping to the provisioned Network Instance in the FAR based on local information. The last SID in the SRH shall be the SID identifying the N4 session at the next UPF, A-UPF U3.

The IPv6 Source address will be set to the UPF U2 IP address. The IPv6 Destination Address will be set to the first SRv6 segment, C2 in this example. The IPv6 Flow Label is computed as per IETF RFC 6437 [13].

Packet is forwarded up to the node C2. Again, this node executes the function 1 which belongs to the endpoint function. The IPv6 Destination Address is updated with the next segment (U:3:TEID) , the last SID in the SRH. The node pops the SRH out since the decremented Segment Left in the SRH becomes zero.

Packet is forwarded through the intended path up to the next segment U:3:TEID, which identifies the N4 session on the UPF U3 (PSA). Once the packet arrives at U3, the UP functions are executed by U3, based on the rules (PDR/FAR/QER/URR) associated to the corresponding N4 provisioned by the SMF in U3 over N4. As the UPF U3 behaves as a PSA, the PDU is decapsulated and forwarded over the N6 interface.

The Network Instance process of UPF will validate the intended path encoded in the SRH. IETF draft-ietf-spring-segment-routing-policy-02 [30] specifies the validation for segment routing policy of the intended path and packet steering to the path. By that, the Network Instance process of UPF should declare the intended path when the reachability for all SIDs in the path can't be resolved with the means of routing mechanisms in the SRv6 transport.

###### 6.2.2.4.2.2 Downlink

The downlink packet flow is depicted in the Figure 6.2.2.4.2.2-1.

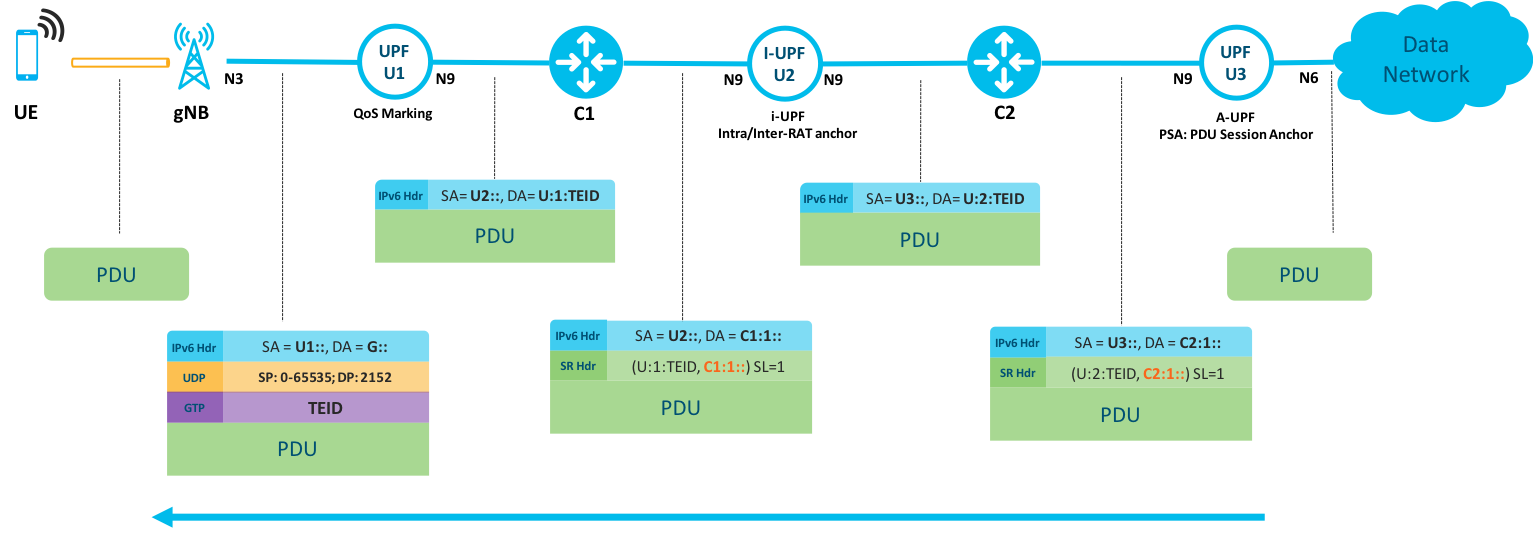


Figure 6.2.2.4.2.2-1: Downlink Packet Flow in SRv6 Enhanced Mode

NOTE: C1 and C2 in the diagram are non-3GPP functions/entities.

In this case the UPF U3 (PSA), upon packet reception, classifies and encapsulates the incoming packets with an outer IPv6 header based on the rule (PDR/FAR) with a SRH mapping to the Network Instance in the rules associated to the corresponding N4 session provisioned by the SMF. The SRH contains the set of SIDs mapping to the provisioned Network Instance in the FAR based on local information. This last SID identifies the N4 session on the I-UPF.

Nodes C1 and C2 process the packet based on the SRH as same as the uplink case.

Upon packet reception, the I-UPF imposes a new SRH containing the SIDs up to the next UPF, U1. Upon packet reception, U1 processes the packet and forwards it over the N3 interface.

As the N3 interface is unmodified (IPv6/GTP), the packet is IPv6, UDP, GTP.

##### 6.2.2.4.3 Hand-over

In mobility scenarios with a change of I-UPF, the PSA shall send one or more End-Marker packet towards the old I-UPF upon switching the user plane path. This End-Marker is configured through the Tag field in SRH (as explained in clause 6.2.1.2). The Figure 6.2.2.4.3-1 shows the hand-over packet flow.

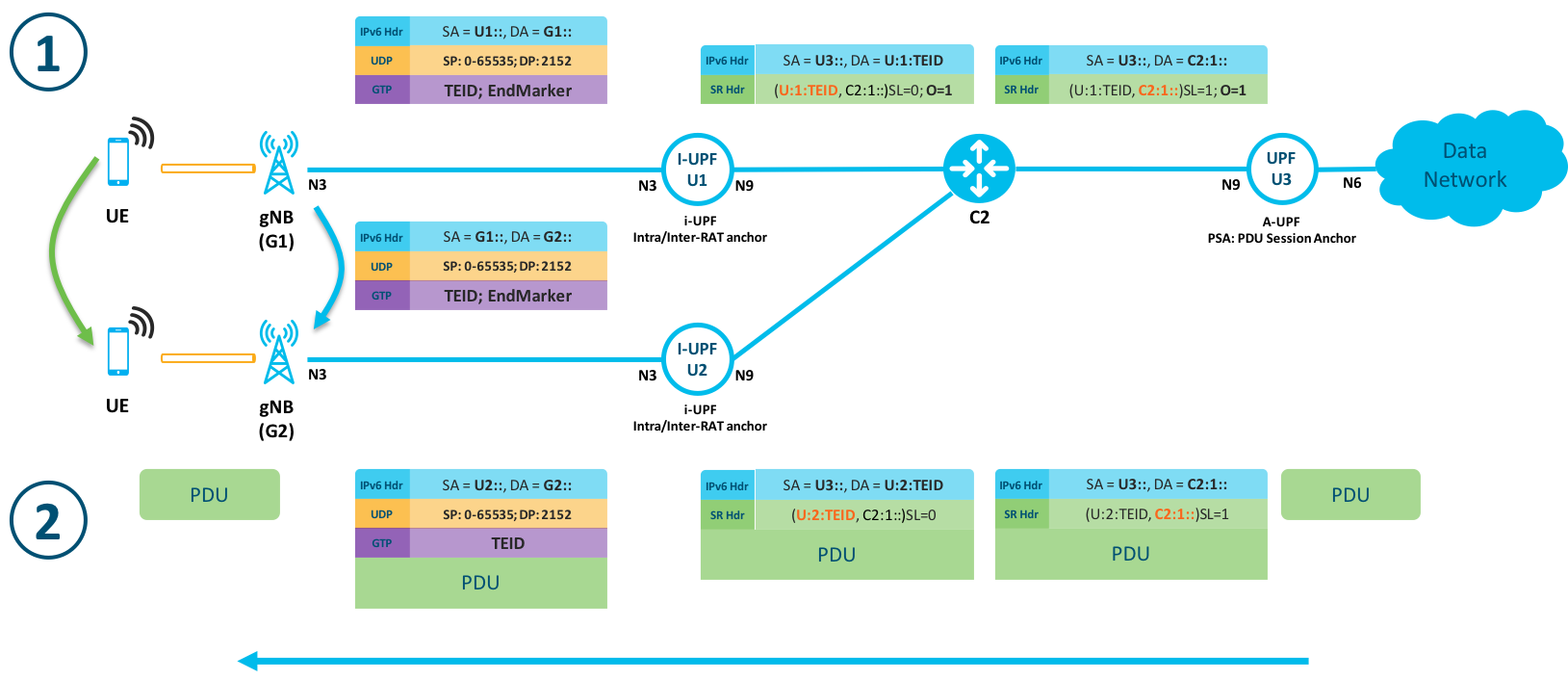


Figure 6.2.2.4.3-1: HO illustration using SRv6

Subsequent traffic is sent to the new I-UPF. This is done by simply updating the SR segment list on the PSA to match the new I-UPF location. This traffic does not have the End Marker bit set in the Segment Routing Header.

The End-Marker based mobility procedure is unmodified.

#### 6.2.2.5 Discovery of SRv6 supported UPF

##### 6.2.2.5.1 General

The SMF needs to discover the UPF which supports SRv6 before selecting the right UPF for handling SRv6 based user plane traffic. SMF can use following methods to discover the SRv6 supported UPF.

##### 6.2.2.5.2 Use PFCP protocol at N4 to pass SRv6 Capability

The PFCP protocol used at N4 interface can be extended to allow SMF to learn the UPF capability. Adding the SRv6 capability information in "UP function feature", clause 8.2.25 of 3GPP 29.244 [9], to indicate node level SRv6 capability and "User Plane IP Resource Information" IE, clause 8.8.82 of 3GPP 29.244 [9], to indicate interface level capability, can be used to allow SMF to learn SRv6 capability during PFCP Association Request procedure. The diagram below shows the details.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 2 | Type = 43 (decimal) | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | |  |
|  | 5 to 6 | Supported-Features | | | | | | | |  |
|  | 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |  |

Figure 6.2.2.5.2-1: UP Function Feature

The spare bits of Supported features (Octet 5 to 6) can be used to indicate SRv6.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 1 to 2 | Type = 116 (decimal) | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | |  |
|  | 5 | Spare | ASSOSI | ASSONI | TEIDRI | | | V6 | V4 |  |
|  | 6 | TEID Range | | | | | | | |  |
|  | m to (m+3) | IPv4 address | | | | | | | |  |
|  | p to (p+15) | IPv6 address | | | | | | | |  |
|  | k to l | Network Instance | | | | | | | |  |
|  | r | Spare | | | | Source Interface | | | |  |
|  | s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |  |

Figure 6.2.2.5.2-2: User plane IP Resource Information

The spare bit of octet 5 can be used to indicate if UPF supports SRv6 or not. The default value 0 indicates UPF does not support SRv6 and value 1 indicates that UPF does support SRv6.

##### 6.2.2.5.3 Use Local Configuration at SMF

SMF may be locally configured with the information about UPF, e.g by OAM system, when a new UPF instantiated or removed. Clause 6.3.3.2 of TS 23.501 [7] mentions about UPF provisioning in SMF.

##### 6.2.2.5.4 Discovery of UPF using NRF

In the 5GC SBA architecture, the NRF acts as NF repository where every NF register or deregister itself. A consumer NF uses NRF Discovery Service before selecting a producer NF as mentioned in clause 5.2.7 of TS 23.502 [8]. The UPF function may indicate SRv6 capability in the NF Profile while registering with NRF. The attribute UpfInfo, clause 6.1.6.2.13 of TS 29.510 [25] can be extended to indicate SRv6 capability of UPF. SMF can then use the NRF Discovery service to know if the UPF supports SRv6 or not. This method can be used by SMF to choose UPF during PDU session creation.

#### 6.2.2.6 IPv4 Transport Support for SRv6 User Plane

##### 6.2.2.6.1 General

As the architectural requirements states that the User Plane protocol shall be able to run over IPv4 and IPv6, described in clause 5.1.1. Since a SRv6 User Plane packet is an IPv6 packet with a SRH, this clause studies whether it is possible or not that SRv6 User Plane is able to run over IPv4 transport networks.

##### 6.2.2.6.2 IPv4 Encapsulation and Decapsulation for IPv6 packet

IPv6 in IPv4 encapsulation and forwarding manipulations (e.g., handling packet markings, checksum verification, etc.) is performed as specified in Clause 3.5 of "Basic Transition Mechanisms for IPv6 Hosts and Routers" in IETF RFC 4213 [26]. ICMPv4 errors are handled as specified in Clause 3.4 of IETF RFC 4213 [26]. By default, the IPv6 Traffic Class field MUST be copied to the IPv4 ToS (Type of Service) field. This default behavior may be overridden by configuration. Since IPv4 node shall not be expected as SRv6 node, there is no impact of SRH to that specified IPv6 over IPv4 encapsulation.

##### 6.2.2.6.3 Routing IPv6 packet over IPv4 Transport Network

An efficient solution for IPv6 encapsulated packets is to be routed based on the destination IPv6 address as standardized in IETF  RFC 5969 [27].

##### 6.2.2.6.4 Mapping SRv6 User Plane IP Resource to IPv4 Transport

As the study result in this clause, SRv6 is able to run over IPv4 transport networks. It is expected that Network Instance can be used to mapping to IPv4 Transport based on local information. How that mapping depends on local information is out of scope of 3GPP.

#### 6.2.2.7 Security Considerations for SRv6

The security consideration related to SRv6 is detailed in IETF draft-ietf-6man-segment-routing-header-18 [6]. The security mechanisms described in that document only allow securing an SRv6 network within a single domain. 5GC requires security mechanisms for nodes communicating in different domains (e.g. inter-PLMN).

In order to secure inter-domain scenarios, 3GPP extends the security requirements defined by IETF as follows:

In the enhanced mode, for SR nodes outside of the domain HMAC can be used. Alternatively, if anti-replay protection is required, IPSec with AH can be used as a substitute of HMAC. In the traditional mode, IPSec with AH can be used.

Editor's Note: All the SRv6 security considerations needs to be reviewed and assessed by SA3 Group.

#### 6.2.2.8 Using SRH for User Plane Messages

##### 6.2.2.8.1 General

The Figure 6.2.1.2-1 shows the Segment Routing Header format. In the SR Extension Header there is 16 bits Tag field, which is explained in IETF draft-ietf-6man-segment-routing-header-18 [6]. IETF does not define the format or use of the Tag field. Hence the format of Tag field can be defined by 3GPP independently of IETF and only the UPF will process the Tag field in the SR Header. Tag can be used to indicate user plane messages, Echo Request, Echo Reply, End Marker and Error Indication. Any other transport router that implements SRv6 must ignore this field upon SRH processing.

Upon presence of user plane messages, the UPF cannot encode any segment in the SRH whose function modifies the Tag value.

##### 6.2.2.8.2 Tag Encoding

The Tags field can be encoded as described in Figure 6.2.2.8.2-1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Bit 4 of Octet [1] to Bit 7 of Octet [1] are  Reserved | Bit 3 [Octet-1]  Echo Reply  Bit | | Bit 2 [Octet-1]  Echo Request Bit | Bit 1 [Octet-1]  Error Indicator Bit | Bit 0 [Octet1]  End Marker bit |
| Octet[2] of Tag is reserved | | | | | |
| Bit 0 | | End Marker Bit. When set to 1, this indicates End Marker. Default value is set to 0 | | | |
| Bit 1 | | Error Indicator Bit. When set to 1, this indicates Error. Default value is set to 0. | | | |
| Bit 2 | | Echo Request Bit. When set to 1, this indicates Echo Request. Default value is set to 0. | | | |
| Bit 3 | | Echo Reply Bit. When set to 1, this indicates Echo Reply. Default value is set to 0. | | | |
| Bit 4- Bit15 | | Reserved. | | | |

Figure 6.2.2.8.2-1 Tags Encoding Details

Additional information elements for Error Indication, e.g Tunnel Endpoint Identifier Data I, GSN Address etc, can be encoded in the SRH TLV as explained in clause 6.2.2.13.

#### 6.2.2.9 Packet forwarding between SMF and UPF

The PFCP-u tunnel, one PFCP tunnel per UPF or PDN, as explained in clause 5.3.4 of 3GPP TS 29.281 [2], shall be used between SMF and UPF. The T-PDU packet received at UPF from N9 or N6 shall be forwarded to SMF as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the SMF for the PFCP-u tunnel corresponding to the UPF or PDN. Similarly, the G-PDU packets received from the UE on N3 interface shall be forwarded to the SMF on PFCP-u tunnel with new GTP-U header.

Even when SRv6 is used for user plane forwarding for N9, the forwarding of data between SMF and UPF still uses GTP-U. UPF will always construct a G-PDU, as defined above, from T-PDU received on N3 or N6 or N9 interface.

#### 6.2.2.10 Roaming Support

As home-routed roaming procedure defined in TS 23.502 [8], the following are the impacts on SMF PDU Session Service of TS 29.502 [29] over N16 (between V-SMF and H-SMF) and over N16a (between I-SMF and SMF) identified due to the principle proposed in clause 6.2.2.2.

- Addition of "SRv6 Capable IE" in Nsmf\_PDUSession Create Request / Response.

- Addition of "SRv6 SID IE" in Nsmf\_PDUSession Create Request / Response / Update.

Based on roaming agreement, operators may configure the UPFs to use Traditional mode or Enhanced mode. The V-SMF and H-SMF do not need to distinguish both two modes over N16 due to the both modes are configured in UPF based on local information.

Security consideration shall be applied for the SRv6 user plane in roaming as described in clause 6.2.2.7.

#### 6.2.2.11 Failure Detection and Recovery

##### 6.2.2.11.1 General

This clause describes failure detection and recovery in SRv6 user plane as per clause 5 of TS 23.527 [11] defined.

##### 6.2.2.11.2 Failure Detection

###### 6.2.2.11.2.1 Loss of SRv6 SID contexts

An SRv6 user plane enabled UPF may lose its SRv6 SID contexts upon a failure or restart.

When an UPF receives a SRv6 User Plane packet for which no corresponding SID exists, the UPF shall discard the SRv6 User Plane packet and return an Error Indication encoded in SRH to the sending UPF, as specified in clause 6.2.2.8.

The receipt of an Error Indication in SRH is an indication for the sending UPF that the peer UPF entity cannot receive any more user plane traffic on the corresponding SID.

###### 6.2.2.11.2.2 User Plane Path Failure

An UPF may detect a user plane path failure by using Echo Request and Echo Response encoded in SRH, as specified in clause 6.2.2.8.

In addition to that, when a Network Instance detects user plan path failure as per IETF draft-ietf-spring-segment-routing-policy-02 [30], the UPF with the Network Instance is able to detect the user plane path failure.

##### 6.2.2.11.3 Restoration Procedure

###### 6.2.2.11.3.1 SRv6 Error Indication received by another UPF

Upon receipt of an Error Indication in SRH, the UPF shall identify the related PFCP session and send an Error Indication Report to the SMF, as specified in clause 5.10 of 3GPP TS 29.244 [9].

Upon receipt of an Error Indication Report from the UPF, the SMF shall identify the PDU session for which the Error Indication is received using the remote SID included in the report.

For an Error Indication received from another UPF, the SMF shall delete the PFCP session and PDU session, unless the UPF from which the Error Indication was received is controlled by the same SMF and the SMF is able to restore the user plane connectivity of the PDU session (e.g. Error Indication received from an Intermediate UPF controlled by the same SMF).

NOTE: The procedure for Error Indication received from 5G-AN case is out of scope of this study.

###### 6.2.2.11.3.2 Restoration Procedures upon User Plane Path Failure

Upon detecting a SRv6 user plane path failure as specified in clause 6.2.2.11.2, the UPF shall report the user plane path failure to the SMF, by sending a PFCP Node Report Request (see TS 29.244 [9]) including a User Plane Path Failure Report with the SID of the remote SRv6 peer(s) towards which a failure has been detected. The UPF should also notify the SRv6 user plane path failure via the Operation and Maintenance system.

The procedure of how the SMF processes the reported failure is described in clause 5.4 of TS 23.527 [11].

##### 6.2.2.11.4 Restoration Procedure for User Plane Related Entities

The restoration procedure of UPF and SMF are all identical with the GTP-U case described in clause 4.3 and 4.4 of TS 23.527 [11] except the user plane protocol is SRv6.

#### 6.2.2.12 SRv6 Guaranteed Packet Delivery

##### 6.2.2.12.1 General

There is a requirement for sending redundant transmission of user plane packets on N9 (and N3). SRv6 provides mechanisms for both packet duplication and dropping the duplicate packet. This mechanism shall be applied to either only the N9 interface, or to both the N3 and N9 interface when interworking with GTP-U.

##### 6.2.2.12.2 Redundant packet transmission for downlink traffic

At the source UPF, the traffic associated with the ultra-low latency, jitter, and loss requirement is steered into the new type of SR-TE (SRv6 Traffic Engineering) policy called Spray Policy. The Spray policy replicates the packets over SID lists that encode a disjoint path in the network. Typically, the packets are replicated over two disjoint SR paths, but replication over more than two paths is also possible. Each packet is tagged with a flow ID and a sequence number in the SRH TLV.

The TLV has the format defined in IETF draft-geng-detnet-dp-sol-srv6 [28]. Clause 5.1 "TLV Based SRv6 Data Plane Solution" details the data replication function.

NOTE: The intermediate SRv6 routers neither process nor inspect the TLV unless explicitly instantiated to do so. clause 2.1 of IETF draft-ietf-6man-segment-routing-header-18 [6] mentions "While processing the SID defined in clause 4.3.1, all the TLVs are ignored unless local configuration indicate otherwise"

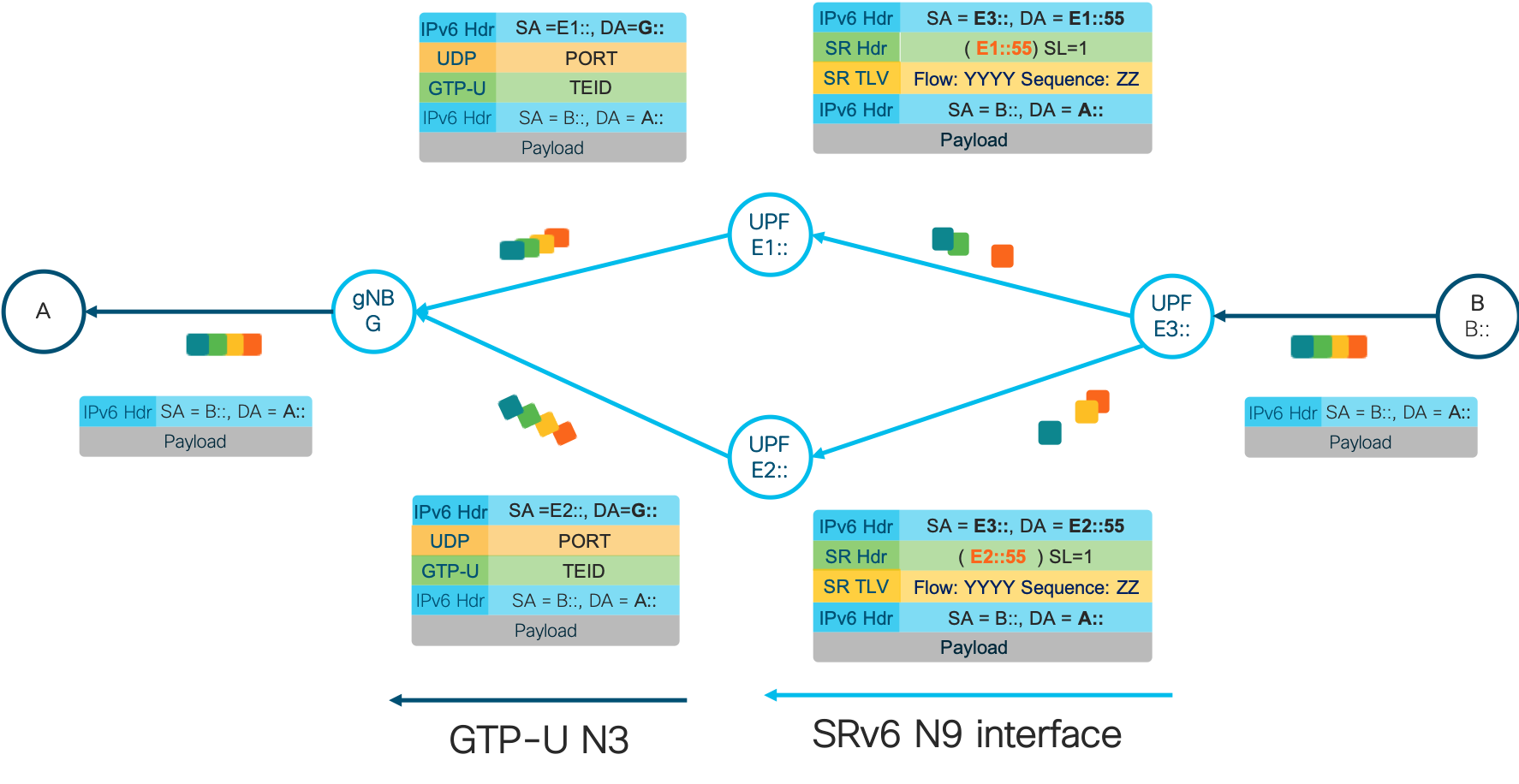


Figure 6.2.2.12.2-1: Redundant downlink packet transmission for URLCC use case

##### 6.2.2.12.3 Removal of Redundant packet for uplink traffic

The endpoint of the Spray policy is represented by the last SID. At the endpoint, the UPF removes duplicate packet arriving with the same SRv6 SID.

Upon reception of a packet with active SID bounded to a duplicate removal function, the node checks whether a packet with same (SA, FlowID, SeqNumber) has been delivered. In case another replica of this packet has indeed been delivered then the current packet is dropped. Otherwise, the packet is delivered and state is recorded.

The TLV has the format defined in IETF draft-geng-detnet-dp-sol-srv6 [28]. Clause 5.1, 'TLV Based SRv6 Data Plane Solution', details the packet elimination function.

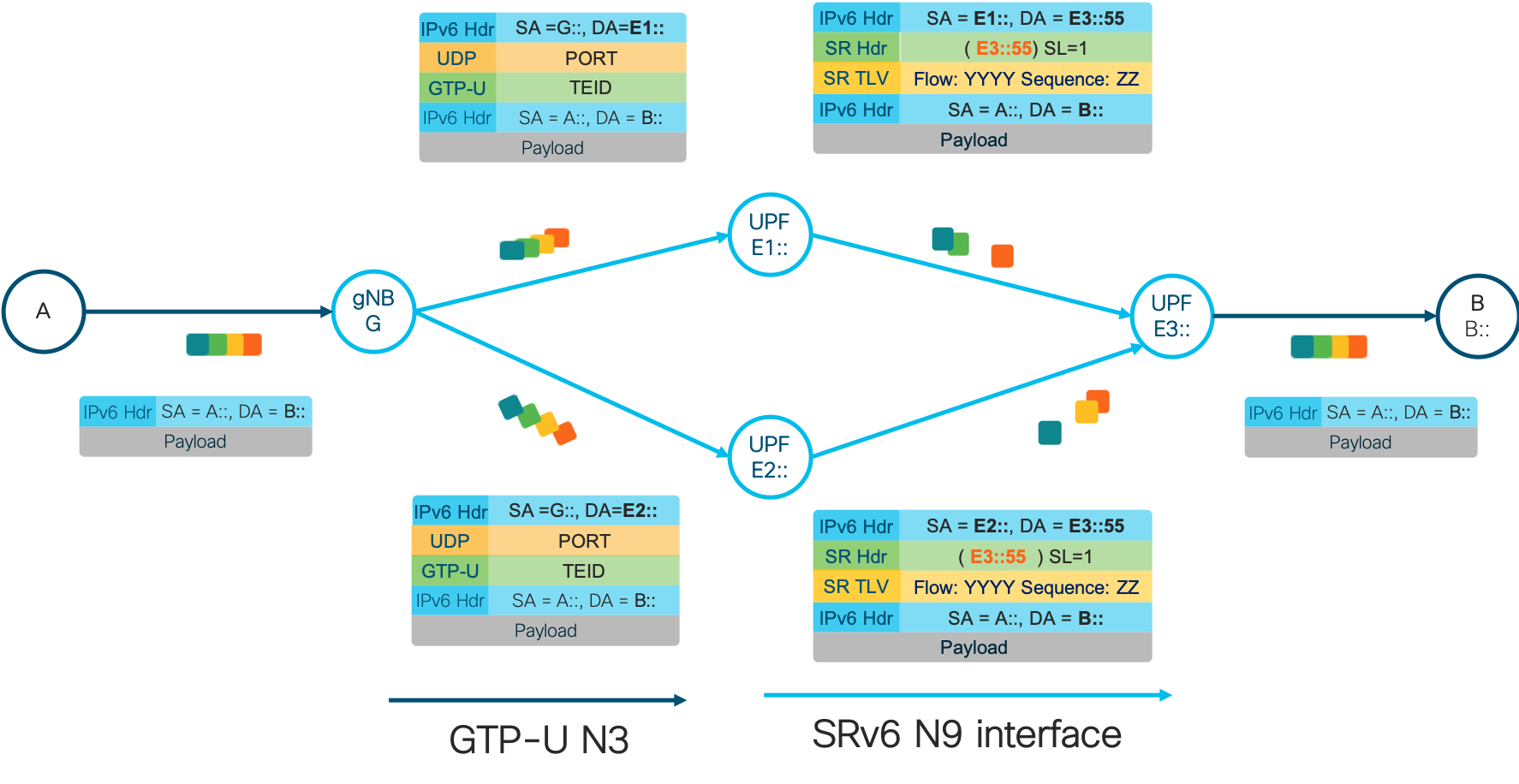


Figure 6.2.2.12.3-1: Removal of Redundant packets for uplink traffic for URLCC case

#### 6.2.2.13 SRv6 extensibility using SRH TLVs

The SRv6 SID carries TEID, QFI and RQI bits which is explained in clause 6.2.2.3. But SRv6 SID has limited space and it cannot carry many information elements which requires additional bits.

For sending more information element, SRv6 shall leverage the SRH TLVs, as explained in clause 6.2.1.2. This document proposes a new SRH TLV that is the "5GS container", which should be allocated by IANA. This new 3GPP specific "Type" can contain additional 3GPP IEs in the nested TLVs within the "5GS container". The number of 3GPP IEs could be one or many, depending on the use case. The diagram below shows an example with only one additional 3GPP IE.

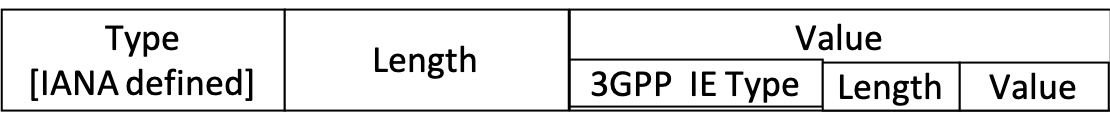


Figure 6.2.2.13-1: Using TLV to send one 3GPP specific IEs in SRH

The diagram below shows an example with multiple additional 3GPP IEs.

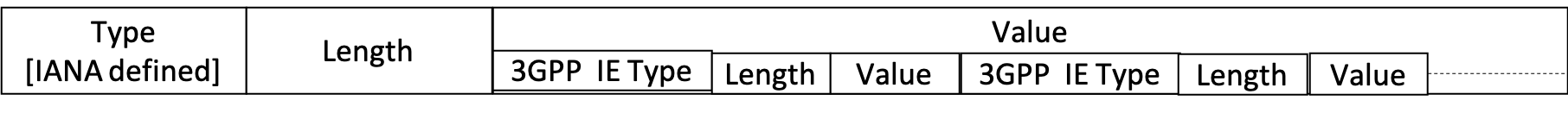


Figure 6.2.2.13-2: Using TLV for sending multiple 3GPP specific IEs in SRH

The current list of objects of PDU Session User Plane Protocol, as defined in TS 38.415 [10], are supported as parts of Argument of SRv6 user plane, except PPI which is not applicable for N9. TLV of SRH is a generic format which can be used to encode all the current list of objects of PDU Session User Plane protocol as defined in TS 38.415 [10] and it also allows encoding of any new IEs that may get added in the future.

TS 38.415 [10] specifies that PDU session information are encoded together in user plane protocol. But SRv6 solution does not comply with the PDU definition of this user plane protocol. In SRv6 solution some of the information elements like QFI, RQI etc are encoded in SID and remaining information elements are encoded in SRH TLV, which follows SID in the SRH.

### 6.2.3 System Impacts

#### 6.2.3.1 General

This clause studies SRv6 impact on 3GPP 5GC system.

#### 6.2.3.2 Common System Impacts of SRv6

See clauses 7.1.3.1.4 and 7.1.3.2.4.

##### 6.2.3.2.1 System Impact on N4 interface

###### 6.2.3.2.1.1 General

This clause studies the impact on PFCP protocol on N4 interface for supporting SRv6. The PFCP procedures, messages and IEs along with the PFCP protocol is defined in TR 29.244 [9].

###### 6.2.3.2.1.2 Impact on PFCP procedure

The existing PFCP protocol, used for N4 interface between SMF and UPF, may be extended in case SMF wants to send some SRv6 specific information to UPF and vice versa. The table below lists the possible changes in the existing PFCP messages.

Table 6.2.3.2.1.2-1: Impact on N4 Procedures

|  |  |  |
| --- | --- | --- |
| PFCP Procedure | | Expected Impacts |
| **Node related procedures** | Heartbeat | N/A |
| Load Control | N/A |
| Overload Control | N/A |
| PFD Management | N/A |
| Association Setup | SMF needs to be indicated about SRv6 capability of UPF. |
| Association Update | Same as Association Setup. |
| Association Release | N/A |
| Node Report | N/A |
| **Session Related Procedures** | Session Establishment | SMF needs to indicate UPF about SRv6 session for every PDU session that is getting established. |
| Session Modification | Same as Session Establishment. |
| Session Deletion | N/A |
| Session Report | UPF needs to report SMF about Error Indication for SRv6 SID context and/or user plane path. |
|  |  | |

Editor's Note: Any additional impact on N4 procedure is FFS.

###### 6.2.3.2.1.3 Impact on PFCP IEs

It is expected that N4 interface protocol shall be able to bring SRv6 related information in the following PFCP IEs. Note that SRv6 leverages IPv6 addresses to represent segments so that the N4 interface protocol does not need to support any new ID type for SRv6 user plane in addition to the existing IPv4 and IPv6 ID format.

Table 6.2.3.2.1.3-1: SRv6 Impacts on PFCP IEs

|  |  |  |
| --- | --- | --- |
| PFCP IE | | Expected Impacts |
| **PDR related IEs** | PDI | The Local F-TEID IE and Traffic End point needs changes to indicate SRv6 capability. |
| Outer Header Removal | Outer Header Removal ID needs changes to indicate SRv6 capability |
| **FAR related IEs** | Forwarding Parameters | The Outer Header Creation IE and Linked Traffic Endpoint ID IE need changes to indicate SRv6 capability. |
| **URR related IEs** |  | N/A |
| **QER related IEs** |  | N/A |
| **BAR related IEs** | Error Indication Report | The Remote F-TEID IE needs changes to indicate error on SRv6 SID. |

Editor's Note: Any additional impact on PFCP IEs is FFS.

##### 6.2.3.2.2 System Impact on N16/N16a/N38 interfaces

The following list shows the impacts for N16, N16a and N38.

- N16:

- impacts V-SMF and H-SMF to negotiate the use of SRv6 during PDU session establishment, and during EPS to 5GS idle mode and connected mode mobility;

- N16a:

- impacts I-SMF and SMF to negotiate the use of SRv6 during PDU session establishment, or insertion of an I-SMF to an existing PDU session;

- N16a and N38:

- impacts V-SMF or I-SMF to include support of SRv6 in SM contexts exchange, and for setting up forwarding tunnels using SRv6 upon insertion or change of V-SMF or I-SMF.

#### 6.2.3.3 System Impacts of Traditional Mode

See clause 7.1.3.1.4.

#### 6.2.3.4 System Impacts of Enhanced Mode

See clause 7.1.3.2.4.

# 7 Evaluations and Comparison

## 7.1 Evaluation

### 7.1.1 Evaluation Points

The candidate user plane protocol solutions are evaluated in this clause on the following aspects:

1) Whether they fulfil the architectural requirements for User Plane specified in clause 5.1;

2) Key issues identified in clause 5.2;

3) System impacts.

### 7.1.2 GTP-U

#### 7.1.2.1 General

This clause evaluates the GTP-U solution described in clause 6.1.

#### 7.1.2.2 Architectural requirements for User Plane

GTP-U supports all the 3GPP architectural requirements specified in clause 5.1. GTP-U supports in particular the following capabilities:

- GTP-U can run over IPv4 and IPv6 networks;

- the PFCP protocol over N4 supports the establishment, modification and release of GTP-U tunnels;

- GTP-U supports signalling messages, such as End Marker to assist packets reordering in the target RAN during mobility scenarios;

- GTP-U extension headers can be defined to convey information together with GTP-PDU; the PDU Session User Plane Protocol (defined in TS 38.413 [10] and containing 5GS information) is conveyed in such a GTP-U extension header;

- GTP-U is supported on roaming interface between VPLMN and HPLMN since Rel-99 onwards;

- GTP-U supports error detection and error reporting capabilities, to detect and handle the loss of a user plane context in a peer UPF and to detect and handle the loss of a user plane context associated with a user plane packet at the receiving UPF.

#### 7.1.2.3 Key issues

Regarding IP connectivity for N9 and Network Slicing, GTP-U can use existing transport technologies, such as L2 or L3 VPNs, MPLS-based services or segment routing (SR-MPLS, SRv6), as described in clause 5.2.1.1.

#### 7.1.2.4 System impacts

GTP-U is already supported in the RAN and Core Network, in the 5G System, EPS and GPRS networks.

No impacts are identified, other than those listed in clause 6.1.3.2.2 for the optional support of UDP zero checksum for GTP-U over IPv6.

### 7.1.3 SRv6

#### 7.1.3.1 Traditional Mode

##### 7.1.3.1.1 General

This clause evaluates the SRv6 Traditional Mode solution described in clause 6.2.

##### 7.1.3.1.2 Architectural requirements for User Plane

SRv6 in Traditional Mode supports the 3GPP architectural requirements specified in clause 5.1, with the following limitations as per the current solution:

1) Requirement 8 of clause 5.1.1: the solution does not support the PDU Session User Plane Protocol over N9 as specified in Annex A of TS 29.281 [2] and in TS 38.415 [10]:

- the solution described in clause 6.2.2.3.2 does only enable to encode the RQI and QFI, which are only two specific parameters of the PDU Session User Plane Protocol;

- the PDU Session User Plane Protocol is a protocol that defines PDU types (e.g. UL PDU SESSION INFORMATION, DL PDU SESSION INFORMATION) and parameters; more PDU types and parameters may be defined in future.

Editor's Note: a solution to support the above requirement is FFS.

2) Requirement 10 of clause 5.1.1: for home routed roaming, security requirements and tentative 3GPP extensions to existing IETF security requirements for use of SRv6 across SR Domain (e.g. inter-PLMN) needs to be reviewed and assessed by SA3 (see clause 6.2.2.7).

##### 7.1.3.1.3 Key issues

Regarding IP connectivity for N9 and Network Slicing, SRv6 in Traditional Mode does not encode any SRH header and therefore has to rely on the IPv6 transport network technologies, or underlay transport technologies such as L2 or L3 VPNs, as described in clause 5.2.1.1.

##### 7.1.3.1.4 System impacts

The solution impacts the following 3GPP system entities:

- UPF:

- N9 impacts to support SRv6 as a replacement of GTP-U, including support of T-PDUs (i.e. user data packets) and GTP-U functionality parity with End Markers, Error Indication, Echo Request/Response and Sequence Number;

- N4 impacts to support use of SRv6 as a replacement of GTP-U (i.e. advertising capabilities of the UPF and establishing N4 sessions using ingress and/or egress SRv6 as replacement of GTP-U);

- support of Interworking between GTP-U and SRv6 as a replacement of GTP-U, i.e. conversion between GTP-U packets and SRv6 packets including conversion between the GTP-U PDU Session Container extension header and the PDU Session Container information in SRv6 packets;

- support of static IPv4 tunnelling or 6rd over N9, if SRv6 is run over IPv6 over IPv4;

- SMF, V-SMF, H-SMF and I-SMF:

- N4 impacts to support use of SRv6 as a replacement of GTP-U (i.e. learn capabilities of the UPF and establish N4 sessions using ingress and/or egress SRv6 as replacement of GTP-U);

- N16 impacts for the V-SMF and H-SMF to negotiate the use of SRv6 as a replacement of GTP-U during the PDU session establishment and during EPS to 5GS idle mode and connected mode mobility;

- N16a impacts for the I-SMF and SMF to negotiate the use of SRv6 as a replacement of GTP-U during the PDU session establishment or during the insertion of an I-SMF to an existing PDU session;

- N4 impacts to support Interworking between GTP-U and SRv6 as a replacement of GTP-U;

- SMF impacts for SMF constructing End Marker packets (see clause 5.8.2.9.2 of TS 23.501 [7]), requiring the SMF to support SRv6 SRH;

- N38 (between two V-SMFs or two I-SMFs) and N16a (for insertion of an I-SMF to an existing PDU session) impacts for exchange of SM contexts including support of SRv6 as a replacement of GTP-U, and for setting up forwarding tunnels using SRv6 as a replacement of GTP-U upon insertion or change of V-SMF or I-SMF;

- Impacts for discovery and selection of UPFs supporting SRv6 as a replacement of GTP-U;

- NRF:

- Impacts to the NF Management and NF Discovery APIs to support the registration and discovery of SMF and UPF supporting SRv6 as a replacement of GTP-U;

- N27 impacts (between vNRF and hNRF) for discovering a H-SMF that supports SRv6 as a replacement of GTP-U;

- AMF:

- AMF impacts for discovering and selecting SMFs supporting SRv6 as a replacement of GTP-U when not all SMFs in the serving or home PLMN support SRv6, e.g. for preferentially selecting a V-SMF and a H-SMF supporting SRv6 as a replacement of GTP-U for a Home Routed PDU session.

The solution requires impacts to the following interfaces (see above for the description of the impacts):

- N9 (between UPFs and between V-UPF and H-UPF);

- N4 (between SMF and UPF);

- N16 (between V-SMF and H-SMF);

- N16a (between I-SMF and SMF);

- N38 (between two V-SMF or I-SMF);

- Nnrf (between AMF, SMF, UPF and NRF);

- N27 (between V-NRF and H-NRF).

Editor's Note: the complete list of impacts is still FFS until the solution is fully described.

Editor's Note: Potential impacts to Lawful Interception should be assessed by 3GPP SA3-LI.

#### 7.1.3.2 Enhanced Mode

##### 7.1.3.2.1 General

This clause evaluates the SRv6 Enhanced Mode solution described in clause 6.2.

##### 7.1.3.2.2 Architectural requirements for User Plane

SRv6 in Enhanced Mode supports the 3GPP architectural requirements specified in clause 5.1, with the following limitations as per the current solution:

1) same limitations as defined for SRv6 in Traditional Mode in clause 7.1.3.1.2;

2) in roaming scenarios, SIDs in SRv6 packets may be limited to segments of one PLMN since information about the transport network topology from one PLMN is not exposed to a roaming partner.

##### 7.1.3.2.3 Key issues

Regarding IP connectivity for N9 and Network Slicing, SRv6 in Enhanced Mode would allow to encode SRH headers to force the data path to go through intermediate SRv6 routers between two UPFs.

##### 7.1.3.2.4 System impacts

All the impacts to the 3GPP system entities and interfaces described in clause 7.1.3.1.4 also apply to SRv6 Enhanced Mode. The following additional impacts also apply:

- UPF:

- configuration of SIDs per Network Instance and insertion of SIDs in egress SRv6 packets;

- the IPv6 DA set by FAR needs to be moved as the last SID in the list and the topmost SID in the SID list configured for the network instance needs to be put as the IPv6 DA of the packet.

Editor's Note: the complete list of impacts is still FFS until the solution is fully described.

## 7.2 Additional Considerations

### 7.2.1 Consideration Points

Additional considerations for the candidate user plane protocol solutions are identified in Table 7.2-1.

Table 7.2.1-1: Additional Considerations

|  |  |
| --- | --- |
| Additional Considerations | Description |
| A1. Proven technology / Time of Availability of used standards | Proven technology and the date of availability of related standards will be indicated. |
| A2. Enabling separation between 3GPP User Plane and Transport | Mobile and transport network operators may be different. Even when the same operator operates the mobile and transport networks, both networks may be managed by different organizations and systems.  This criterion evaluates whether the solution allows to keep the mobile and transport networks separate. |
| A3. Transport network requirements | This criterion evaluates whether the solution imposes specific requirements on the transport networks. |
| A4. Co-existence with existing User Plane solution | This criterion evaluates the coexistence with network entities implementing the existing solution. |
| A5. Interworking with RAN | This criterion evaluates how the solution interworks with the RAN. |
| A6. Interworking with EPS | This criterion evaluates how the solution interworks with the EPS. |
| A7. Impacts to GSMA GRX/IPX | This criterion evaluates whether the solution may impact GRX/IPX. |
| A8. Security | GSMA has specified user plane security solution for GTP-U in EPC (based on GTP-U firewall). GSMA and 3GPP SA3 are further studying GTP-U security in 5G System. See Study on Security Aspects of the 5G Service Based Architecture and Inter-PLMN Communication in S3-190464.  This criterion evaluates whether the solution may impact GSMA and require SA3 work for user plane security across roaming interfaces. |
| A9. Minimize number of protocols in network | It is desirable to minimize the number of protocols in the network, when possible.  This criterion evaluates the impact of the solution on the resulting number of protocols in the network. |
| A10. Reusability of existing 3GPP implementations | This criterion evaluates whether the solution allows reuses of existing 3GPP implementations, e.g. reuse of UPF. |
| A11. Protocol Extensibility | This criterion evaluates the extensibility of the User Plane protocol to support additional features in future. |
| A12. Protocol Overhead | This criterion evaluates the user plane protocol stack / overhead of the solution. |
| A13. Resource-efficiency | This criterion evaluates whether the solution allows to remove states from the UPF. |
| A14. Routing capabilities | This criterion evaluates the solution in terms of routing capabilities and whether the solution allows to support fast rerouting if a failure affects the user plane path between UPFs. |
| A15. Scalability | This criterion evaluates whether the solution meets the scalability requirements of 5G to support massive number of connected devices. Both scale in and out should be evaluated. |
| A16. Performance | This criterion evaluates whether the user plane protocol can easily meet the diverse performance requirement of different network slices. E.g the performance requirement for URLCC slice can be very different from any other slice. |
| A17. Programmability | SMF needs to handle a large number of UPFs in large deployments. This criterion evaluates how easy or difficult is to program network instructions between SMF and UPF. |
| A18. Signalling Optimisation | The current N4 interface between SMF and UPF is very chatty and there is a need to optimise the N4 interface signalling. This criterion evaluates which solution offers better signalling optimisation. |
| A19. Load Balancing | There could be multiple transport path between ingress and egress UPFs. This criterion evaluates the load balancing capability of user plane protocol among multiple paths. |
| A20. Entropy support | The transport network routers use standard fields of the IP headers to perform hashing of packets.  In the case of IPv4 based protocols, this is a standard 5-tuple based on the IP SA, DA, Transport header type, Transport header protocol source and destination.  In the case of IPv6 based protocols, this is a standard 3-tuple based on the IP SA, DA and FlowLabel. This criterion evaluates which user plane protocol is better suited for Entropy support. |

### 7.2.2 GTP-U

Table 7.2.2-1 describes the GTP-U solution on the additional considerations defined in clause 7.2.1.

Table 7.2.2-1: Additional Considerations for the GTP-U solution

|  |  |
| --- | --- |
| Additional Considerations | Description |
| A1. Proven technology / Time of Availability of used standards | GTPv1 has been specified by 3GPP from Rel-99 onwards.  GTP-U has been used extensively in the 3GPP system, in the RAN and Core Network in 5G System, EPS and earlier generation's mobile networks. |
| A2. Enabling separation between 3GPP User Plane and Transport | The 3GPP User Plane and Transport are decoupled, allowing different operators, organization and systems to operate the mobile and the transport networks.  The 3GPP User Plane and Transport can evolve in parallel without restricting either technology (e.g. GTP-U over IP, MPLS, SR-MPLS, SRv6). |
| A3. Transport network requirements | GTP-U runs over IPv4, IPv6 and existing transport network technologies.  GTP-U supports heterogenous transport network and segment optimized transport options (e.g. MPLS or SR MPLS in Backhaul, SR MPLS or SRv6 in Aggregation/Core, SR MPLS or VxLAN/GRE in Data Center). |
| A4. Co-existence with existing User Plane solution | This is the existing solution.  Use of UDP zero checksum over IPv6 is negotiated via control plane signalling during the setup of the GTP-U tunnel. |
| A5. Interworking with RAN | Same solution as supported in the RAN.  Use of UDP zero checksum over IPv6 is negotiated via control plane signalling during the setup of the GTP-U tunnel. |
| A6. Interworking with EPS | Same solution as supported in EPS. |
| A7. Impacts to GSMA GRX/IPX | No impact. |
| A8. Security | GSMA has specified user plane security solution for GTP-U in EPC. GSMA and 3GPP SA3 are further studying GTP-U security in 5G System. |
| A9. Minimize number of protocols in network | Same protocol as in existing solution in RAN and CN in 5GS, EPS and earlier mobile network generations. |
| A10. Reusability of existing 3GPP implementations | Existing SMF and UPF implementations can be reused, with the only optional addition of UDP zero checksum negotiation for IPv6.  Transport remains agnostic of the number of PDU sessions setup in the network (number of 5-tuple flows visible in transport layer is relatively low as PDU sessions are aggregated). |
| A11. Protocol Extensibility | GTP-U supports the capability to define new extension headers. This has been used in past releases to support several features, e.g. RAN containers, PDU Session Container (5GS information) over N9 and N3, Service Class Indicator, PDCP PDU numbers.  GTP-U does not place any constraint on the size of the GTP-U extension headers, and therefore allows future extensions of the PDU Session Container Protocol used over N9 and N3. |
| A12. Protocol Overhead | GTP-U header: 12 octets.  GTP-U Extension Header (PDU Session Container): 4 octets  UDP header: 8 octets. |
| A13. Resource-efficiency | Per 3GPP system architecture requirements, 3GPP user plane functionalities are controlled in UPF by the SMF over the N4 interface; the UPF shall keep states for the established PFCP associations and PFCP sessions.  A GTP-U tunnel endpoint is identified by an IP address and a TEID (4 octets). |
| A14. Routing capabilities | Routing capabilities supported by IPv4, IPv6 or the underlying transport technologies (e.g. MPLS, SR-MPLS, SRv6).  GTP-U in addition to the basic routing capabilities supported by IPv4, IPv6 or the underlying transport technologies, exposes session and QoS flow in GTP-U header which allows to provide routing differentiation by look up of the corresponding header. Routers in 3GPP systems can support look up of GTP-U headers, but this may not be supported by basic IP routing nodes.  GTP-U supports error detection and error reporting capabilities.  MPLS Fast Reroute is supported (if MPLS is used). |
| A15. Scalability | No difference between both solutions: UPF functionalities are controlled by the SMF over N4 and UPFs keep the same states for PFCP associations and PFCP sessions. |
| A16. Performance | No difference expected between both solutions. There is an extra UDP layer. Most implementations are expected to process 5-tuple with UDP header as standard function with negligible impact on performance. |
| A17. Programmability | No difference between both solutions: UPF functionalities are controlled by the SMF over N4. |
| A18. Signalling Optimisation | No difference between both solutions: UPF functionalities are controlled by the SMF over N4. |
| A19. Load Balancing | Load sharing can be achieved in multiple levels:  On GTP-U protocol level, per tunnel-session based load sharing is supported as the destination IP address and Tunnel Endpoint ID is allocated by the receiver. This mechanism is complemented by lower layer load balancing mechanism. See A20 for other levels using entropy bits in protocol headers. |
| A20. Entropy support | On UDP/IP level, Entropy for load balancing is also permitted but not mandated by the GTP-U protocol.  Use of dynamic source UDP port for entropy support is documented in the GTP-U specification (the algorithm to set the dynamic source UDP port is implementation specific). Flow Label can also be used for entropy support with IPv6.  Additionally, when GTP-U is transported over IPv6/SRv6, entropy for load balancing is recommended using IETF RFC 6438 [31]. |

### 7.2.3 SRv6

Table 7.2.3-1 describes the SRv6 Traditional Mode on the additional considerations defined in clause 7.2.1.

Table 7.2.3-2 evaluates the SRv6 Enhanced Mode on the additional considerations defined in clause 7.2.1.

Table 7.2.3-1: Additional Considerations on SRv6 in Traditional Mode

|  |  |
| --- | --- |
| Additional Considerations | Description |
| A1. Proven technology / Time of Availability of used standards | IETF work on SRv6 related improvements is still in progress.  SRv6 as a replacement of GTP-U would require new 3GPP standardization work. |
| A2. Enabling separation between 3GPP User Plane and Transport | 3GPP User Plane and IP transport are collapsed/integrated, with the IP destination address encoding the IP address of the peer UPF, the TEID of the specific user plane tunnel and other 3GPP related information (e.g. QFI, RQI).  With SRv6 as a GTP-U replacement, 3GPP User Plane and Transport are tied in one technology. |
| A3. Transport network requirements | SRv6 essentially relies on IPv6. IPv4 networks might be considered but at the expense of extra signalling overhead and operational costs.  The length of the IPv6 prefix is constrained to keep enough bits to the Function and Arguments of the SID (see Figure 6.2.2.3.2.1). |
| A4. Co-existence with existing User Plane solution | Co-existence with 3GPP user plane entities supporting only GTP-U is required.  Use of SRv6 in Traditional Mode needs to be negotiated via control plane signalling during the setup of the user plane tunnel (in a backward compatible manner to take into account implementations that do not support SRv6 and corresponding negotiation signalling). |
| A5. Interworking with RAN | The solution requires interworking GTP-U over N3 and SRv6 over N9, including interworking the PDU Session User Plane Protocol (in GTP-U extension header over N3, and in the Destination IP address in SRv6 in Traditional Mode), causing impacts in UPF. |
| A6. Interworking with EPS | GTP-U is supported on user plane interfaces in the EPS.  The solution requires the UPF/PGW-U to support different user plane protocols and to switch from one to the other as the PDU session moves between EPS and 5GS. |
| A7. Impacts to GSMA GRX/IPX | GSMA would need to study the support of SRv6 in GRX/IPX as a replacement of GTP-U (including security aspects, see A8). |
| A8. Security | Due to security considerations mentioned in clause 8.2 of IETF RFC 8402 [5], packets sent over SRv6 from one PLMN to another across N9 in home routed roaming cases will be filtered/dropped. Security requirements and proposed 3GPP extensions to existing IETF security requirements for use of SRv6 across SR Domain (e.g. inter-PLMN) need to be reviewed and assessed by SA3 (see clause 6.2.2.7).  GSMA has specified user plane security solution for GTP-U in EPC (based on GTP-U firewall). GSMA and 3GPP SA3 are further studying GTP-U security in 5G System. GSMA and 3GPP SA3 would need to be involved to study SRv6 user plane security in 5G System. |
| A9. Minimize number of protocols in network | The solution would add one new 3GPP user plane protocol solution, for use over the N9 interface. Other interfaces would continue to support GTP-U, e.g. N3, N4-u, S5/S8. |
| A10. Reusability of existing 3GPP implementations | SMFs and UPFs need to be modified to implement SRv6 as a replacement of GTP-U and reproduce existing GTP-U functionalities (e.g. End Markers, PDU Session User Plane Protocol). |
| A11. Protocol Extensibility | The SRv6 extensibility is explained in clause 6.2.1.2. |
| A12. Protocol Overhead | No UDP (8 octets) and GTP-U (12 octets) headers.  If SRv6 is supported over IPv4: extra IPv6 header (40 octets). |
| A13. Resource-efficiency | Per 3GPP system architecture requirements, 3GPP user plane functionalities are controlled in UPF by the SMF over the N4 interface; the UPF shall keep states for the established PFCP associations and PFCP sessions, like for GTP-U. |
| A14. Routing capabilities | SRv6 in Traditional Mode does not encode any SRH header and therefore has to rely on the IPv6 transport network or underlay transport technologies.  SRv6 in addition to the basic routing capabilities supported by IPv6 or the underlying transport technologies, exposes session and QoS flow in IPv6 DA to IP transport to provide routing differentiation by fundamental IP forwarding mechanism (i.e. longest prefix match). The solution supports error detection and error reporting capabilities. Fast Rerouting is also supported. |
| A15. Scalability | No difference between both solutions: UPF functionalities are controlled by the SMF over N4 and UPFs keep the same states for PFCP associations and PFCP sessions. |
| A16. Performance | No difference expected between both solutions. There is no UDP layer. |
| A17. Programmability | No difference between both solutions: UPF functionalities are controlled by the SMF over N4. SRv6 network programmability is not used in the 3GPP system. |
| A18. Signalling Optimisation | No difference between both solutions: UPF functionalities are controlled by the SMF over N4. |
| A19. Load Balancing | See A20. |
| A20. Entropy support | Entropy for load balancing is mandated by the SRv6 protocol (using the Flow Label field in the IPv6 header, see clause 5.5 of IETF draft-ietf-6man-segment-routing-header-18 [6]). This is identical to GTP-U over SRv6. |

Table 7.2.3-2: Additional Considerations on SRv6 in Enhanced Mode

|  |  |
| --- | --- |
| Additional Considerations | Description |
| A1. Proven technology / Time of Availability of used standards | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A2. Enabling separation between 3GPP User Plane and Transport | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1).  In addition, SRH headers also encode IP addresses of intermediate IP routers on the path, requiring the UPF (mobile network) to be configured with information about the SIDs and thus topology of the transport network.  This essentially assumes mobile and transport networks from a same operator. |
| A3. Transport network requirements | To use the full set of functionalities, the solution relies on IPv6 and SRv6 capable networks. |
| A4. Co-existence with existing User Plane solution | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1), but with negotiating the use of SRv6 in Enhanced Mode. |
| A5. Interworking with RAN | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A6. Interworking with EPS | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A7. Impacts to GSMA GRX/IPX | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A8. Security | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A9. Minimize number of protocols in network | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A10. Reusability of existing 3GPP implementations | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A11. Protocol Extensibility | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A12. Protocol Overhead | *No UDP (8 octets) and GTP-U (8 to 12 octets) headers.*  Generic Routing Extension header: 4 octets  SRH header: 4 octets + 16 octets per SID + optional objects (if any)  If SRv6 is supported over IPv4: extra IPv6 header (40 octets). |
| A13. Resource-efficiency | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A14. Routing capabilities | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). However, routing differentiation by fundamental IP forwarding mechanism (i.e. longest prefix match) on intermediate routing segments is only possible if 3GPP specific information (TEID, QFI) can be embedded in the intermediate SIDs of the transport network, i.e. if the prefix length of the intermediate SIDs provide enough bits space and the encoding of the 3GPP session and QoS flow information does not collide with the structure of the intermediate SIDs (e.g. Function, Arguments).  In addition, SRv6 in Enhance Mode enables to route packets through intermediate IP routers on the path between two UPFs. |
| A15. Scalability | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A16. Performance | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A17. Programmability | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A18. Signalling Optimisation | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A19. Load Balancing | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |
| A20. Entropy support | Same as for SRv6 in Traditional Mode (see Table 7.2.3-1). |

## 7.3 Comparison

|  |  |  |
| --- | --- | --- |
| Description | GTP-U | SRv6 as a replacement of GTP-U |
| A. Common aspects | 1) UPF functionalities are controlled by the SMF over the N4 interface (PFCP protocol), i.e. SRv6 network programmability (see clause 6.2.1.3) is not used in the 3GPP system;  2) As a result of 1), the UPF shall keep the same states for PFCP associations and PFCP sessions in both solutions;  3) User plane tunnels are established hop by hop between UPFs, i.e. source based routing of SRv6 is not used beyond the possibility for the UPF to force packets to go through intermediate routers between the 2 UPFs using the Network Instance information, in SRv6 Enhanced Mode or with GTP-U over SRv6. | |
| B. Architectural requirements for User Plane | All requirements are supported. | Requirements are supported with following restrictions or comments:  1) the PDU Session User Plane Protocol over N9 as specified in Annex A of 3GPP TS 29.281 [2] and in 3GPP TS 38.415 [10] is not supported;  Editor's Note: a solution to support the above requirement is FFS.  2) security requirements and proposed 3GPP extensions to existing IETF security requirements for use of SRv6 across SR Domain (e.g. inter-PLMN) need to be reviewed and assessed by SA3 (see clause 6.2.2.7). |
| C. IP connectivity for N9 and network slicing | Not supported by the GTP-U protocol itself but supported by existing underlying transport technologies, including GTP-U over SRv6. | SRv6 in Enhanced Mode allows to encode SRH headers to force the data path to go through intermediate SRv6 routers between two UPFs, but the same can be achieved with GTP-U over SRv6. |
| D. System Impacts | No impacts are identified for GTP-U other than those identified for the optional support of UDP zero checksum for GTP-U over IPv6. | Impacts several 3GPP system entities (UPF, SMF, V-SMF, H-SMF, I-SMF, NRF, AMF) and several interfaces (N9, N4, N16, N16a, N38, Nnrf, N27) including roaming interfaces.  Editor's Note: Potential additional impacts to lawful interception need to be assessed by SA3-LI. |
| E. Key additional considerations | GTP-U enables separation between 3GPP user plane and IP-based transport, e.g. when mobile and transport network are different. | 3GPP User Plane and IP transport are collapsed/integrated, with the IP destination address encoding the IP address of the peer UPF, the TEID of the specific user plane tunnel and other 3GPP related information (e.g. QFI, RQI). |
| GTP-U runs over existing transport network technologies and enables segment optimized transport options. | To use the full set of functionalities, the solution relies on IPv6 and, for Enhanced Mode, on SRv6 capable networks. |
| Same solution as used in RAN, EPS and Rel-15 5GC. | Interworking required with GTP-U supported in RAN, EPS and Rel-15 5GC, causing impacts in UPF. |
| The protocol is fully extensible by defining new GTP-U extension headers. | Editor's Note: protocol extensibility of the solution is FFS. |
| Transport remains agnostic of the number of PDU sessions setup in the network (number of 5-tuple flows visible in transport layer is relatively low as PDU sessions are aggregated).  Entropy for load balancing is permitted but not mandated by the GTP-U protocol. | Number of flows visible in transport layer is function of the number of PDU sessions. |
| Protocol overhead: 24 octets (\*)  *(GTP-U header + GTP-U Extension header + UDP header)*  MPLS Label stack header: 4 octets per MPLS label (if SR-MPLS transport is used).  SRv6 overhead: see SRv6 solution (if SRv6 transport is used)  Protocol overhead is not an issue for CN internal interfaces.  (\*) not counting IP header and transport layer headers | Protocol overhead:  - Traditional Mode: none  - Enhanced Mode: 24/40/56 octets for e.g. 1/2/3 SIDs (\*).  *(Generic Routing Extension header + SRH header + 16 octets per SID)*  (not counting IPv6 header and transport layer headers, nor SRH optional objects, if any)  Protocol overhead is not an issue for CN internal interfaces.  (\*) not counting IP header and transport layer headers |

Table 7.3-1: Comparison of solutions

# 8 Conclusion

## 8.1 General

This technical report presents the detailed analysis of the following candidate user plane protocols, based on 5GC architectural requirements, key issues, system impacts and additional considerations:

1) GTP-U protocol over IP-based transport (including SRv6) - see clause 6.1;

2) SRv6 user plane protocol (without GTP-U) - see clause 6.2.2.

Both solutions rely on the same 5GS architecture principles, with UPF functionalities controlled by the SMF over N4 using the PFCP protocol, with the same states in UPF for PFCP associations and PFCP sessions, and with user plane tunnels established hop by hop between UPFs.

## 8.2 GTP-U over IP-based transport (including SRv6)

GTP-U can run over various transports (such as IPv4, IPv6, SR-MPLS or SRv6) and enables to separate the 3GPP user plane from the transport layer as required e.g. when mobile and transport network are different. This protocol has been used over all the user plane interfaces in the 3GPP system since Rel-99 onwards, in the RAN and Core Network, in the 5GS, EPS and earlier generation's mobile networks, including roaming interfaces between VPLMN and HPLMN. It supports all the 3GPP architectural requirements for user plane specified in Rel-16.

Existing transport technologies (e.g. SR-MPLS, SRv6) allow forcing the GTP-U traffic to go through specific intermediate routers between two UPFs by referencing a specific Network Instance, e.g. for network slicing, exactly like the SRv6 user plane protocol (without GTP-U) solution.

GTP-U is fully extensible, by allowing new extension headers to be defined as this has been done in Rel-15 and earlier releases to support several features, e.g. RAN containers, PDU Session Container (5GS information).

TS 29.281 [2] currently refers to IETF RFC 2460 [3] for the IPv6 protocol, which has been obsoleted by IETF RFC 8200 [4]. The analysis in clause 6.1.2 shows that the changes in IPv6 protocol in the latest RFC do not impact the GTP-U protocol, other than the need to negotiate the optional use of UDP zero checksum during the setup of GTP-U tunnel over IPv6 as described in clause 6.1.3.2.

It is recommended to update the GTP-U specification in Rel-16 to:

- update the IPv6 protocol reference to IETF RFC 8200 [4] and to enable the optional use of the UDP zero checksum over IPv6;

- recommend the use of dynamic source UDP port or the Flow Label field to ease load balancing of the traffic in the transport network.

## 8.3 SRv6 user plane protocol (without GTP-U)

The SRv6 user plane protocol (without GTP-U) solution proposes to remove the GTP-U/UDP headers, which saves 24-bytes, by placing 3GPP user plane information (e.g. Tunnel Endpoint Identifier, QoS Flow Identifier, Reflective QoS Indicator, Echo Request/Response, Error Indication, End Marker) within 3GPP specific extensions in the SRH header (e.g. 3GPP specific tags and TLV objects) and in the SID/IP Destination Address.

The solution supports all the 3GPP architectural requirements for user plane specified in Rel-16, except the architectural requirement 8) from clause 5.1.1, where the solution results in splitting the contents of the PDU Session User Plane PDUs into two places of the TLV and the SID in the SRv6 packets and does not allow the PDU session user plane protocol to evolve without impacting the SRv6 user plane packets:

"8) The PDU Session User Plane Protocol (see TS 38.415 [10]) shall be supported to transfer 5GS information over N3 and N9 (e.g. QoS Flow Identifier, Reflective QoS Indicator, Paging Policy Indicator) together with user plane packets."

SRv6 in Traditional Mode does not allow to force the data path to go through intermediate routers between two UPFs, e.g. for network slicing. SRv6 in Enhanced Mode allows to force the data path to go through intermediate routers between two UPFs by referencing a specific Network Instance, e.g. for network slicing, like e.g. GTP-U over SRv6 or GTP-U over SR-MPLS.

CT4 could not reach consensus on the final assessment and conclusion for the SRv6 user plane protocol (without GTP-U) solution. A technical vote took place during CT4#93 (26-30 August 2019) with the following question and results:

Question: Do you want to standardize SRv6 user plane protocol (w/o GTP-U) as described in clause 6.2.2 of TR 29.892?

Results:   
YES: 13.924 %   
NO: 86.076 %  
The quorum was reached.

It was therefore concluded to not standardize the SRv6 user plane protocol (without GTP-U) solution within the scope of this study (i.e. based on stage 2 requirements specified in Rel-16).

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-07 | CT4#85bis | C4-185497 |  |  |  | Initial Draft | 0.1.0 |
| 2018-08 | CT4#86 | C4-186683 |  |  |  | Implementation of C4-186502, C4-186503, C4-186504, C4-186506, C4-186507, C4-186611, C4-186612 and C4-186613 agreed in CT4#86 | 0.2.0 |
| 2018-10 | CT4#86bis | C4-187645 |  |  |  | Implementation of C4-187522, C4-187620, C4-187621, C4-187622, C4-187623, C4-187624 and C4-187625 agreed in CT4#86bis. | 0.3.0 |
| 2018-12 | CT4#87 | C4-188696 |  |  |  | Implementation of C4-188598, C4-188600, C4-188602, C4-188604, C4-188608, C4-188686, C4-188687 and C4-188689 agreed in CT4#87. | 0.4.0 |
| 2019-03 | CT4#89 | C4-190633 |  |  |  | Implementation of C4-190270, C4-190542, C4-190560, C4-190566, C4-190568, C4-190569, C4-190570, C4-190592, C4-190593, C4-190596, C4-190628 and C4-190629 agreed in CT4#89. | 0.5.0 |
| 2019-03 | CT#83 | CP-190060 |  |  |  | Presented for information | 1.0.0 |
| 2019-04 | CT4#90 | C4-191540 |  |  |  | Implementation of C4-191013, C4-191442, C4-191445, C4-191447, C4-191449, C4-191451, C4-191453, C4-191456, C4-191458, C4-191513, C4-191514 and C4-191515 agreed in CT4#90. | 1.1.0 |
| 2019-05 | CT4#91 | C4-192482 |  |  |  | Implementation of C4-192029, C4-192406, C4-192415 and C4-192420 agreed in CT4#91. | 1.2.0 |
| 2019-09 | CT4#93 | C4-193843 |  |  |  | Implementation of C4-193843 agreed in CT4#93. | 1.3.0 |
| 2019-09 | CT#85 | CP-192203 |  |  |  | Presented for approval | 2.0.0 |
| 2019-09 | CT#85 |  |  |  |  | TR was approved in CT#85. | 16.0.0 |