

RTG Working Group
Internet Draft
Intended status: Informational
Expires: October 14, 2022

K. Majumdar
CommScope
U. Chunduri
Intel
L. Dunbar
Futurewei
April 14, 2022

Extension of Transport Aware Mobility in Data Network
draft-mcd-rtgwg-extension-tn-aware-mobility-04

Abstract

The existing Transport Network Aware Mobility for 5G [TN-AWARE-MOBILITY] draft specifies a framework for mapping the 5G mobile systems Slice and Service Types (SSTs) to corresponding underlying network paths in IP and Layer 2 Transport networks. The focus of that work is limited to the mobility domain and transport network characteristics till the UPF and doesn't go beyond the UPF to the Data Network.

To maintain E2E transport network characteristics the framework needs to be extended beyond UPF. This document describes a framework for extending the mobility aware transport network characteristics from the UPF through the Data Network.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 23, 2021.

Copyright Notice

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

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

Table of Contents

1.	Introduction.....	3
2.	Conventions used in this document.....	4
3.	Framework for Extension of Transport Network Aware Mobility....	4
4.	Mobility Packet Transition to the Data Network.....	5
5.	Transport Network Characteristics Mapping to SR-TE Paths.....	7
5.1.	Extend TN Aware Mobility for BGP SR-TE Policy.....	9
5.2.	Extend TN Aware Mobility for SR-PCE Controller.....	13
5.3.	Extend TN Aware Mobility for RestConf/gRPC based SR-TE Controller.....	16
5.4.	Extend BGP FlowSpec for TN Aware Mobility.....	18
6.	Mapping of TN Characteristics on SD-WAN Edge Node.....	21
6.1.	SD-WAN Hybrid Use Case with SR-TE Integration.....	23
7.	IANA Considerations.....	25
8.	Security Considerations.....	25
9.	Contributors.....	25
10.	References.....	25
10.1.	Normative References.....	25

10.2 . Informative References.....	26
11 . Acknowledgments.....	26
Authors' Addresses.....	28

[1](#). Introduction

The [[TN-AWARE-MOBILITY](#)] draft defines the transport path characteristics in backhaul, midhaul, and fronthaul segments between the radio side network functions and user plane functions (UPF). It describes how various transport network underlay routing mechanisms apply to the framework laid out including RSVP-TE, SR, and also a data plane agnostic integrated routing and TE mechanism - Preferred Path Routing (PPR) to map the network slice properties into the IP/L2 transport network.

The current [[TN-AWARE-MOBILITY](#)] draft doesn't extend the transport network characteristics from the UPF through the Data Network. If the user service termination happens in the data network, the Transport Path Network characteristics through the Data Network would be lost.

This proposed Extension of Transport Aware Mobility in Data Network extends the mobility aware transport network characteristics from the UPF through the Data Network.

The UPF can be placed on the edge of the network where it can perform entry or exit point to the Data Network. It can connect to a Provider Edge node as well and bring all the mobile connections in a distributed way to the Data Network.

The UPF can as well connect to the SD-WAN edge node or L3 aggregator device and would try to bring all the 5G mobility connections for small, medium, and large enterprises. This would be a scenario for Enterprise 5G.

The current draft proposes mechanisms on how mobility aware transport network characteristics to be mapped into SR-TE paths or Un-secure, Secure, Secure SR-TE paths based in the Data Network on different use cases scenarios.

[2.](#) Conventions used in this document

BSID	- Binding SID
DC	- Data Center
DN	- Data Network (5G)
EMBB	- enhanced Mobile Broadband (5G)
gNB	- 5G NodeB
GTP-U	- GPRS Tunneling Protocol - Userplane (3GPP)
MIOT	- Massive IOT (5G)
PECP	- Path Computation Element (PCE) Communication Protocol
SD-WAN	- Software-Defined Wide Area Network
SID	- Segment Identifier
SLA	- Service Layer Agreement
SST	- Slice and Service Types (5G)
SR	- Segment Routing
SR-PCE	- SR Path Computation Element
UE	- User Equipment
UPF	- User Plane Function (5G)
URLLC	- Ultra reliable and low latency communications (5G)

[3.](#) Framework for Extension of Transport Network Aware Mobility

Architecture wise, the proposed Extension of Transport Aware Mobility in the Data Network solution focuses on the following areas:

- a) The Mobility packet transition in and out from the UPF to the C-PE Node maintaining the Transport Path Characteristics.
- b) On a PE node, based on the transport characteristics, use different methods of fetching SR-TE path segments from the SR-TE Controller and map the SR-TE segments with the mobility aware transport packets.
- c) On an SD-WAN CE Node, based on the transport characteristics, mapping of mobility aware transport packets to the secure and un-secure tunnel path.

Figure 1 captured under [Section 4](#) provides the representation of a network on how UE could be connected to the UPF and C-PE nodes in the Data Network. The C-PE node represents a combined CE and PE node. In some cases, UPF would be connected to the pure PE or CE node.

[4](#). Mobility Packet Transition to the Data Network

As the Transport Aware Mobility packets transition in and out from the UPF to the PE or C-PE (in SDWAN case) node, the Mobility Transport Characteristics need to be maintained in the Data Network. The current solution proposes a generic approach to how the mobility packet transition can happen in the Data Network maintaining the same transport characteristics.

There are two scenarios could happen here:

A) The UPF is not co-located with the C-PE in the same device. Based on the local policy the proposed new header format for the TN Aware Mobility Packets transitioning from the UPF to the C-PE device and vice-versa is proposed below:

. From the UPF to the C-PE Node:

Inner IP Hdr (UE Packet) + Transport Hdr (Carrying UDP Src Port) + Outer IP (C-PE Node Address)

. From the C-PE to the UPF Node:

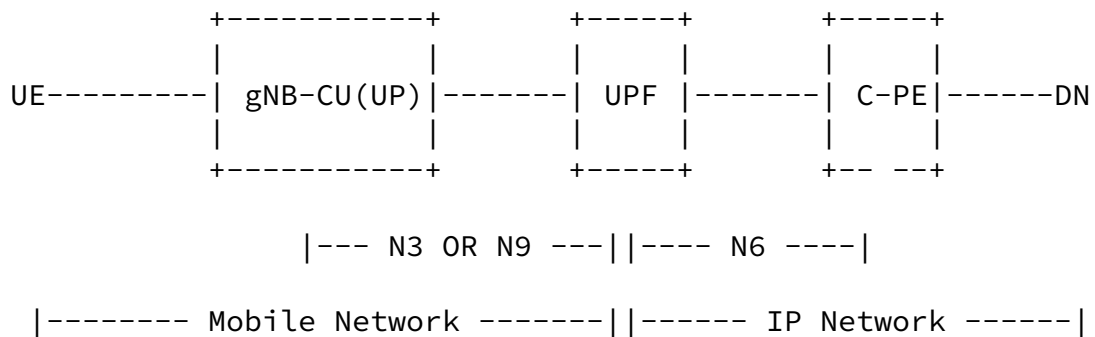
Outer IP (UPF Node Address) + Transport Hdr (Carrying UDP Src Port) + Inner IP Hdr (UE Packet)

B) The UPF is co-located with the C-PE in the same device. Based on the local policy the original UDP Source Port information can be passed to the local C-PE node and no new header is needed here.

The current draft proposes to create a new encapsulation header in scenario A. At the UPF node, the TN aware mobility UE packet carrying the original UDP header Source Port information along with the Inner IP packet to get encapsulated with the outer IP header of the outgoing C-PE node IP address.

In below Figure 1, both scenarios are captured. Scenario A captures the UPF is physically separated from the C-PE node over an IP network. Scenario B captures the edge networking deployment. In that case, the virtual UPF could be co-located with the physical C-PE node in the same device.

Scenario A:



Scenario B:

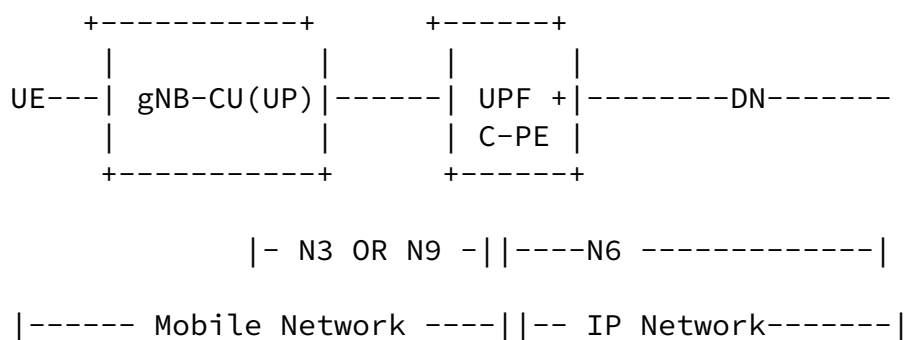


Figure 1: Mobile and IP Data Network for UE

The Figure 2 captures the TN Aware Mobility packet format under the scenario A.

1. UE Packet format in the Mobile Network to the UPF:

```

+-----+-----+-----+-----+-----+
| UE Data | Inner IP | GTP-U | UDP Header | Outer IP |
+-----+-----+-----+-----+-----+

```

2. UE Packet format in the IP Network to the Ingress C-PE Node:

```

+-----+-----+-----+-----+
| UE Data | Inner IP | Transport Header | C-PE Header |
+-----+-----+-----+-----+

```

Figure 2: UE Packet Transition from Mobile to IP Network

The source port in the original UDP header indicates the TN Aware Mobility SST type.

5. Transport Network Characteristics Mapping to SR-TE Paths

With the 5G Mobile Networking, the UPF would be terminating the mobile connection from the UE. In some Edge Networking scenarios, the virtual UPF would be co-located with the C-PE or it would be connected to the C-PE node over IP Network.

The 5G UE traffic coming to the UPF might be carrying Transport Network Characteristics. In that scenario, there would be a need to maintain the Transport Path Characteristic through the core of the network so that end to end SLA can be maintained for the UE traffic.

In scenarios, where ingress PE acting as SR-TE node, the mapping of Transport Network Aware Mobility {5G UDP Src Port Range} to {BGP SR-TE Policy, BSID} to be done at the ingress PE. Once this mapping is done, the mobility Transport Path Characteristics can

be maintained in the data network.

On a PE node, based on the transport characteristics, the current solution proposes different methods of applying SR-TE path segments:

Scenario 1: In this scenario, the assumption is that the Ingress PE node is connected to the BGP SR-TE Controller through the BGP SR-TE Policy SAFI Session. This solution defines a mechanism to

map the BGP SR-TE Underlay Path Segments based on the Mobility Transport Characteristics.

- . This mechanism would require a new BGP Sub-TLV as part of the existing SR Policy SAFI NLRI to download SR-TE Policies corresponds to the mobility Transport Path characteristics. If the TN aware mobility packet UDP Source Port value falls within the UDP Src Port range value of this Sub-TLV, then the pre-downloaded SR-TE Policy MUST be applied on the mobility traffic to map to the correct network slice in the Data Network. Once the Policy is fetched it would be cached by the PE node for operating in line with the subsequent mobility TN aware packets.

Scenario 2: In this scenario, the assumption is that the Ingress PE node is connected to the SR-PCE (Path Compute Element) Controller through the PCEP Session. This draft defines a mechanism to map the SR-TE Underlay Segments based on the Mobility Transport Path Characteristics.

- . Currently, this mechanism does not require new encoding in the PCEP based communication, though it needs local Configuration in the PE node to request the SR-TE Paths from the PCEP based Controller based on on-demand TN aware mobility traffic metric types.

Scenario 3: In this scenario, the assumption is that the Ingress PE node is connected to the SR-TE Controller over Restconf/ Netconf or gRPC session. The existing mechanism would be used to download the SR-TE Underlay Path Segments to the PE node based on the Mobility Transport Path Characteristics.

- . The Yang Data Model or Protobuf definition is required to

define a new Sub-TLV like Scenario 1. The SR-TE Controller would pre-download the SR-TE Policies with the new Sub-TLV in the Ingress PE using the existing session. Once the specific SR-TE Policy is fetched, it would be cached by the Ingress PE to apply for the mobility TN aware traffic in-line to maintain the network characteristics in the Data Network.

Scenario 4: In this scenario, the assumption is that the Ingress PE node is connected to the BGP SR FlowSpec Controller through the BGP FlowSpec Session. This draft defines a mechanism to map the

FlowSpec redirect to indirection-id community-based SR Traffic rules to the Mobility Transport Path Characteristics.

- . Currently, this mechanism does not require any new encoding in the BGP SR FlowSpec path redirect draft [FLOWSPEC-PATH-REDIRECT], though it needs local Configuration in the Ingress PE node that is acting as BGP FlowSpec Client to map the Mobility traffic based on the SR FlowSpec traffic re-direction rules.

[5.1](#). Extend TN Aware Mobility for BGP SR-TE Policy

- 1) To integrate Transport Network Aware Mobility with BGP SR-TE Policy at the Ingress PE UPF, the Class-map needs to be defined to classify the incoming mobility traffic with different Transport Path Characteristic.
- 2) The Ingress PE UPF is assumed to have a BGP SR-TE Policy SAFI connection with the BGP SR-TE Controller. The Mobility traffic destination would resolve in the BGP Peer Next Hop for which SR-TE Policy to be applied to maintain the same network characteristics beyond the mobility domain.
- 3) A new 5G Metadata Sub-TLV has been defined for existing SR-Policy SAFI with the UDP Source Port Range to identify the SR-TE path based on the Transport Path characteristics.
- 4) The BGP SR-TE Controller would be programmed with {5G UDP Src Port Range}. That would create internal mapping Table for {5G UDP Src Port Range} < -- > {BGP SR-TE Policy, BSID}.

- 5) The BGP SR-TE Controller would download the SR-TE Policy in the Ingress PE through the existing BGP SR-Policy SAFI session, and that the BGP update would include an additional 5G Metadata Sub-TLV. The UDP Src Port range in the 5G Metadata Sub-TLV MUST fall within the UDP Source Port range for the SSTs defined by the [TN-AWARE-MOBILITY] draft. If the UDP Src Port range falls outside the range defined by the [TN-AWARE-MOBILITY] draft, then the SR-TE Policy SHOULD be ignored by the Ingress PE.
- 6) The SR-TE Policy-based traffic steering would be applied in the Ingress PE and it would maintain the local mapping for the reverse Mobility traffic to the UE.

The following class-map definition needs to be applied in the headend PE for the incoming Transport Network aware mobility traffic path:

Class-map type traffic match MIOT

Match UDP Src Port Range Xx - Xy

Class-map type traffic match URLLC

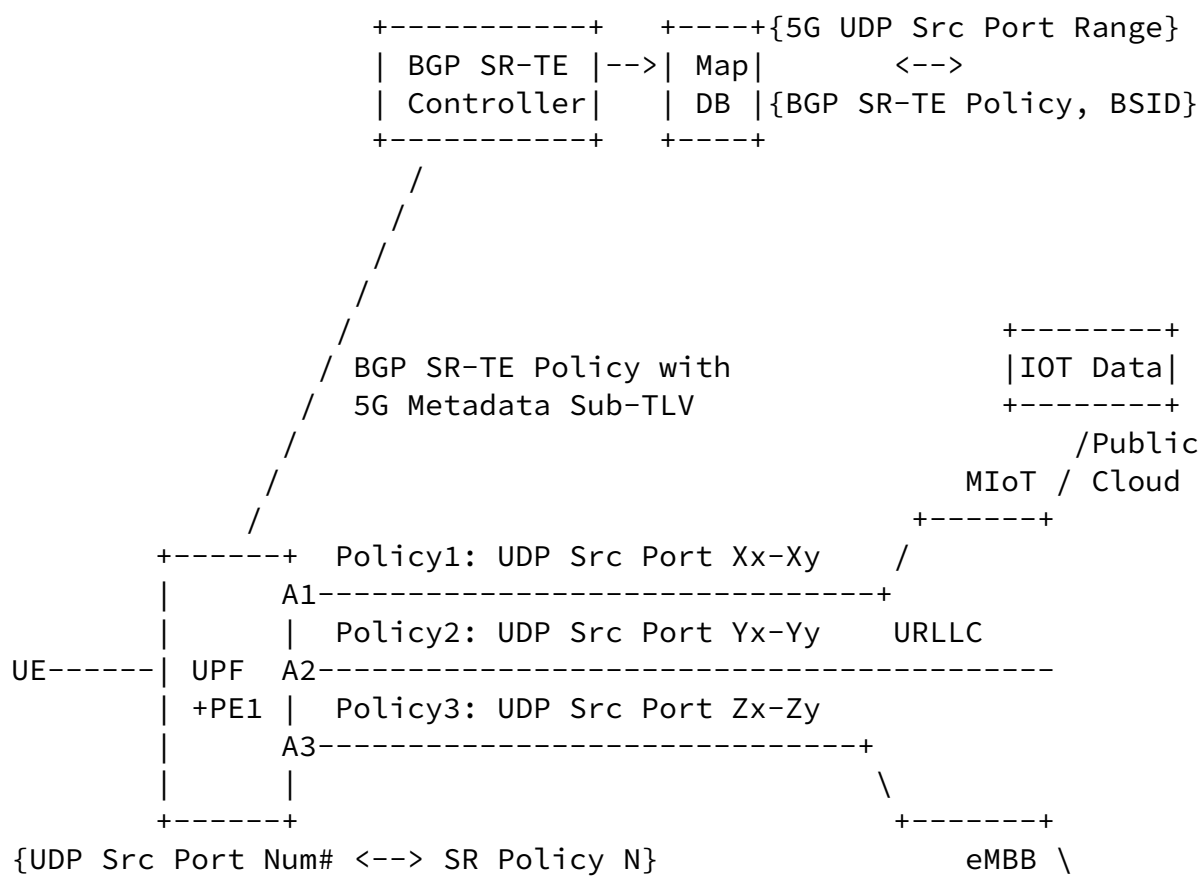
Match UDP Src Port Range Yx - Yy

Class-map type traffic match EMBB

Match UDP Src Port Range Zx - Zy

The class-map would help to identify the incoming mobility traffic characteristics. Based on these characteristics the headend PE would be able to map the Transport Network aware mobility traffic to the appropriate BGP SR-TE Policy path over the Data Network to reach the UE's destination.

The below figure tries to capture the overall topology, and how to map the mobility traffic in the Ingress PE having BGP SR-Policy SAFI connection with the BGP SR-TE Controller:



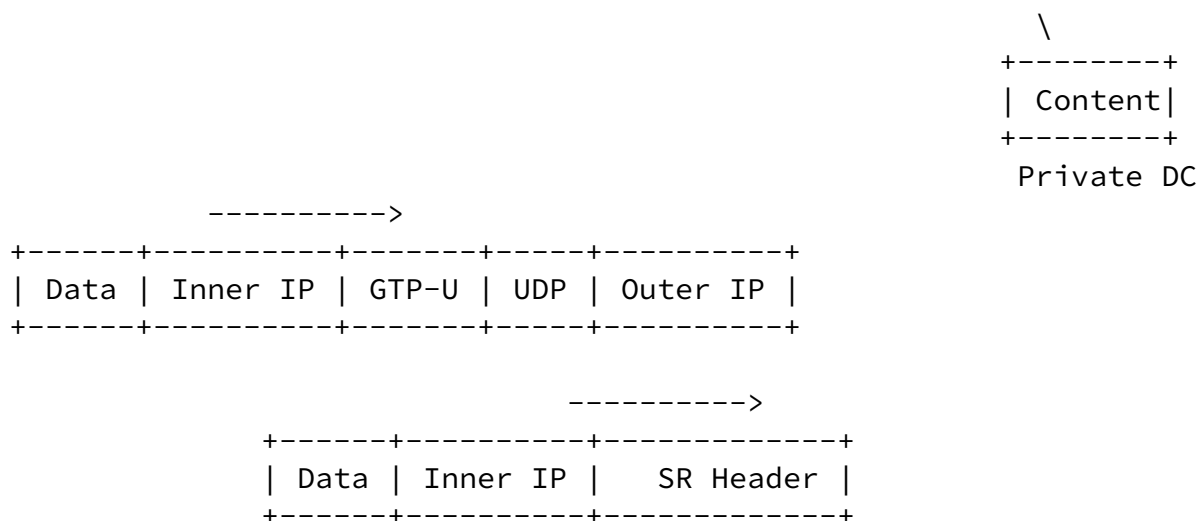


Figure 3: TN Aware Mobility Traffic Mapping to BGP SR-TE Policy Path

Note that, in the above figure SR Header is shown as an illustrative purpose and the actual outgoing packet format is based on the BGP SR-TE mechanism (SR-MPLS or SRv6) on the Ingress PE. That could be SR-MPLS or SRv6 Header. Though if the BSID is not present with the BGP SR-TE Policy, the local Ingress PE would map the incoming traffic to the best effort policy map path in the underlay.

To support the Transport Network Mobility Traffic Mapping to BGP SR-TE Policy Path in the headend PE, a new 5G Metadata Sub-TLV needs to be supported. The proposed BGP SR Policy Encoding from the BGP SR-TE Policy Controller to the headend PE node is defined below:

SR Policy SAFI NLRI: <Distinguisher, Policy-Color, Endpoint>

Attributes:

Tunnel Encap Attr (23)

Tunnel Type: SR Policy

Existing Policy Sub-TLV

5G Metadata Sub-TLV

The draft [[BGP-SR-TE-POLICY](#)] defines BGP SR-TE Policy encodings. There is no change in the existing encoding that is being used from the BGP SR-TE Controller to the headend PE node. The current

solution proposes the new 5G Metadata Sub-TLV for BGP SR-TE Controller to download the SR Policies to the headend PE and to apply the SR-TE Policy-driven path for the Transport Network aware mobility traffic.

The incoming TN aware mobility traffic with UDP Src port and BGP NH to the traffic destination would be used as a key to find the BGP SR-TE Policy. If the BGP Next Hop of the traffic matches with the SR Policy SAFI NLRI Endpoint, and UDP Src Port value falls within the UDP Src Port range defined by the 5G Metadata Sub-TLV, the SR Policy would be applied to the mobility traffic to maintain the traffic characteristics in the data network. The BGP SR-TE Controller would be pre-provisioned with the 5G UDP SRC Port Range based on the [TN-AWARE-MOBILITY] draft, and their corresponding BGP SR-TE Policy.

The 5G Metadata sub-TLV is optional and it MUST NOT appear more than once in the SR-TE Policy.

The format of the new SR-TE 5G Metadata Sub-TLV is captured below:

Majumdar, et al. Expires October 15, 2022 [Page 12]

Internet-Draft Extension of TN Aware Mobility April 2022

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Sub-Type      |      Length      |      Flags      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      UDP Src Port Start Value      |      UDP Src Port End Value      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
                                5G Metadata Sub-TLV

```

where:

- o Type: To be defined by IANA.
- o Sub-Type: This field has one of the following values:
 - 0: Reserved.
 - 1: UDP Source Port Range.
 - 2 - 255: Reserved for future use.
- o Length: 6 octets.
- o Flags: 1 octet of flags. None are defined at this stage. Flags SHOULD be set to zero on transmission and MUST be ignored on receipt.
- o UDP Src Port Start Value: 2 octets value to define the starting of the value of the UDP Src Port range.
- o UDP Src Port End Value: 2 octets value to define the end value of the UDP Src Port range.

[5.2.](#) Extend TN Aware Mobility for SR-PCE Controller

- 1) To integrate Transport Network Aware Mobility with SR-TE ODN based PCE Controller at the Ingress PE UPF, the Class-map needs to be defined to classify the incoming mobility traffic with different Transport Path Characteristic.
- 2) The Ingress PE UPF is assumed to have PCEP based communication with the SR-PCE Controller.

- 3) The Ingress PE would define the Policy-map to map the Transport Path characteristics into SR-TE Color.
- 4) The Segment Routing TE Configuration for different Metric types will associate the SR-TE Colors with their corresponding TE metric type.
- 5) The existing SR-TE ODN based PCEP messages with TE metric type and value MUST be used to associate the SR-TE Path corresponding to the 5G UDP Src Port.

- 6) In this case, the mapping between {5G UDP Src Port} and {SR-TE Policy} would be maintained by the Ingress PE.
- 7) Once the TN aware mobility traffic destination resolves into a destination of BGP Peer Next Hop, the SR-TE ODN based traffic steering MUST be applied based on the UDP Src Port value of the incoming traffic.

The class-map definition to identify the incoming mobility traffic characteristics is already defined in [Section 5.1](#). The same class-map definition applicable here as well.

The policy-map definition to associate SR-TE color with Transport Path characteristics is defined below:

Policy-map type Transport-Network-Aware-Mobility

Class type traffic MIOT

Set color <MIOT-10>

Class type traffic URLLC

Set color <URLLC-20>

Class type traffic EMBB

Set color <EMBB-30>

The Segment Routing TE Configuration mechanism can associate the SR-TE Colors with their corresponding metric type. That exists today, and there is no change there. It is captured here to show how TN

aware mobility network characteristics get mapped to different TE metrics through this mechanism.

Segment-routing traffic-eng

On-demand color <MIOT-10> dynamic

Metric

Type <MIOT>

On-demand color <URLLC-20> dynamic

Metric

Type <URLLC>

On-demand color <EMBB-30> dynamic

Metric

Type <EMBB>

As a result, mobility Transport Network aware of different traffic characteristics like MIOT, URLLC, or EMBB get to assigned corresponding "te" metric types. To fetch the corresponding SR-TE dynamic path from the SR-PCE Controller based on the newly defined "te" metric types <MIOT>, <URLLC> or <EMBB> needs to be extended in the PCEP RFC [[RFC5440](#)].

The below figure tries to capture the overall topology, and how to map the mobility traffic in the headend PE having PCEP connection with the SR-PCE Controller:

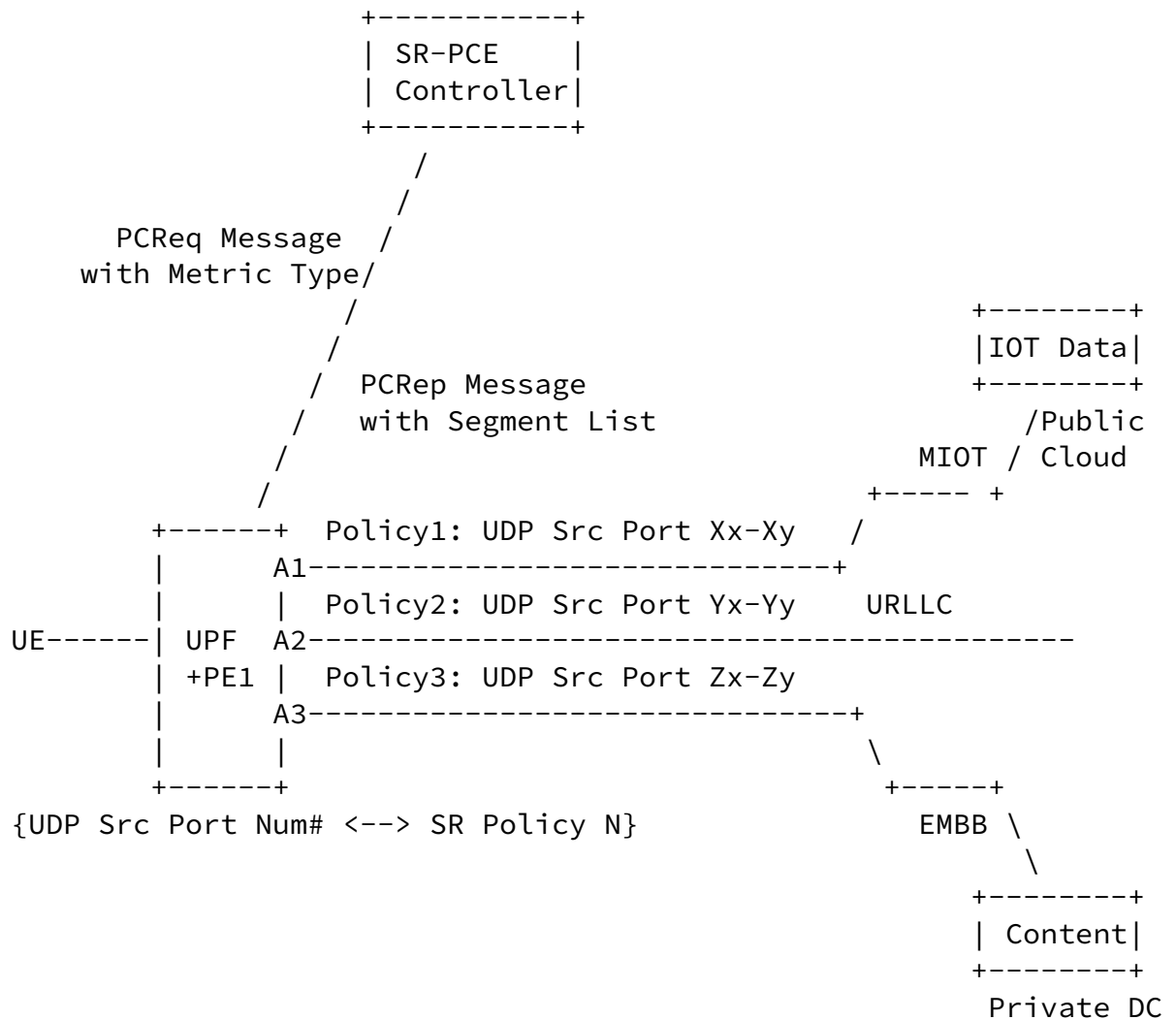


Figure 4: TN Aware Mobility Traffic Mapping to SR-TE Path

5.3. Extend TN Aware Mobility for RestConf/gRPC based SR-TE Controller

- 1) To integrate Transport Network Aware Mobility with SR-TE Policy at the Ingress PE UPF, the Class-map needs to be defined to classify the incoming mobility traffic with different Transport Path Characteristic.
- 2) The Ingress PE UPF is assumed to have Restconf or gRPC connection with the SR-TE Controller. The Mobility traffic destination would resolve in the BGP Peer Next Hop for which SR-TE Policy to be applied to maintain the same network characteristics beyond the mobility domain.

- 3) A new 5G Metadata Yang data model and Protobuf to be defined for SR-Policy SAFI with UDP Source Port Range to identify the SR-TE path based on the Transport Path characteristics.
- 4) The SR-TE Controller would be programmed with {5G UDP Src Port Range}. That would create internal mapping Table for {5G UDP Src Port Range} < -- > {BGP SR-TE Policy, BSID}.
- 5) As the Headend PE sends the 5G metadata Yang data model or Protobuf, the Controller will find a matching SR-TE Policy based on the UDP Source Port.
- 6) The SR-TE Controller would download the SR-TE Policy in the Ingress PE through the existing Restconf or gRPC session, and that BGP update would include an additional 5G Metadata Sub-TLV. The UDP Src Port range in the 5G Metadata Sub-TLV MUST fall within the UDP Source Port range for the SSTs defined by the [TN-AWARE-MOBILITY] draft. If the UDP Src Port range falls outside the range defined by the [[TN-AWARE-MOBILITY](#)] draft, then the SR-TE Policy SHOULD be ignored by the Ingress PE.
- 7) The SR-TE Policy-based traffic steering would be applied in the Ingress PE UPF and it would maintain the local mapping for the reverse Mobility traffic to the UE.

The class-map definition to identify the incoming mobility traffic characteristics is already defined in [Section 5.1](#). The same class-map definition works here as well.

The below figure tries to capture the overall topology, and how to map the mobility traffic in the headend PE having BGP SR-Policy SAFI connection with the BGP SR-PCE Controller:

Internet-Draft

Extension of TN Aware Mobility

April 2022

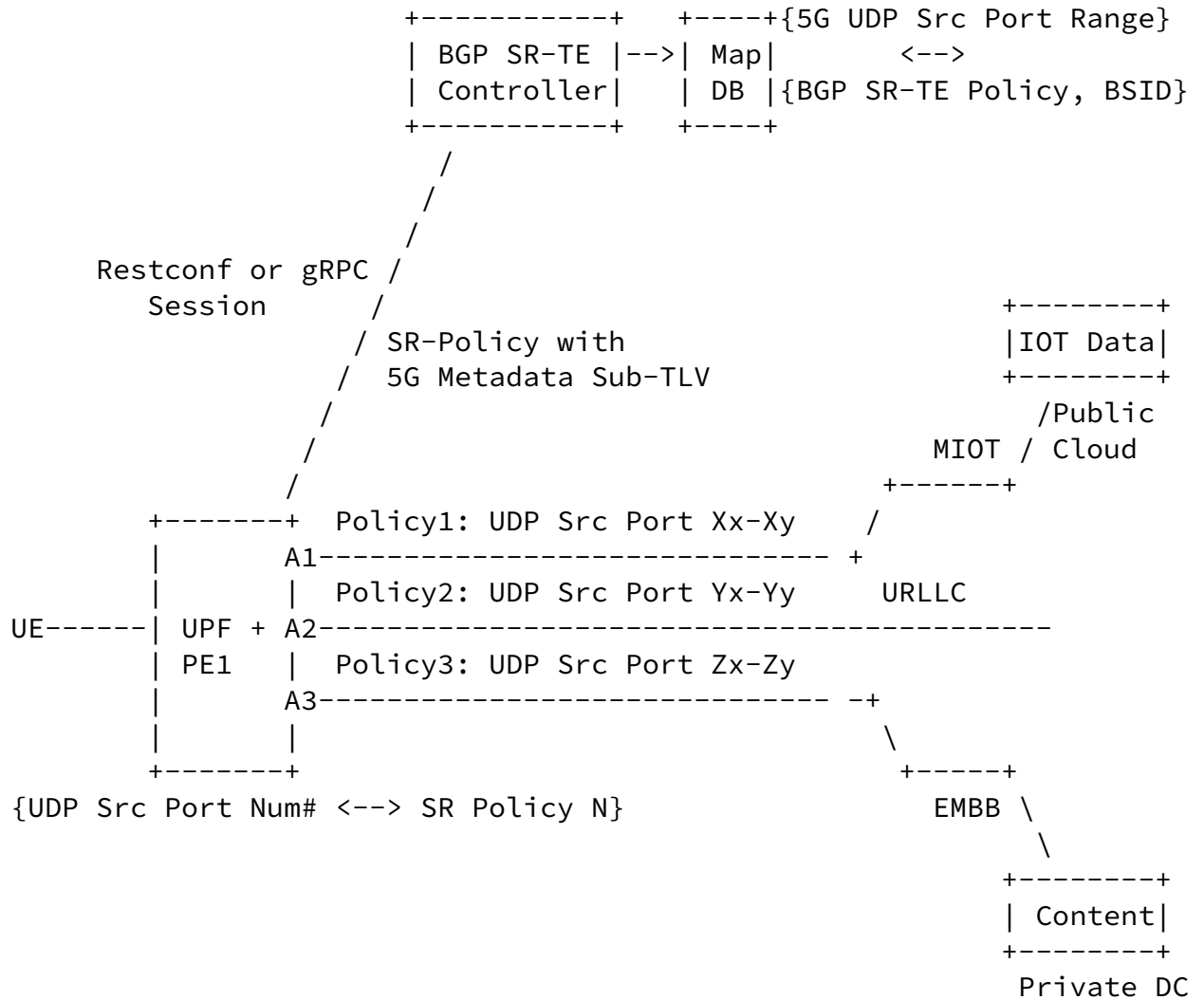


Figure 5: TN Aware Mobility Traffic Mapping to SR-TE Path

5.4. Extend BGP FlowSpec for TN Aware Mobility

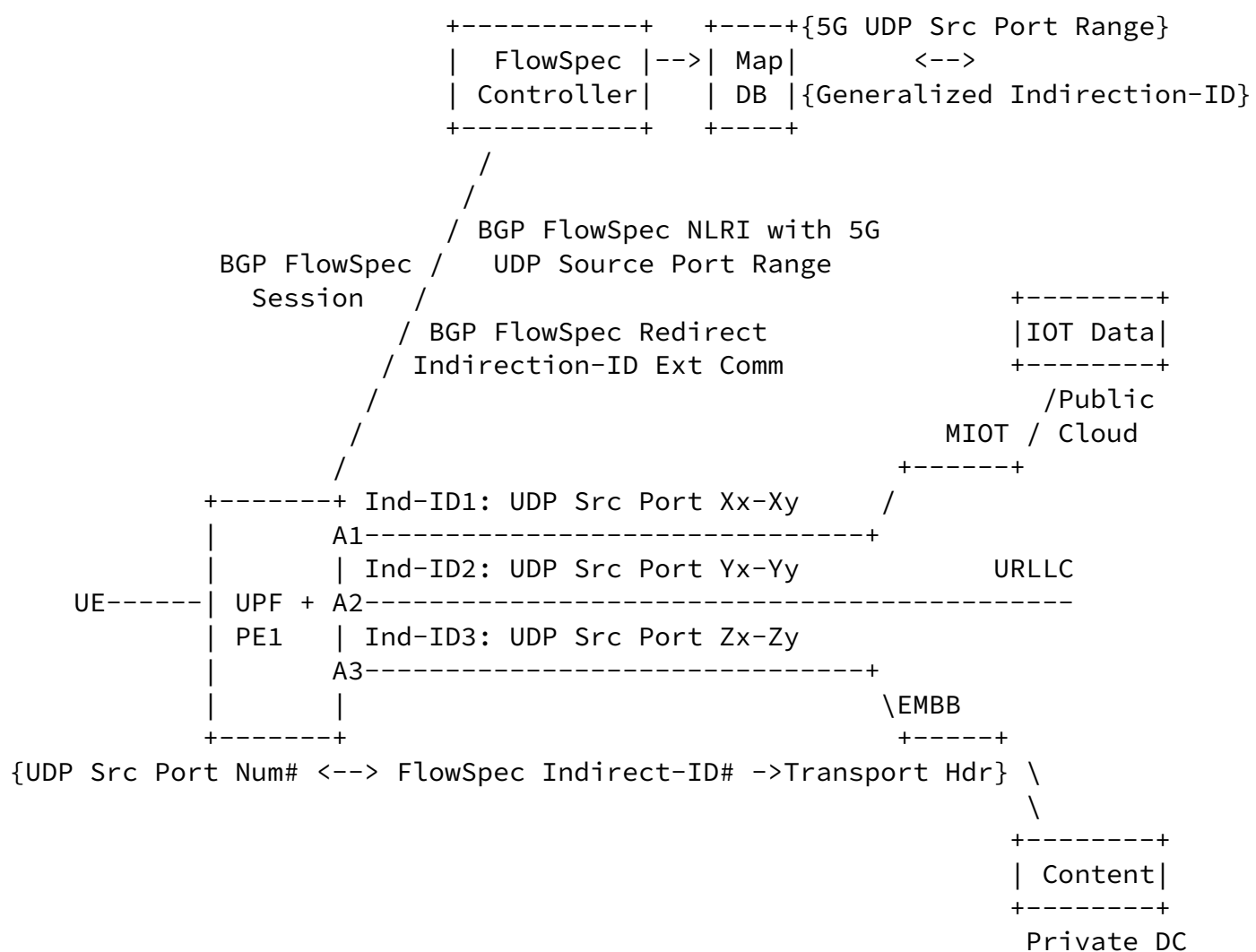
- 1) To integrate Transport Network Aware Mobility with SR-TE Policy at the Ingress PE UPF, the Class-map needs to be defined to classify the incoming mobility traffic with different Transport Path Characteristic.

- 2) The Ingress PE UPF that is acting as BGP FlowSpec Client is assumed to have a BGP FlowSpec session with the FlowSpec Controller. The Mobility traffic destination would resolve in the BGP Peer Next Hop for which SR FlowSpec traffic re-direct policy to be applied to maintain the same network characteristics in the data network.

- 3) The current proposal tries to integrate FlowSpec Redirect to Indirection ID [FLOWSPEC-PATH-REDIRECT] based traffic rules with the TN aware mobility traffic based on the UDP Source Port range at the FlowSpec Client Router/Ingress PE.
- 4) Based on the BGP FlowSpec [RFC 8955](#) the BGP FlowSpec NLRI can carry out the UDP Source Port range. The 5G SST specific UDP Source Port range values can be pushed over a BGP FlowSpec session between the FlowSpec Controller and the Ingress PE node.
- 5) There are no additional changes required on the BGP FlowSpec side other than provisioning 5G SST specific UDP Source Port range at the FlowSpec Controller along with the corresponding FlowSpec Redirect to indirection-id.
- 6) The BGP FlowSpec Controller would be programmed with {5G UDP Src Port Range} to map different SSTs defined in [[TN-AWARE-MOBILITY](#)] draft to map the corresponding FlowSpec Redirect to Indirection-id. That would create internal mapping Table for {5G UDP Src Port Range} < -- > {BGP FlowSpec Generalized Indirection-ID}.
- 7) The BGP FlowSpec NLRI carrying 5G UDP Source Port Range along with the corresponding Redirect to indirection-id Extended Community can be pushed to the Ingress PE node.
- 8) The Mobility traffic coming from the UPF to the Ingress PE in the Data Network carrying specific UDP Source Port from UE can be classified based on the local Policy and apply the BGP FlowSpec based re-direction rule based on the matching FlowSpec policy.

The class-map definition to identify the incoming mobility traffic characteristics is already defined in [Section 5.1](#). The same class-map definition works here as well.

The below figure tries to capture the overall topology, and how to map the mobility traffic in the Ingress PE acting as FlowSpec Client having BGP FlowSpec SAFI connection with the BGP FlowSpec Controller:



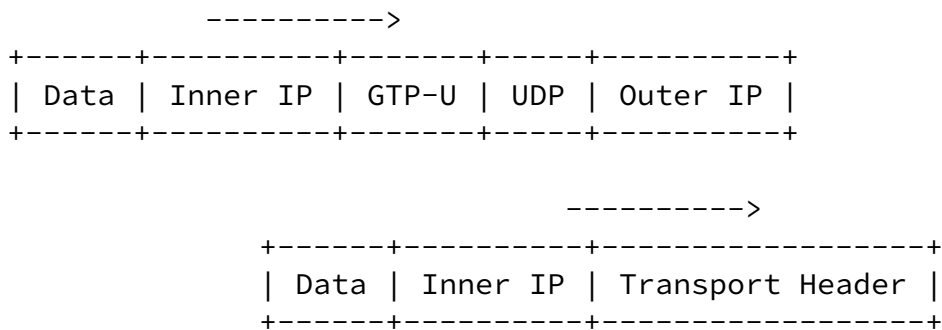


Figure 6: TN Aware Mobility Traffic Mapping to FS Redirect Path

6. Mapping of TN Characteristics on SD-WAN Edge Node

On an SD-WAN CE Node, based on the mobility Transport Network characteristics, mapping of mobility aware transport packets to the secure and un-secure tunnel path needs to be achieved.

The [[BGP-IPSEC-Discover](#)] draft defines how SD-WAN Edge Node maps the overlay/client routes to the underlay secure tunnel routes.

The current proposal specifies a generic approach on how SD-WAN Edge Node maps the Mobility Transport Network aware traffic to the Secure Tunnels, or Un-Secure TE Paths, or Secure SR-TE Tunnel Paths.

The [[SDWAN-BGP-USAGE](#)] draft describes how BGP can be used as a Control Plane for the SD-WAN network and defines the use case for the Hybrid SD-WAN network.

In the case of a hybrid SD-WAN use case, UPF can run part of the SD-WAN edge node or it could be connected to it over an IP network. This would be a use case scenario for Enterprise 5G.

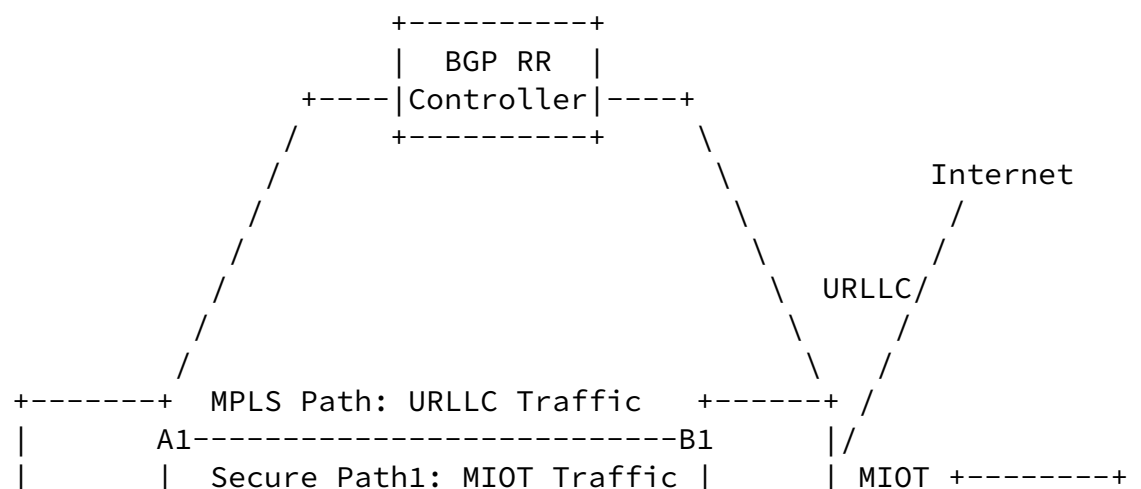
In that scenario, the Transport Path Characteristic for the 5G

mobile traffic need to be mapped to Secure (IPSec Tunnel) or Un-secure path (could be MPLS based).

The existing [\[TN-AWARE-MOBILITY\]](#) draft is extended to support new Transport Path Characteristics "Security" for the mobile traffic where security is important for certain mobile traffic.

Based on the UDP Src Port characteristics coming from the mobile network, the SD-WAN edge node would be able to decide what traffic it needs to put in the secure tunnel vs. an un-secure tunnel where low latency more important than security.

The below figure tries to capture the overall topology, and how to map the mobility traffic in the SD-WAN Edge Device for Enterprise 5G cases:



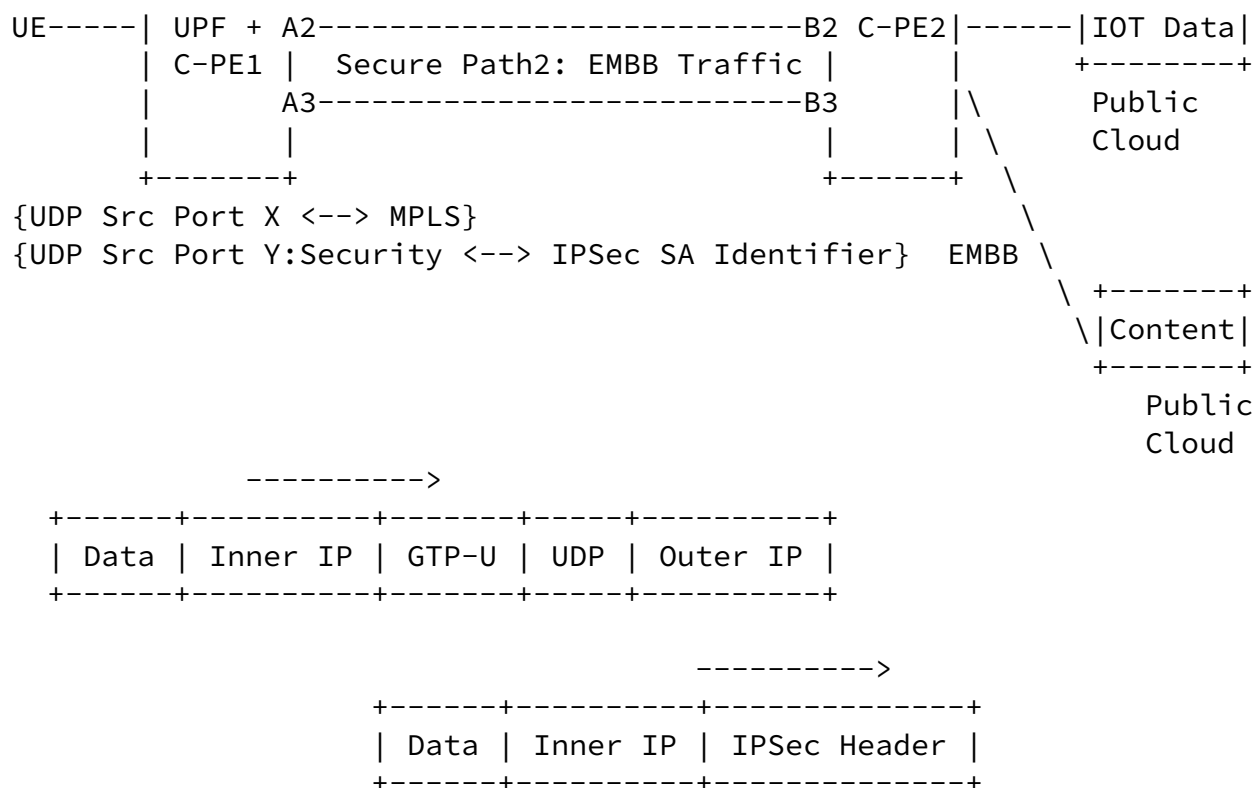


Figure 7: Secure TN Aware Mobility Traffic Mapping in the SD-WAN Edge Device

Here in this diagram, the traffic coming from the mobility side with Transport Network characteristics gets mapped to the underlay un-secure or secure traffic path.

The SD-WAN Edge Node can map the URLLC traffic without any security characteristics to the underlay MPLS path, whereas MIOT, and EMBB traffic with security characteristics gets mapped to the underlay Secure IPsec Tunnel path. The mapping between SD-WAN overlay and underlay routes are described in the [BGP-IPSEC-Discovery] draft.

This solution extends it for Transport Network aware mobility traffic. The SD-WAN Edge Node here identifies the incoming mobility traffic characteristics using the class-map definition, and that is already defined under [Section 5.1](#). Based on the incoming traffic characteristics, the Edge Node will be able to map the mobility overlay traffic to the respective SD-WAN underlay tunnel.

6.1. SD-WAN Hybrid Use Case with SR-TE Integration

- 1) In the case of SD-WAN hybrid use cases, UPF can run part of the SD-WAN edge node, or it could be connected to it over an IP network. This would be a use case scenario for Enterprise 5G.
- 2) The SD-WAN edge node can act as an SR-TE Headend PE in some use case scenarios that are described in [[SDWAN-BGP-USAGE](#)] draft.
- 3) In that case, the Headend PE could be connected with SR-TE Policy Controller over the BGP SR-Policy SAFI session, or SR-PCE Controller over the PCEP session, or SR-TE Controller over Netconf/ Restconf, or GRPC session, or even SR FlowSpec Controller over BGP FlowSpec session.
- 4) The SD-WAN edge node can map the "Un-secure" mobility traffic to the SR-TE path the same way as described under PE acting as ingress SR-TE headend.
- 5) Though the mapping for "Secure" mobility traffic to the SR-TE path would be slightly different than "Un-secure" mobility traffic.
- 6) The mobility 5G UE client traffic with the Transport Path Characteristics "Security" would be encapsulated with Tunnel mode IPSec header between the two SD-WAN SAFI underlay endpoints (belong to the same BGP AS domain). This encapsulated secure traffic will become the new overlay for the SR-TE traffic.
- 7) The rest of the mechanism for the secure mobility traffic with SR-TE traffic forwarding is the same as un-secure SR-TE based traffic forwarding.

The below figure tries to capture the overall topology, and how to map the mobility traffic in the SD-WAN Edge Device for SD-WAN Hybrid Use Cases described above:

```
+-----+
| BGP SR-Based|
| Controller  |
```

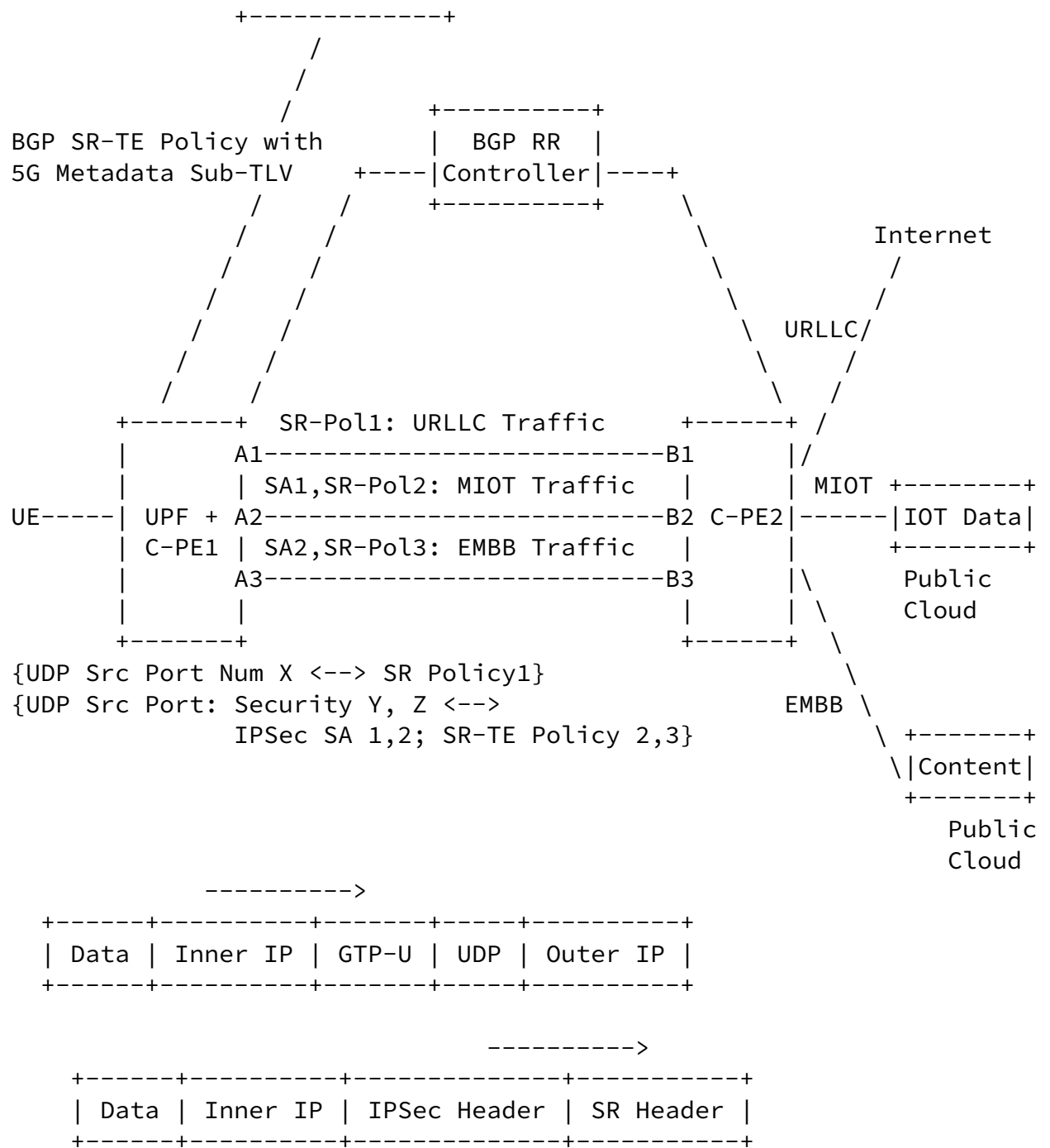


Figure 8: Secure TN Aware Mobility Traffic Mapping for Hybrid SD-WAN Use Cas

In Figure 8, the traffic coming from the mobility side with Transport Network characteristics gets mapped to the underlay un-secure or secure SR-TE path to maintain the traffic network characteristics in the Data Network.

The SD-WAN Edge Node can map the URLLC traffic without any security characteristics to the underlay SR-TE path without any IPSec encapsulation. Whereas MIOT and EMBB traffic with the security characteristics can be mapped to the underlay Secure IPSec Tunnel path with the SR-TE encapsulation to the SD-WAN endpoints.

[7.](#) IANA Considerations

The newly defined 5G Metadata Sub-TLV would need an IANA code point allocation for the Type field. A request for any IANA code point allocation would be submitted.

[8.](#) Security Considerations

This document does not introduce any new security issues.

[9.](#) Contributors

The following people have contributed to this document.

Dhruv Dhody
Huawei Technologies

Email: dhruv.ietf@gmail.com

[10.](#) References

[10.1.](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

10.2. Informative References

[RFC5440] JP. Vasseur, Ed., JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", March 2009

[TN-AWARE-MOBILITY] U. Chunduri, et al, "Transport Network aware Mobility for 5G", [draft-ietf-dmm-tn-aware-mobility-03](#), March 2022

[BGP-SR-TE-POLICY] S. Previdi, et al, "Advertising Segment Routing Policies in BGP", [draft-ietf-idr-segment-routing-te-policy-16](#), March 2022

[SDWAN-BGP-USAGE] L. Dunber, et al, "BGP Usage for SDWAN Overlay Networks", [draft-ietf-bess-bgp-sdwan-usage-04](#), October 2021

[BGP-IPSEC-Discover] L. Dunber, et al, "BGP UPDATE for SDWAN Edge Discovery", [draft-ietf-idr-sdwan-edge-discovery-01](#), March 2022

[RFC9012] K. Patel, et al, "The BGP Tunnel Encapsulation Attribute", April 2021.

11. Acknowledgments

TBD.

This document was prepared using 2-Word-v2.0.template.dot.

Internet-Draft

Extension of TN Aware Mobility

April 2022

Authors' Addresses

Kausik Majumdar
CommScope

Email: kausik.majumdar@commscope.com

Uma Chunduri
Intel Corporation

Email: umac.ietf@gmail.com

Linda Dunbar
Futurewei

Email: linda.dunbar@futurewei.com

