broadband forum

Technical Report

TR-521
5G Transport Networks

Issue: 1
Issue Date: June 2022

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. This Technical Report is owned and copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be owned and/or copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License
Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES
THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT AND ANY IMPLIED WARRANTIES ARE EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE USER'S OR IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY USER, IMPLEMENTER, OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS TECHNICAL REPORT, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, AND INDIRECT DAMAGES.

3. THIRD PARTY RIGHTS
Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE TECHNICAL REPORT, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

All copies of this Technical Report (or any portion hereof) must include the notices, legends, and other provisions set forth on this page.

Issue History

Issue Number	Issue Date	Issue Editor	Changes
1	30 June 2022	Ron Insler, RAD Data Communication	Original

Comments or questions about this Broadband Forum Technical Report should be directed to info@broadband-forum.org.

Editor:
Ron Insler, RAD

Access and Transport Architecture (ATA) Work Area Director(s):
David Sinicrope, Ericsson

Mobile Transport and Routing Project Stream Leader(s):
David Sinicrope, Ericsson

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This document provides a functional reference architecture, design, and protocol requirements for Transport networks supporting 5G cellular fronthaul and backhaul. It is intended to be used by operators in specifying what is expected of the equipment they procure and some guidance on deployment to support 5G. It is intended to be used by vendors in deciding what to implement and support and how it will be used.

1 Purpose

In the context of transport networks, the purpose of this Technical Report is:

- To provide technical architecture and equipment (HW and SW components) requirements for 5G transport.
- To define end-to-end reference architectures for transport solutions and services addressing control, user and management traffic in support of 5G mobile networks. The different 5G RAN functional splits and network slicing mechanisms for various 5G use cases need to be addressed.
- To assess the suitability of multiple transport technologies for various 5G use cases.
- To define the role in the 5G transport architecture considering SDN and automation as well as virtualization and edge cloud.
- To address stand alone (a sole 5G mobile network) and non-stand alone (5G-enabled smartphones will connect to 5G frequencies for data-throughput improvements but will still use 4G for non-data duties such as talking to the cell towers and servers) RAN deployment scenarios for migration and dual connectivity cases.
- To provide specifications for various 5G transport scenarios that are depicted in this reference architecture.
- To target deployment of energy saving technologies.
- To define 5G transport considering DetNet/TSN.
- To promote multi-vendor interoperability for 5G RAN transport SW and HW components, in coordination with 3GPP, and IEEE, and other standardization activities, and to create a basis for evaluation for compliance assessment.

2 Scope

The target is to define functional and architecture requirements for a suite of transport nodes for 5G transport, to address various functional splits of the 5G RAN, as defined in 3GPP TR38.801[10], as well as User Plane – Control Plane split options. Specifically, Cell-site Gateway and Aggregator devices would be deployed for higher layer splits (e.g., options 1 and 2), while dedicated fronthaul nodes are engineered for low layer splits (Out of scope for this document). In addition the target is to define network slicing management plane, control plane and data plane architecture and nodal requirements.

For each transport node (e.g., CSG,MASG), the following requirements should be included in the scope:

- Transport service (TNL) technology, for example, Ethernet, IP,802.1CMde [53] etc.
- Synchronization requirements (see below).
- Underlay network technology (IP, Ethernet, MPLS) with regards to encapsulation, signaling and routing, QoS, OAM mechanisms, resiliency, and security.
- Slicing mechanisms for different types of applications and services for different QoE and enabling end-to-end slicing traffic engineering.
- Transport mechanisms to support network slicing with a transport network and their relevant requirements.

Synchronization architecture and out of band distribution is out of scope.

The scope should cover co-location of 5G with 2/3/4G networks aligned with TR-221 [1],TR-224 [82], TR-350 Issue 2 [5] and consider multiple RAN interfaces: along with 5G's N2, N3 U and C, Xn U and C interfaces, F1, C and U interfaces as well as legacy RAN interfaces (e.g., Abis for GSM, Iub for UMTS, A15, A8, A9 for CDMA, S1/X2 for LTE) from the point of view of TDM, ATM, Ethernet and IP services. RAN interfaces over TDM and ATM are covered in TR-221 [1] and are not covered in this document.

The following Transport Network Layers are within scope of BBF 5G transport:

- IP TNL (e.g., for 3G R5 and beyond, and LTE R8 and beyond)
- Ethernet TNL (e.g., as defined in 802.1Q [8] and 802.1CMde [53]).

The following requirements should be defined:

- Requirements for supporting clock distribution to the base stations, including frequency and Time/phase synchronization.
- Resiliency requirements taking into account failover times appropriate for mobile backhaul networks.
- OAM requirements and capabilities for each transport network.
- RAN equipment with a range of physical interfaces (e.g., Gigabit Ethernet, 10G, 25G and 100G Ethernet etc.), connected through intervening access and aggregation networks.
- Support for Time Sensitive Networking (IEEE 802.1CM for Ethernet fronthaul, IETF DetNet),).
- Support for Segment Routing, EVPN.

The project approaches the 5G transport architecture from the point of view of the transport network. Mobile traffic is considered as application (overlay) data of the respective TNL and is transparent to the transport network.

Different service types E-line, E-Tree, E-LAN are in scope for each transport network type.

Notwithstanding the references used in prior (source) BBF Technical Reports used in the document, this document relies on reference to the backward compatible subset of more recently published versions of revised MEF specifications (including MEF 6.2, MEF 10.3, MEF 22.3 & MEF 22.3.1, and MEF 23.2) to

achieve 5G Transport function. One of the things this accomplishes is to make this document compatible with more recently published versions of TR-221 [1], TR-224 [82], and TR-350 [5].

3 References and Terminology

3.1 Conventions

In this Working Text, several words are used to signify the requirements of the specification and RFC 8174 [98]. These words are always capitalized. More information can be found be in RFC 2119 [97].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC 2119] [97] [RFC 8174] [98] when, and only when, they appear in all capitals, as shown here.

3.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document	Title	Source	Year
[1] TR-221	Technical Specifications for MPLS in Mobile Backhaul Networks	BBF	2011
[2] TR-221 Amendment 2	Technical Specifications for MPLS in Mobile Backhaul Networks	BBF	2017
[3] TR-221 Corrigendum 1	Technical Specifications for MPLS in Mobile Backhaul Networks	BBF	2014
[4] TR-221 Amendment 1	Technical Specifications for MPLS in Mobile Backhaul Networks	BBF	2013
[5] TR-350 Issue 2	Ethernet Services Using BGP MPLS Based Ethernet VPNs (EVPN)	BBF	2018
[6] TR-390	Performance Measurement from IP Edge to Customer Equipment using TWAMP Light	BBF	2017
[7] IP-MPLS 22.0.0	BGP Autodiscovery and Signaling for VPWS-Based VPN Services	BBF	2009
[8] IEEE 802.1Q	Bridges and Bridged Networks	IEEE	2014
[9] 3GPP TS 23.501	Technical Specification Group Services and System Aspects; System Architecture for the 5G System (5GS); Stage 2 (Release 16)	3GPP	2019
[10] 3GPP TR 38.801 v2.00	Technical Specification Group Radio Access Network; Study on new radio access technology: Radio access architecture and interfaces (Release 14)	3GPP	2017
[11] 3GPP TS 38.401	NG-RAN; Architecture description	3GPP	2019

[12] *3GPP TS 33.501	Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16)	3GPP	2019
[13] 3GPP TS 38.410	Technical Specification GroupRadio Access Network; NG-RAN; NG general aspects and principles (Release 15)	3GPP	2018
[14] 3GPP TS 38.470	Technical Specification Group Radio Access Network;NG-RAN; F1 general aspects and principles (Release 15)	3GPP	2019
[15] 3GPP TR 29.891	Technical Specification Group Core Network and Terminals; 5G System – Phase 1; CT WG4 Aspects	3GPP	2017
[16] 3GPP TR 29.561	Technical Specification Group Core Network and Terminals;5G System; Interworking between 5G Network and external Data Networks; Stage 3	3GPP	2020
[17] 3GPP TS 38.420	Technical Specification Group Radio Access Network; NG-RAN; Xn general aspects and principles	3GPP	2020
[18] MEF 6.2	EVC Ethernet Services Definitions Phase 3	MEF	2014
[19] MEF 10.3	MEF 10.3Ethernet Services Attributes	MEF	2013
[20] MEF 22.3	Transport Services for Mobile Networks	MEF	2018
[21] IETF RFC 4762	Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) signaling	IETF	2007
[22] IETF RFC 4761	Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling	IETF	2007
[23] IETF RFC 7432	BGP MPLS-Based Ethernet VPN	IETF	2015
[24] IETF RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)	IETF	2006
[25] IETF RFC 5036	LDP Specification	IETF	2007
[26] IETF RFC 3209	RSVP-TE: Extensions to RSVP for LSP Tunnels	IETF	2001
[27] IETF RFC 3473	Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions	IETF	2003
[28] IETF RFC 5283	LDP Extension for Inter-Area Label Switched Paths (LSPs)	IETF	2008
[29] IETF RFC 2328	OSPF Version 2	IETF	1998
[30] IETF RFC 5340	OSPF for IPv6	IETF	2008
[31] IETF RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments	IETF	1990
[32] IETF RFC 5308	Routing IPv6 with IS-IS	IETF	2008
[33] IETF RFC 3630	Traffic Engineering (TE) Extensions to OSPF Version 2	IETF	2003
[34] IETF RFC 5329	Traffic Engineering Extensions to OSPF Version 3	IETF	2008
[35] IETF RFC 5305	IS-IS Extensions for Traffic Engineering	IETF	2008

[36] IETF RFC 3985	Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture	IETF	2005
[37] IETF RFC 6073	Segmented Pseudowire	IETF	2011
[38] IETF RFC 4447	Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)	IETF	2006
[39] IETF RFC 7348	Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks	IETF	2014
[40] IETF RFC 4271	A Border Gateway Protocol 4 (BGP-4)	IETF	2006
[41] IETF RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks	IETF	2006
[42] IETF RFC 8666	OSPFv3 Extensions for Segment Routing	IETF	2019
[43] IETF RFC 8667	IS-IS Extensions for Segment Routing	IETF	2019
[44] IETF RFC 5880	Bidirectional Forwarding Detection (BFD)	IETF	2006
[45] IETF RFC 5881	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	IETF	2010
[46] IETF RFC 5151	Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions	IETF	2008
[47] IETF RFC 4553	Encapsulation Methods for Transport of Ethernet over MPLS Networks over Packet (SAToP)	IETF	2006
[48] IETF RFC 5086	Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)	IETF	2006
[49] IETF RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)	IETF	2008
[50] IETF RFC 3386	Network Hierarchy and Multilayer Survivability	IETF	2002
[51] IETF RFC 8402	Segment Routing Architecture	IETF	2018
[52] IETF RFC 8572	Secure Zero Touch Provisioning (SZTP)	IETF	2019
[53] 802.1CMde	Time Sensitive Network for Fronthaul	IEEE	2020
[54] MEF 22.3.1	Amendment to MEF 22.3: Transport Services for Mobile Networks	MEF	2020
[55] MEF 23.2	Carrier Ethernet Class of Service – Phase 3	MEF	2016
[56] MEF 26.2	External Network Network Interface (ENNI) and Operator Service Attributes	MEF	2016
[57] MEF 33	Ethernet Access Services Definition	MEF	2015
[58] MEF 51	OVC Services Definitions	MEF	2012
[59] G.8271	Time and phase synchronization aspects of packet networks	ITU-T	2016
[60] G.8271.2	Network limits for time synchronization in packet networks with partial timing support from the network	ITU-T	2016
[61] G.8275.2/Y.1369.2	Precision time protocol telecom profile for phase/time synchronization with partial timing support from the network	ITU-T	2016

[62] G.811	Timing Characteristics of Primary Reference Clocks	ITU-T	1997
[63] G.8261	Timing and Synchronization Aspects in Packet Networks	ITU-T	2007
[64] G.8265	Architecture and requirements for packet based frequency delivery	ITU-T	2007
[65] 8265.1	Precision time protocol telecom profile for frequency synchronization	ITU-T	2010
[66] IEEE 1588V2 (PTPV2)	Precision Clock Synchronization Protocol for Networked Measurement and Control Systems	IEEE	
[67] G.8271.1	Network limits for time synchronization in packet networks	ITU-T	2013
[68] G.8273.2	Timing characteristics of telecom boundary clocks and telecom time slave clocks	ITU-T	2014
[69] G.8273.3	Timing characteristics of telecom transparent clocks	ITU-T	2017
[70] G.8273.4	Timing characteristics of telecom boundary clocks and telecom time slave clocks for use with partial timing support from the network	ITU-T	2020
[71] G.8275 Amd 1	Architecture and requirements for packet-based time and phase distribution, Amendment 1	ITU-T	2015
[72] G.8275	Architecture and requirements for packet-based time and phase distribution	ITU-T	2013
[73] G.8275.1	Precision time protocol telecom profile for phase/time synchronization with full timing support from the network	ITU-T	2016
[74] RFC 1305	Network Time Protocol Specification, Implementation and Analysis, Version 3	IETF	1992
[75] RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification	IETF	2010
[76] RFC 3809	Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)	IETF	2004
[77] RFC 4301	Security Architecture for the Internet Protocol	IETF	2005
[78] RFC 4302	IP Authentication Header	IETF	2005
[79] RFC 4303	IP Encapsulating Security Payload (ESP)	IETF	2005
[80] RFC 4111	Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)	IETF	2005
[81] RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)	IETF	2014
[82] TR 224	Technical Specification for MPLS in Carrier Ethernet Networks	BBF	2014
[83] IETF RFC 8572	Secure Zero Touch Provisioning (SZTP)	IETF	2019

[84] IETF RFC 4023	Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)	IETF	2005
[85] IETF RFC 8661	Segment Routing MPLS Interworking **with LDP	IETF	2019
[86] IETF RFC 7471	OSPF Traffic Engineering (TE) Metric Extensions	IETF	2015
[87] IETF RFC 8570	IS-IS Traffic Engineering (TE) Metric Extensions	IETF	2019
[88] IETF RFC 8491	Signaling Maximum SID Depth (MSD) Using IS-IS	IETF	2018
[89] IETF RFC 8669	Segment Routing Prefix Segment Identifier Extensions for BGP	IETF	2019
[90] IETF RFC 8221	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)	IETF	2017
[91] IETF draft-ietf-teas-ietf-network-slices-05	Framework for IETF Network Slices	IETF	2021
[92] IETF RFC 4203	OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS	IETF	2005
[93] IETF RFC 5307	IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)	IETF	2008
[94] IETF RFC 5420	Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE)	IETF	2009
[95] G.8275 amd2	Architecture and requirements for packet-based time and phase distribution, Amendment 2	ITU-T	2019
[96] 3GPP TR 38.912	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on New Radio (NR) access technology (Release 16)	ITU-T	2020
[97] RFC 2119	Key words for use in RFCs to Indicate Requirement Levels	IETF	1997
[98] RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words	IETF	2017

3.3 Definitions

The following terminology is used throughout this Technical Report.

CSG	Cell Site Gateway – Node at the cell site that presents the transport network interface to the Mobile RAN equipment. For purposes of this document this device is IP capable node or an MPLS capable node
IP TNL	The Transport Network Layer defined in this document as the transport bearer for 5G and

	LTE IP traffic
ETH TNL	The Transport Network Layer defined in this document where the transport commits to preserving the Ethernet/802.3 PDU end-to-end in forwarding Ethernet frames between TNL end-points, the TNL is an Eth TNL (irrespective of what is encapsulated within the Ethernet frames).
MASG	Mobile Aggregation Site Gateway – Last transport node before the MME or serving gateway site or Edge DC, that presents the transport network interface to the mobile equipment. For purposes of this document this device is an MPLS capable node.

3.4 Abbreviations

This Technical Report uses the following abbreviations:

TR	Technical Report
WA	Work Area
WT	Working Text
APTS	Assisted Partial Timing Support
PTP	IEEE 1588 Precision Time Protocol
GNSS	Global Navigation Satellite System
PRTC	Primary Reference Time Clock
PRC	Primary Reference Clock
3GPP	3rd Generation Partnership Project
5GC	5G Core Network
AC	Access Circuit
AN	Access Node
AMF	Access and Mobility Management Function
ATM	Asynchronous Transfer Mode
BBF	Broadband Forum
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BS	Base Station
BSC	Base Station Controller
BTS	Base Transceiver Station
BW	Bandwidth
CDMA	Code Division Multiple Access
CE	Customer Edge
CES	Circuit Emulation Service
COS	Class Of Service
CSG	Cell Site Gateway
CV	Connectivity Verification
DC	Data Center
ECMP	Equal Cost Multi-Path
EDGE	Enhanced Data Rates for GSM Evolution
EN	Edge Node
eNB	E-UTRAN Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVC	Ethernet Virtual Connection

FDD	Frequency Division Duplex
FEC	FEC Forwarding Equivalence Class
ES	End System
GTP-U	GPRS Tunneling Protocol User Plane
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GSM	Global Standard for Mobile Communication
GW	Gateway
HDLC	High-Level Data Link control
HSPA	High Speed Packet Access
H-VPLS	Hierarchal Virtual Private LAN Service
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunication Union - Telecom
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switched Path
LSR	Label Switch Router
LTE	Long Term Evolution
MASG	Mobile Aggregation Site Gateway
MEF	Metro Ethernet Forum
MME	Mobility Management Entity
MPLS	Multi Protocol Label Switching
MSC	Mobile Switching Center
MS-PW	Multi-Segment Pseudowire
NB	Node B (Base Station)
NTP	Network Time Protocol
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
OAM	Operations, Administration and Management
P	Provider
PCP	Priority Code Point
PDV	Packet Delay Variation
PE	Provider Edge
P-GW	PDN (Packet Data Network) Gateway
PHP	Per Hop Behavior
POS	Packet over SONET / SDH
PTPv2	Precision Time Protocol version 2 as defined in IEEE 1588v2
PPP	Point to Point Protocol
PSN	Packet Switched Network
PW	Pseudowire
PON	Passive Optical Networking
PPP	Point-to-Point Protocol
PRC	Primary reference clock
PRTS	Primary Reference Time Clock
QoS	Quality of Service
(R)AN	(Radio) Access Network
RC	Radio Controller
RFC	Request for Comments
RNC	Radio Network Controller
RSVP-TE	Resource ReSerVation Protocol
RTP	Real Time Transport Protocol
SATOP	Structure Agnostic TDM Over Packet
SDN	Software-Defined Networking

S-GW	Serving – Gateway
SLA	Service Level Agreement
SMF	Session Management Function
SONET	Synchronous Optical Network
S-PE	Switching Provider Edge Router
SRG	Shared Risk Group
SS-PW	Single-Segment Pseudowire
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TE	Traffic Engineering
T-LDP	Targeted Label Distribution Protocol
TLV	Type/Length/Value
TNL	Transport Network Layer
T-PE	Terminating Provider Edge Router
TR	Technical Report
UMTS	Universal Mobile Telecommunications System
UNI	User to Network Interface
UTRAN	UMTS Terrestrial Radio Access Network
VCCV	Virtual Circuit Connectivity Verification
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WCDMA	Wideband Code Division Multiple Access
WG	Working Group
WT	Working Text
UPF	User Plane Function

4 Technical Report Impact

4.1 Energy Efficiency

By using MPLS technology to facilitate convergence in mobile backhaul networks, energy efficiency can be realized. For example:

Several releases/generations (e.g., 2G/3G/4G/5G) of mobile network services (i.e., TDM, ATM, Ethernet and IP RAN backhaul traffic) can be transported on a converged network infrastructure.

More functions can be combined into the same node (e.g., L2VPN and L3VPN hybrid), which means fewer nodes are needed in the networks, thus energy consumption can be reduced.

MPLS based technologies such as L3VPN or VPLS can support multicast services efficiently, thus source replication is not needed and energy efficiency for multicast service can be improved.

4.2 IPv6

IPv6 is an integral part of the specification below.

4.3 Security

Security requirements above the transport layer are specified by 3GPP. For example, for LTE, traffic between eNB and MME or S-GW, may be encrypted using IPsec if the deployment scenario demands it.

For 5G traffic between gNB and UPF / AMF and traffic between the DU and the CU can also be encrypted with IPsec if the deployment scenario demands it. In some cases, for DU to CU traffic MACSEC can be used as well.

Security risks on the mobile backhaul network (e.g., securing the MPLS control plane or IP control plane) are addressed by the security requirements described further in the document in Sections 7.1.6 and 9.3.

4.4 Privacy

Any issues regarding privacy are not affected by TR-521.

5 Reference Architecture

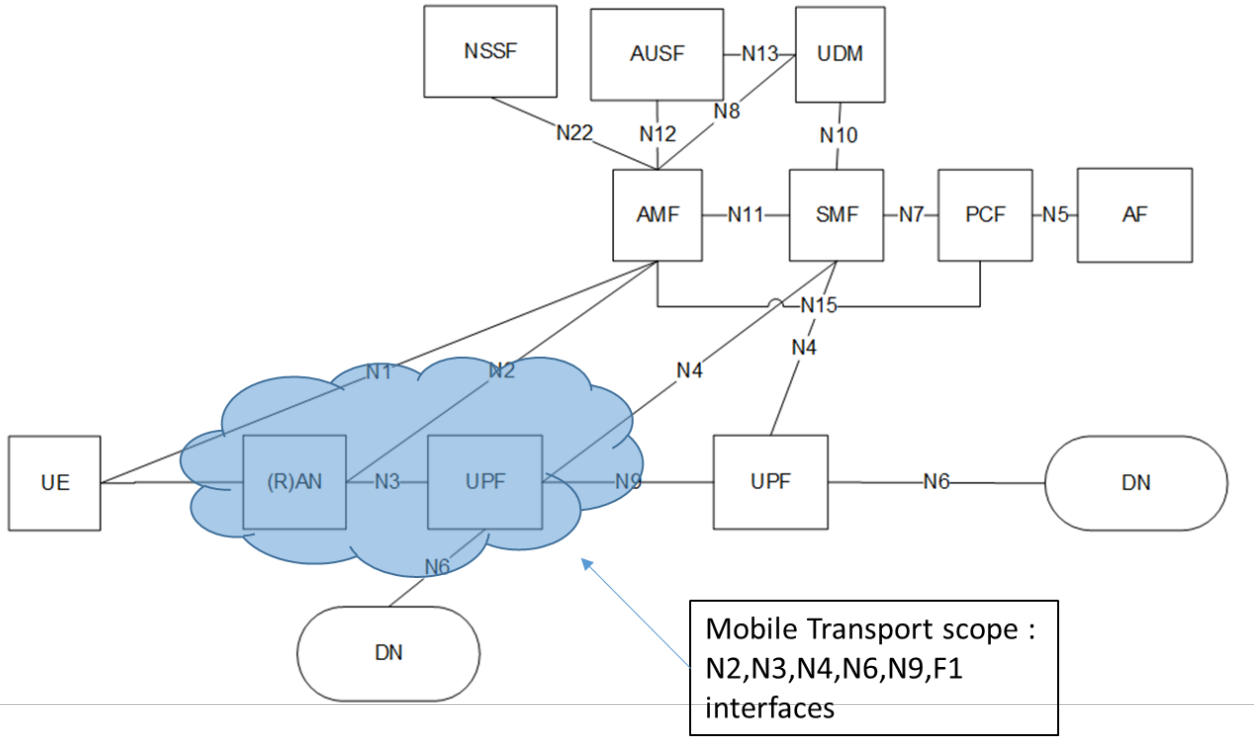


Figure 5.1: 5G system architecture as depicted in 3GPP TS 23.501 document with Mobile transport portion of it

Figure 5.1 depicts the 5G system architecture as per 3GPP TS 23.501 [9] with the Mobile transport scope indicated. The mobile transport scope will include the following interfaces:

1. N3, N2 from the RAN to data and control
2. N6, N4 and N9 in case the UPF resides in the aggregation network.

Note: N1 is not in scope as well as other interfaces between 5G control elements that runs in the Mobile core. This architecture does not include the different split options in the RAN.

Beside the radio access and core network, the **transport network will play a key role in 5G** to flexibly and dynamically address the requirements of future mobile networks. In order to support the required flexibility, an **enhanced packet-based network** is required. In order to address backhaul and fronthaul interfaces, traffic class concepts at the transport layer will be leveraged. Furthermore, to efficiently support network slicing by the transport network, SDN and network functions virtualization (NFV) may be supported by the transport network, e.g., by separating the control and data planes through common packet-based data path abstraction. This **unified data and control plane** interconnects distributed 5G radio access and core network functions, hosted on the mobile in-network cloud infrastructure. The 5G transport network will consist of **integrated optical, Ethernet, IP and wireless e.g., Microwave network infrastructure**.

5.1 Functional Splits and RAN interfaces

3GPP TR 38.801 v2.00 [10] defines functional splits as follows:

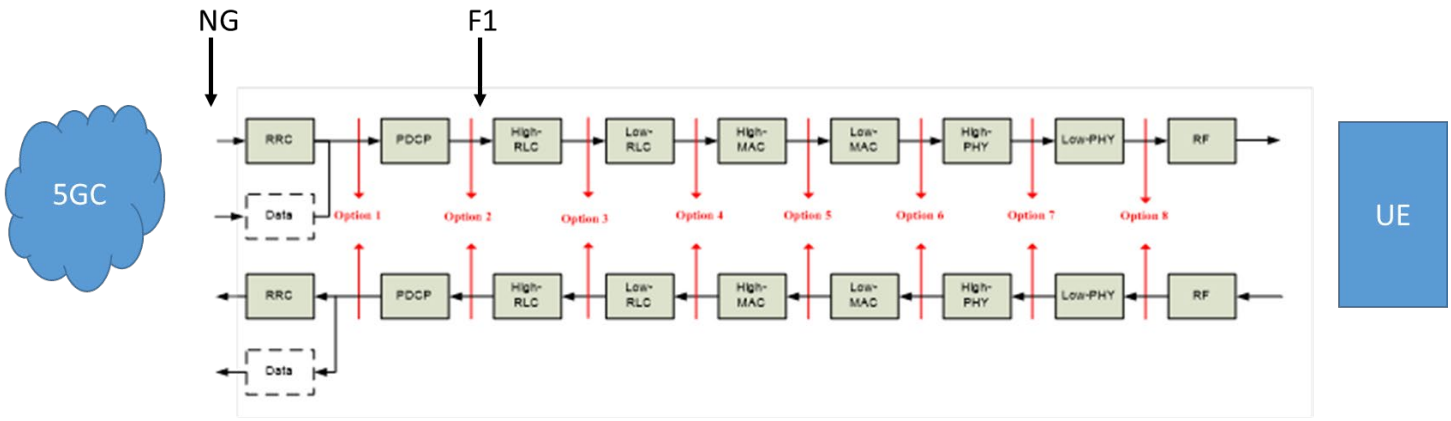


Figure 5.2: Function Split between central and distributed unit

PHY – Physical layer processing
MAC – Medium Access Control
RLC – Radio Link Control
PDCP – Packet Data Convergence protocol
RRC – Radio Resource Control

Lower Layer functional splits are splits above the PHY layer and higher layer functional splits are splits below the PHY layer. Currently 1 Higher layer splits is defined for 5G Option 2 [CU/DU split]) F1.

Figure 5.2 depicts the following:

- NG Interface: When the gNB is not split provides data interface between the gNB to the UPF
- F1 interface: The interface between the CU and the DU High Layer Split defined as split option 2

5.2 Supported technologies and TNL types

The reference architecture (Figure 5.3) shows various scenarios that are based on the type of the Transport Network Layer (TNL) carried over the access and aggregation network. Two types of TNL are considered in this document (IP and Ethernet) depending on for example the mobile network generation and network split type, as shown in Table 5.1 which presents different TNL scenarios using various transport technologies in the access and aggregation networks to transport these TNL types. TR-221 [1] specifies the TDM and ATM TNLs used for 2G & 3G mobile networks. TR-221 [1] also specifies that IP TNL can be implemented by transporting the IP packet over different transport layers, but it also enables transport the Ethernet frame encapsulating the IP as part of the IP TNL transport.

This document includes the concept of an Ethernet (Eth) TNL for transparent bridging of Ethernet frames. In this document IP TNL is distinguished from Eth TNL as flows:

1. *If the transport allows IP forwarding at any point between TNL end-points, the TNL is an IP TNL as defined in TR-221 [1].*

2. *If the transport commits to preserving the Ethernet/802.3 PDU end-to-end in forwarding Ethernet frames between TNL end-points, the TNL is an Eth TNL (irrespective of what is encapsulated within the Ethernet frames).*

In this document, IP TNL will have the same definition, however in Eth TNL it is not sufficient to transport just an IP packet encapsulated by Ethernet frame. It is a must to transport any Ethernet frame (802.1CMde [53], for example).

Table 5.1: RAN Access Technologies

Network	Specification	TNL type
LTE	R8,R9,R10	IP
5G – High layer Splits	R15	IP
5G – Low layer Splits	R15 / xRAN	Eth (Ethernet)
5G – UPF resides in the Aggregation network	R15	IP

In the context of the TR-221 [1], the scenarios arising out of these TNLs are hereafter referred to as TNL Scenarios since they refer to the transport service provided by the packet-based network to the mobile access/aggregation network. Thus the following TNL scenarios are included:

1. Eth TNL
2. IP TNL

The architecture and requirements for the ETH TNL support are specified per TR-224 [82] for VPLS and per TR-350i2 [5] for EVPN. These detail how to provide an Ethernet service such as EPL or EVPL. Ethernet services for 5G Transport are as specified by MEF. 22.3 [20] (as amended by MEF 22.3.1 [54]).

Time-Sensitive Networking (TSN) features for mobile transport, that may be supported over an ETH TNL, are described by IEEE Std. 802.1CM. This includes Ethernet interface support of traffic classes, strict priority, flow metering and synchronization. This support ensures support of these features all the way to the gNB. It should be noted that the underlying VPLS and EVPN networks can provide enhanced features using IETF DetNet technology.

For each supported TNL scenario, the packet transport network may extend from the MASG to various nodes in the mobile access/aggregation network as indicated by the cases (a) to (e) in Figure 5.3. These are referred to as Architecture Scenarios.

The specific combinations of TNLs supported by mobile transport equipment are a business consideration and not a subject for standardization.

5.3 Architecture Scenarios

Figure 5.3 provides a reference architecture, depicting the access, aggregation, and core parts of the mobile backhaul network considering all current types of TNL used in LTE and 5G in mobile networks.

5.3.1 Architecture of 5G/4G high layer splits scenario

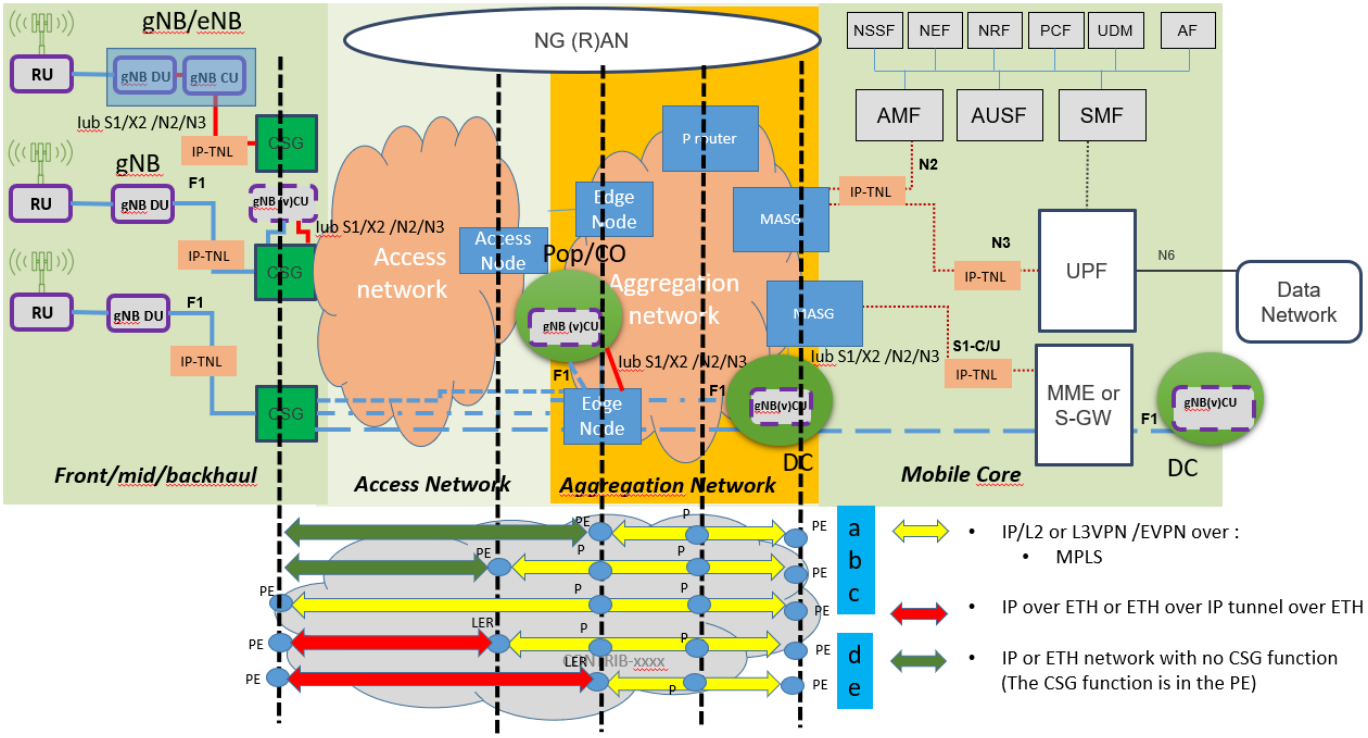


Figure 5.3: Reference Architecture for mobile backhaul network using packet Transport in the Access, Aggregation, and Core Networks for high layer splits

Note: The above figure does not depict the case in Figure 5.3 where the UPF is located in the aggregation network which then put N4 (to the SMF) and N6 (to the Data Network) and N9 (data between UPFs) over the IP TNL.

The green Arrow on Figure 5.3 shows a case where the transport provider's first PE is not located on the cell site but on the Access or aggregation network. In this case there is no Transport provider CSG at the Cell site. In this case the connection between the cell site and the first Transport PE might be an Ethernet or IP network. The last device in the cell site simply delivers (and receives) packets over that ETHERNET or IP network.

The red arrow depicts a case where the CSG belongs to the transport provider/ mobile provider and the CSG provides a point to point connection over the Ethernet (case d or e) or IP (case e) network. In this case the CSG can be Eth device, IP Router, or bridge device. In case it is router and bridge then we need to transport the Eth over IP tunnel.

All encapsulations over packet network solutions performed in the CSG require suitable adaptation mechanisms at the MASG to provide a compliant interface N2, N3 and S1 C and U for interconnection to the AMF UPF MME and S-GW. Figure 5.1 depicts packet-based mobile backhaul network in the Access and Aggregation networks connecting Base Stations to AMF, UPF, MME/S-GW, and cases to connect UPF to other UPF or SMF or DN. The reference architecture depicts the following connectivities:

1. Split option 1 for both LTE and 5G where the interface that is connected to the CSG connects the PDCP and the RRC layers. In this case the TNL is generated from the Iub S1/X2 in 4G and N2/N3 and Xn in 5G.

2. Split option 2 defined for 5G only where the interface that is connected to the CSG connects the RLC and PDCP layers. In this case the TNL is generated from the F1 interface in 5G.
3. UPF residing in the aggregation network:
    a. The TNL is generated from N6 connecting the UPF to the DC
    b. The TNL is generated from N9 connecting the UPF to another UPF
    c. The TNL is generated from N4 connecting the UPF to the SMF

In the reference architecture, the location of packet-based solutions functions for the various TNL scenarios is flexible; i.e., the interworking functions required to transport mobile traffic (TNL) could be located either in the Edge Node (EN), or in the Access Node (AN), or in the CSG. Moreover, in Split option 2 the TNL connection is split from the DU to the CU and from the CU to AMF/UPF. In this case the CU can reside in the cell site over local NFVI or in different DC location in the network. The location and reachability to the CU depends on various deployment considerations.

Various Deployment Scenarios arise based on the location of MPLS functions and the extent of MPLS in the mobile backhaul network. Cases (a) through (e) in Figure 5.3 depict these deployment scenarios through the access and aggregation networks:

1. MPLS or VXLAN transport is used between the EN and the MASG via LSP or L3VPN or EVPN carrying a TNL.
2. MPLS or VXLAN transport is used between the AN and the MASG via LSP or L3VPN or EVPN carrying a TNL.
3. MPLS or VXLAN transport is used between the CSG and the MASG, with the AN transparent to MPLS. LSP or L3VPN or EVPN carrying a TNL is established between the CSG and the MASG, which act as PE devices, while all MPLS nodes in the aggregation network act as P routers.
4. IP/MPLS transport is used between the CSG and the MASG using segment routing, with an AN that is IP/MPLS segment routing aware. LSP or L3VPN or EVPN carrying a TNL is established between the CSG and the MASG, which act as PE devices, while the AN and MPLS devices in the aggregation network act as P routers all aware of segment routing.
5. IP/MPLS transport is used between the CSG and the MASG, with the AN transparent to IP/MPLS / segment routing. LSP or L3VPN or EVPN carrying a TNL is established between the CSG and the MASG, which act as PE devices, while all MPLS nodes in the aggregation network act as P routers

For each IP/MPLS use case, an overlay model based upon L2VPN could be used between any IP/MPLS routers. L2VPN can be based upon VPWS or VPLS, EVPN over MPLS or VXLAN in the aggregation network, and even down to the AN or CSG. This overlay model relies on the separation of IP control planes: there is one IP control plane to support MPLS carrying the TNL, and another IP control plane used for the aggregation network which is completely independent from the previous one. It is important to note that in this overlay model the TNL is carried over an Ethernet PW at the CSG/MASG and / or AN / EN, and the Ethernet layer is carried over L2VPN in the aggregation and Access network (including AN and CSG optionally). This overlay model could be chosen by operators to tackle operational or equipment constraints or in order to provide an Ethernet connectivity to a specific Ethernet Managed Service.

There are different types of solutions based upon MPLS and/or IP that could be used to transport LTE traffic in the Access/Aggregation/Core networks: L2VPN and L3VPN solutions.

The IP TNL may be realized by either a L3VPN or an L2VPN or EVPN over MPLS or IP with or without segment routing. The architectures described in this section have to support IP connectivity requirements between DU part of the BS and the CU part of it that reside in different locations in the network, as well as between the CUs and AMF, UPF, and UPF SMF other UPF and data network. In addition, it needs to support connectivity between BSs.

5.3.1.1 NG-RAN Architecture

The below figure depicts the NG-RAN architecture and its corresponding interfaces:

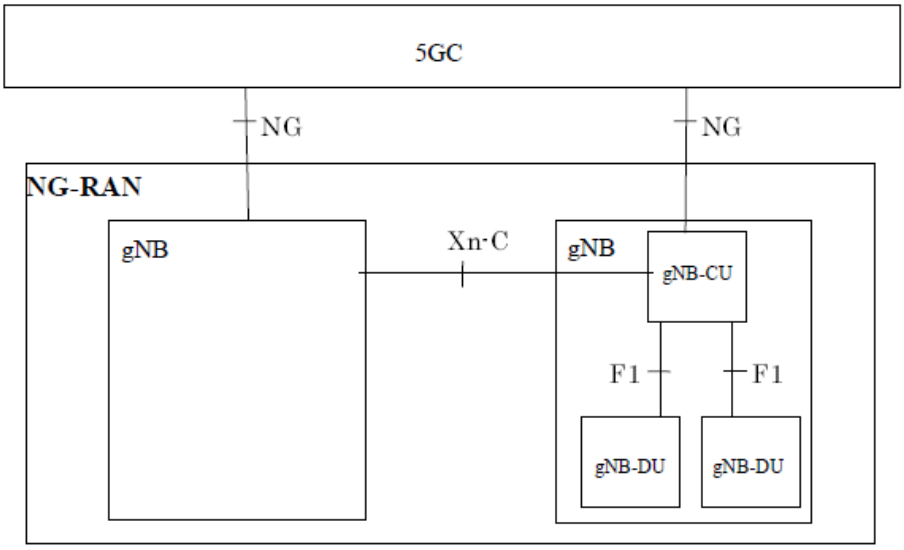


Figure 5.4: NG-RAN architecture no gMB split and Split option 2 and the corresponding interfaces.

5GC – 5G Core

gNB- 5G Node B.

> **Note:** NG and N3 are similar interfaces.

As indicated in 3GPP TS 38.401 [11] version 16.1 Release 16:
The NG-RAN consists of a set of gNBs connected to the 5GC through the NG interface.

An gNB can support FDD mode, TDD mode or dual mode operation.

gNBs can be interconnected through the Xn interface.

A gNB may consist of a gNB-CU and one or more gNB-DU(s). A gNB-CU and a gNB-DU is connected via F1 interface. One gNB-DU is connected to only one gNB-CU.

> **Note:** For resiliency, a gNB-DU may be connected to multiple gNB-CUs by appropriate implementation.

NG, Xn and F1 are logical interfaces.

For NG-RAN, the NG and Xn-C interfaces for a gNB consisting of a gNB-CU and gNB-DUs, terminate in the gNB-CU.

The NG-RAN is layered into a Radio Network Layer (RNL) and a Transport Network Layer (TNL).

The NG-RAN architecture, i.e., the NG-RAN logical nodes and interfaces between them, is defined as part of the RNL.

For each NG-RAN interface (NG, Xn, F1) the related TNL protocol and the functionality are specified. The TNL provides services for user plane transport, signaling transport.

In NG-Flex configuration, each gNB is connected to all AMFs within an AMF Region. The AMF Region is defined in *3GPP TS 33.501 [12].

If security protection for control plane and user plane data on TNL of NG-RAN interfaces has to be supported, NDS/IP *3GPP TS 33.501 [12] shall be applied.

6 Specifications and Requirements

This chapter specifies requirements of equipment and functions in 5G transport networks.

6.1 Transport Service

6.1.1 Connectivity

The traffic at the Aggregation Network and Core Network will be over MPLS. The Access network is not a routed network but can carry IP TNL over MPLS or IP TNL over IP tunnel and/or over VLAN. Since the IP TNL includes a case of carrying the full Ethernet frame End to End, and even though the access network is not a routed network, IP tunnels are needed when MPLS is not used. 5G multicast and broadcast services can be supported by L2VPN and L3VPN MPLS technologies.

6.1.1.1 MPLS connectivity

6.1.1.2 L2VPN/EVPN MPLS connectivity for IP TNL using Ethernet

The mobile technologies identified in Table 5.1 using the IP TNL may utilize Ethernet services for the backhaul network. When L2VPNs are used to provide MEF Mobile Backhaul services between MEF compliant UNIs at the BS and AMF UPF MME and S-GW sites, MEF compliant EVC based services and attributes as specified in MEF 22.3 [20] are used. MEF services are supported as VPWS or VPLS or EVPN across the domain that uses MPLS for transport. Specifically, this document realizes the E-Line and E-LAN services described by the MEF mobile backhaul IA (MEF 22.3 [20] and MEF 6.2 [18]). This document also realizes an E-Tree* service (a subset of MEF E-Tree service defined in Appendix F) that is based on hub & spoke topology with only one root (i.e., replication is done in a single node).

> **Note:** MEF 22.3 [20] describes how mobile backhaul can be supported by Carrier Ethernet Services in MEF 6.2 [18], using Service Attributes defined in MEF 10.3 [19] and MEF 22.3 [20]. The additional service attributes focus on availability, resiliency performance, CoS and synchronization.

In the mobile backhaul network, Ethernet VLAN tagging as per IEEE 802.1Q [8], may be used for traffic separation, for example to separate management from user traffic, to separate traffic between operators in case of RAN sharing or to separate 2G, 3G LTE, and 5G traffic in case of traffic aggregation.

Figure 5.3 provides the reference architecture for L2VPN solutions as VPLS (e.g., IETF RFC 4762 [21] and/or IETF RFC 4761 [22]) or EVPN (e.g., IETF RFC 7432 [23]), H-VPLS option of RFC 4762 [21] and VPWS in the mobile backhaul network for 2G/3G using IP TNL or LTE or 5G, depicting the Access, Aggregation and Core parts of the mobile backhaul network to transport Ethernet frames encapsulating IP TNL between mobile nodes. The same L2VPN transport solution could be used to backhaul N2, N3, N6, N9 and N4 interfaces in order to get a converged and efficient network solution for 5G.

VPLS or EVPN can be used in the Aggregation network with PE routers embedded into the ENs and optionally moved to the ANs. VPLS can be extended down to the CSGs and up to the MASG through the Access and Aggregation networks.

H-VPLS can be used in the Aggregation and Access networks to enhance scalability by reducing the mesh between the nodes.

VPWS can be used in the Aggregation network with PE routers embedded into the ENs. VPWS can be extended down to the CSGs and up to the MASG though the Access and Aggregation networks.

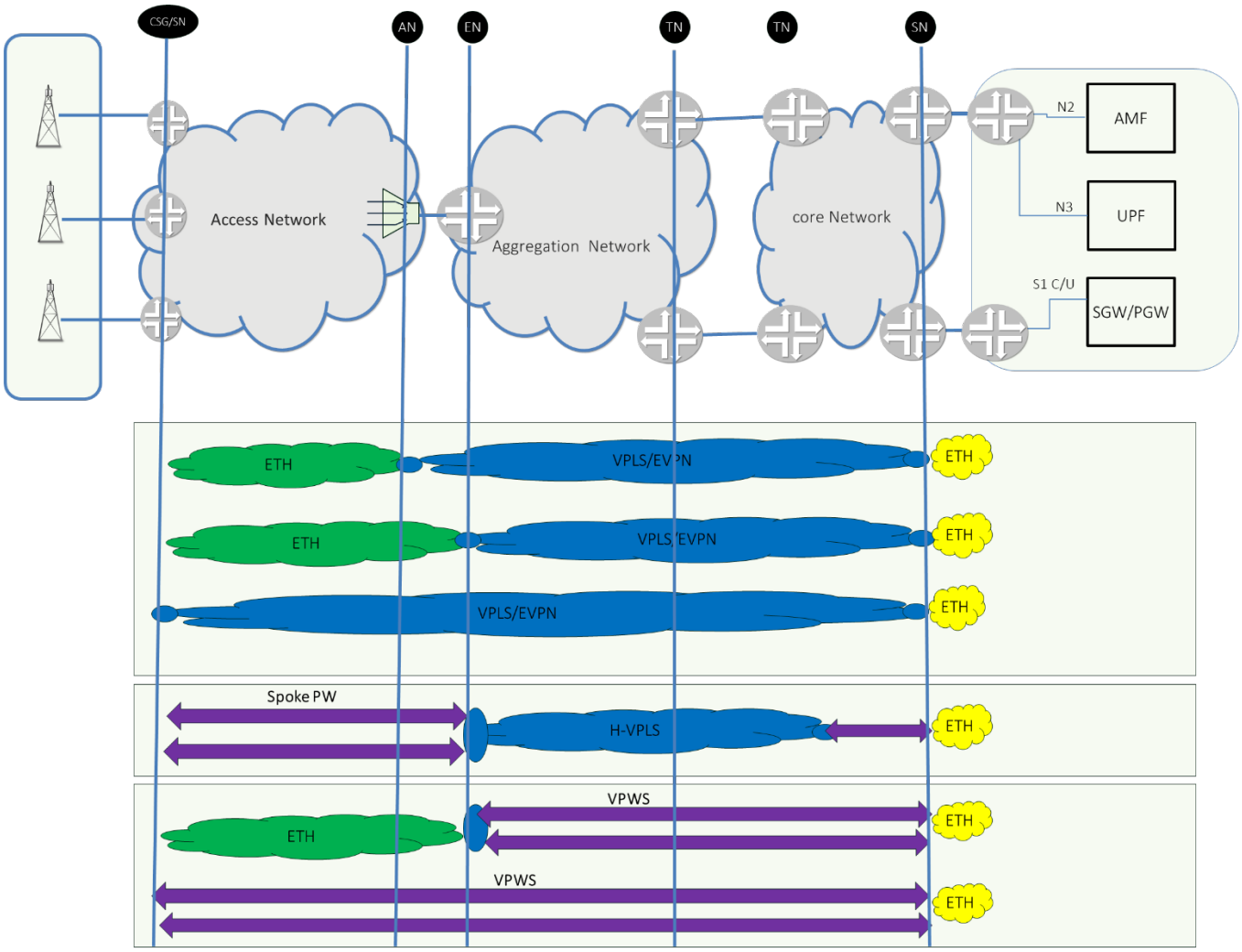


Figure 6.1: Reference Architecture of L2VPN/EVPN MPLS connectivity for IP TNL using Ethernet

Figure 6.1 depicts several use cases:

- Eth access to L2VPN
- L2VPN from the CSG
- Spoke PW to H-VPLS
- Eth from the CSG to VPWS
- VPWS from the CSG end to end

6.1.1.3 *L3VPN MPLS connectivity for IP TNL

Figure 6.2 provides the reference architecture for L3VPN solutions IETF RFC 4364[27] in the mobile backhaul network for 2G/3G using IP TNL, LTE or 5G, depicting the Access, Aggregation and Core parts of the mobile backhaul network to transport IP TNL between mobile nodes. It is interesting to note that a single

L3 VPN MPLS transport solution IETF RFC 4364 [24] could be used to backhaul both N2, N3, N6, N4 and N9 interfaces in order to get a converged and efficient network solution for 5G.

L3VPN MPLS can be used in the Aggregation network with PE routers embedded into the ENs and optionally moved to the ANs. L3VPN MPLS can be extended down to the CSGs and up to the MASG through the Access and Aggregation networks.

MPLS Layer 3 VPNs use a peer-to-peer VPN Model that leverages BGP to distribute VPN-related information. They are based on IETF RFC 4364 [24] and support QoS and Traffic Engineering. The VPNs provide layer 3 connectivity across the backhaul network and provide any to any topology to support N2, N3, N4, N6, N4 and N9 interfaces. MPLS Layer 3 VPNs can be deployed over MPLS TE enabled networks with related mechanisms, QoS reliability to offer strict SLA.

Different VPNs remain distinct and separate, even if two VPNs have an overlapping address space.

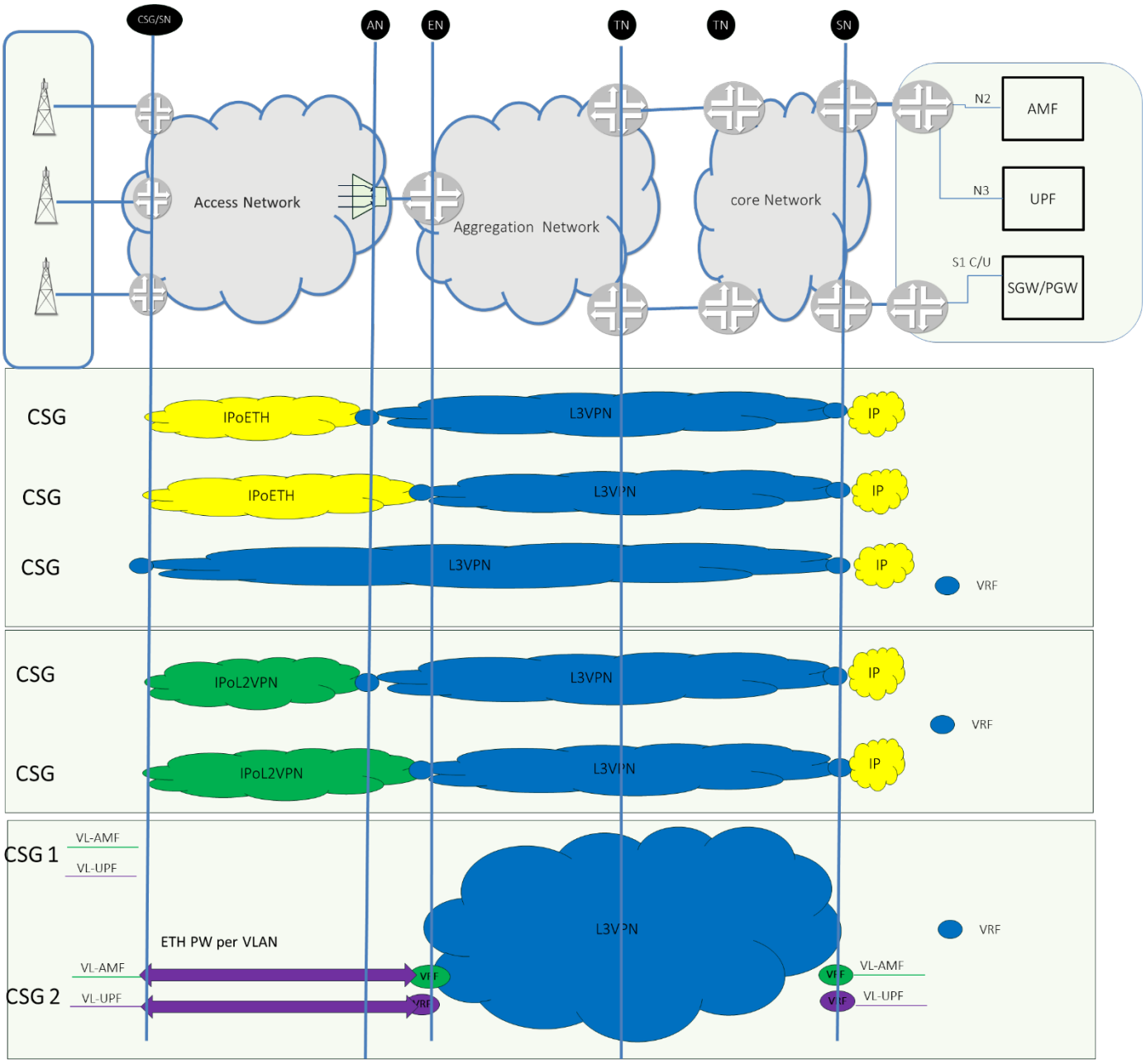


Figure 6.2: Reference Architecture of L3VPN MPLS connectivity for IP TNL

Figure 6.2 depicts several cases:

- IPoETH with or without VLAN in the access networks to L3VPN. In this case a VLAN is used to indicate the VRF#
- L3VPN directly from the CSG
- IPoL2VPN In the access networks to L3VPN
- Eth PW to L3VPN

6.1.1.4 IP connectivity

IP connectivity can be in the access network only since the assumption is that the aggregation and core network will be based on MPLS.

6.1.1.5 IP connectivity for IP TNL using Ethernet

In this case the CSG is connected to the PE (AN/PE) over IP via Ethernet access network, since it needs to transfer the ETH as part of the TNL it will use some kind of ETH over IP tunneling Mechanism.

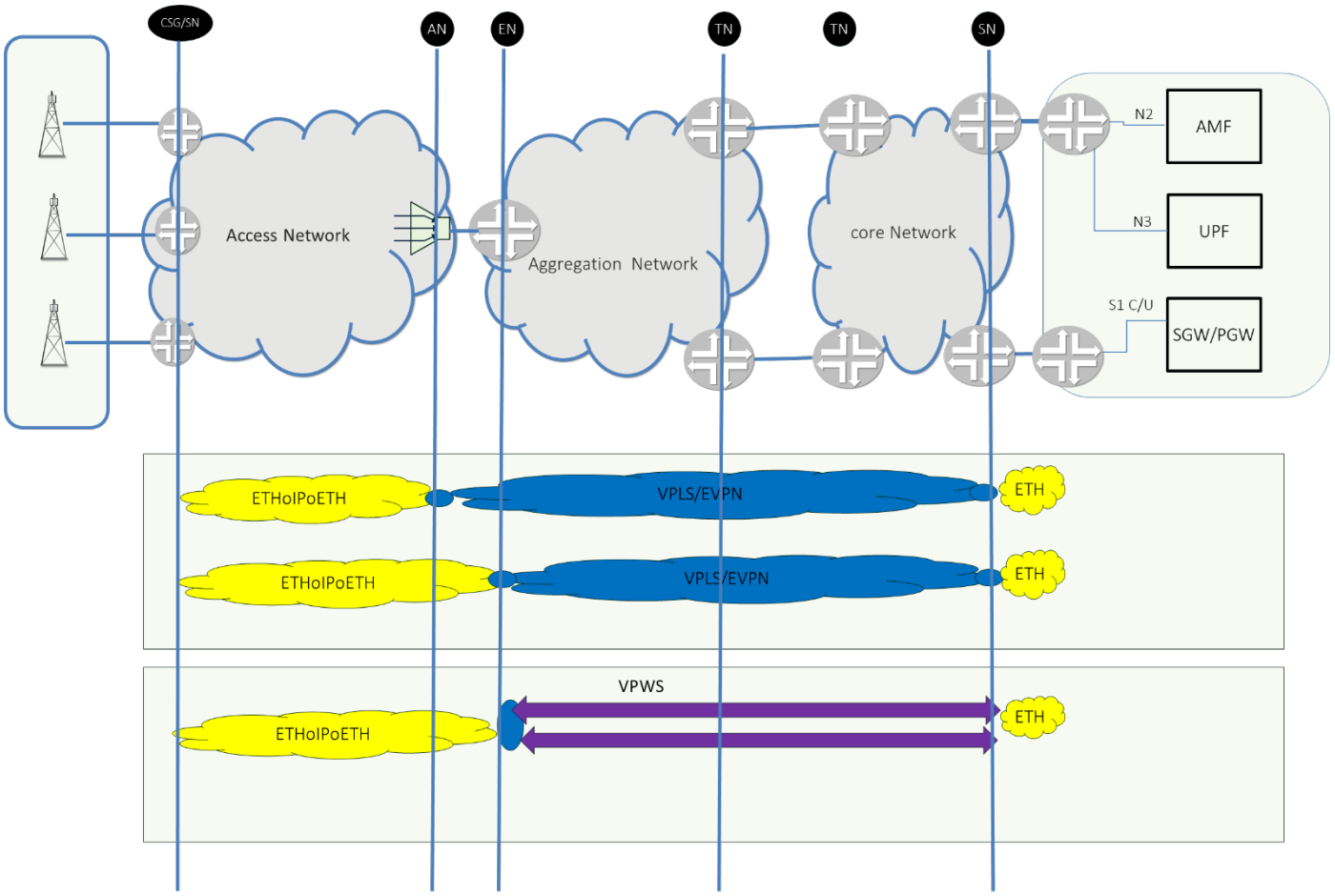


Figure 6.3: IP connectivity in the access for IP TNL over Ethernet.

6.1.1.6 IP connectivity for IP TNL

In this case the CSG is connected to the PE (AN/PE) over IP using Ethernet access network, there are some cases where the CSG runs “Flat” IP as depicted in Figure 6.4 and some other cases depicted below where the IP network in the access uses different address space than the backhaul equipment. In this case a tunnel should be used to carry IP in IP.

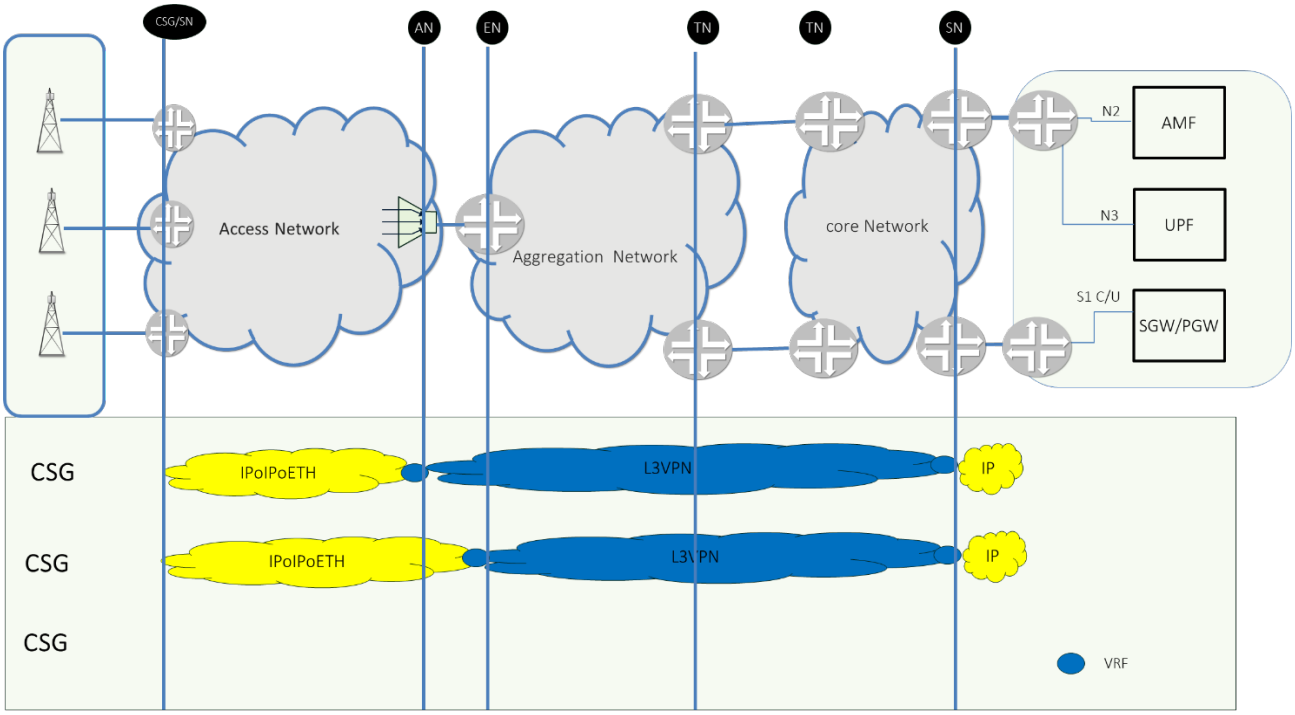


Figure 6.4: IP connectivity in the access for IP TNL

On the above figure there is an IP network at the access network and a tunnel is used to carry the original IP packet over the access network in to the L3VPN in the aggregation and core.

6.1.2 Protocol stack

6.1.2.1 TNL encapsulation

- NG (N3) interface

As depicted in 3GPP TS 38.410 [13] V15.2.0 (2018-12) the following are the NG-U and NG-C encapsulations:

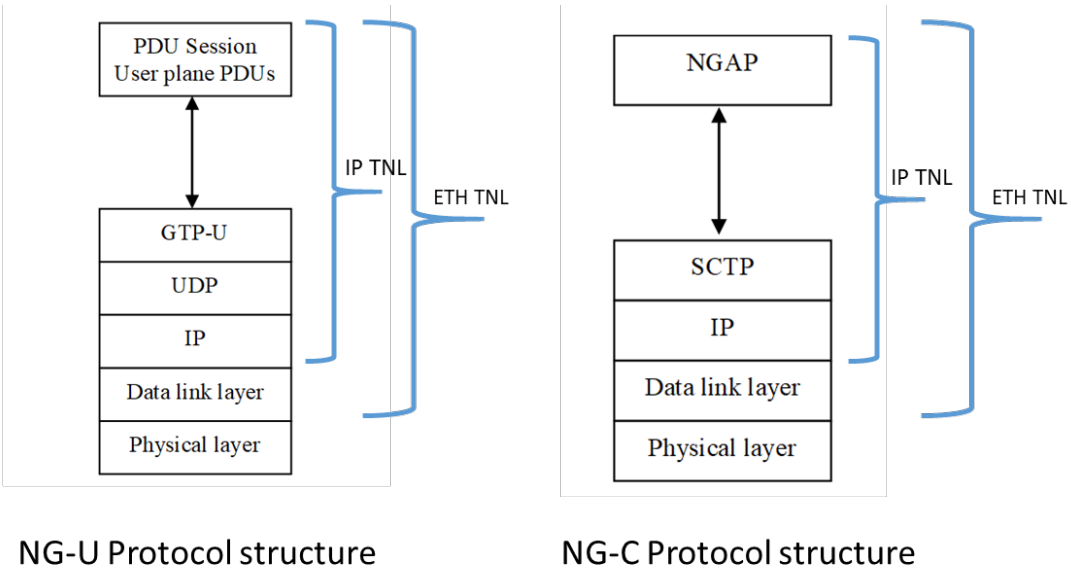


Figure 6.5: NG-U/C protocol structure

The NG user plane (NG-U) interface is defined between a NG-RAN node and a UPF. The NG-U interface provides non-guaranteed delivery of PDU Session user plane PDUs between the NG-RAN node and the UPF.

In the NG-U transport network layer is built on IP transport. For the reliable transport of signaling messages, SCTP is added on top of IP. The application layer signaling protocol is referred to as NGAP (NG Application Protocol).

- F1 interface

As defined in 3GPP TS 38.470 [14] V15.6.0 (2019-07):

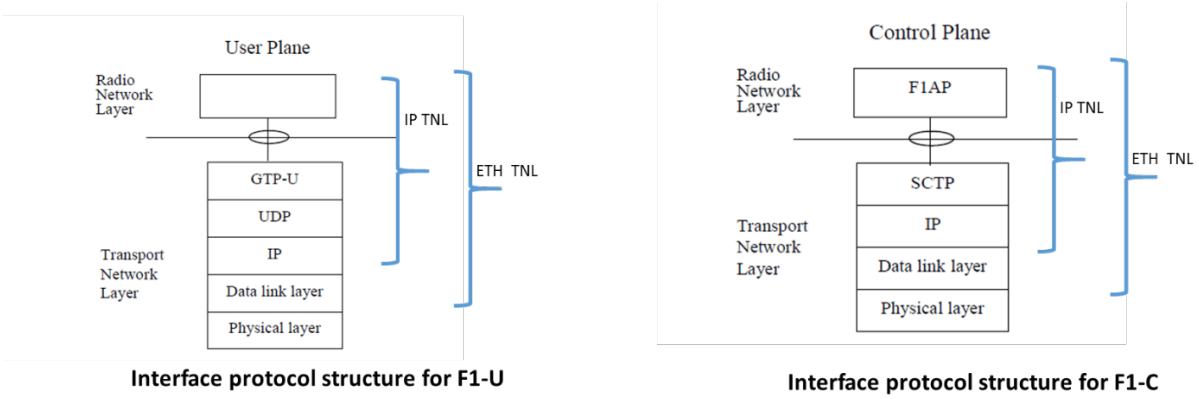


Figure 6.6: F1-U/C protocol structure

The F1-U interface is connecting the gNB-DU with the gNB-CU-UP (User plan) while the F1-C interface connected the gNB-DU with the gNB-CU-CP (control protocol)

In case of IP –TNL the CSG will transfer either IP TNL I.E only the IP layer or in case of ETH-TNL the Ethernet part as well.

- N9 interface

As depicted in 3GPP TR 29.891 [15] V15.0.0 (2017-12) section 5.2.1.1 the following is the N9 encapsulations:

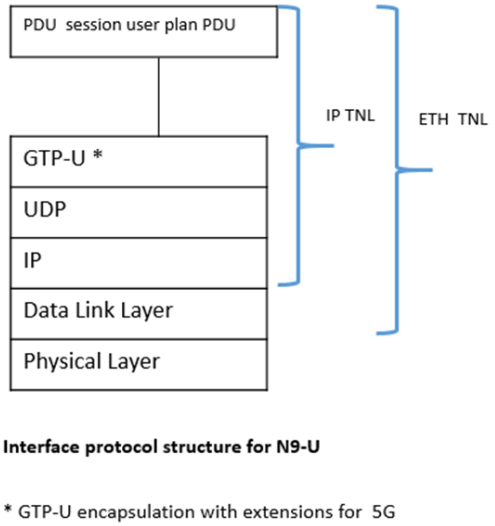


Figure 6.7: N9 protocol structure

- The N9 user plane (N9-U) interface is defined between a pair of UPFs. The N9-U interface provides non-guaranteed delivery of PDU Session user plane PDUs between the two UPFs.
- The protocol stack for N9 is shown in Figure 6.7.
- In case of IP –TNL the CSG/ Transport device will transfer either IP TNL I.E only the IP layer or in case of ETH-TNL the Ethernet part as well
- N6 interface

As defined in 3GPP TS 29.561 [16]V16.3.0 (2020) section 8.2 following is N6 encapsulation

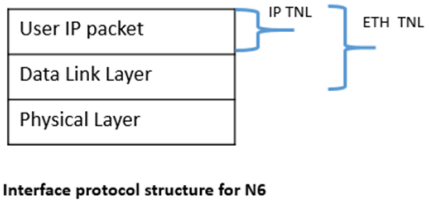


Figure 6.8: N6 protocol structure

- The N6 interface is defined between the UPF and a Data Network. The N6 interface provides non-guaranteed delivery of PDU Session, user plane PDUs, between the a UPF and a Data Network. The protocol stack for N6 is shown in Figure 6.8 In case of IP –TNL the MASG will transfer either IP TNL I.E only the IP layer or in case of ETH-TNL the Ethernet part as well.
- Xn interface
- As defined in 3GPP TS 38.420 [17] version 16.0.0 Release 16 section 7 following is the Xn encapsulation

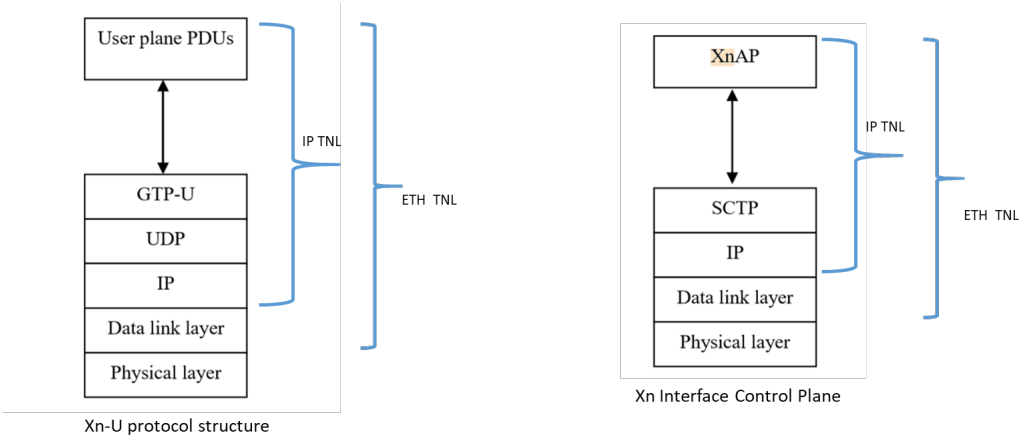


Figure 6.9: Xn protocol structure

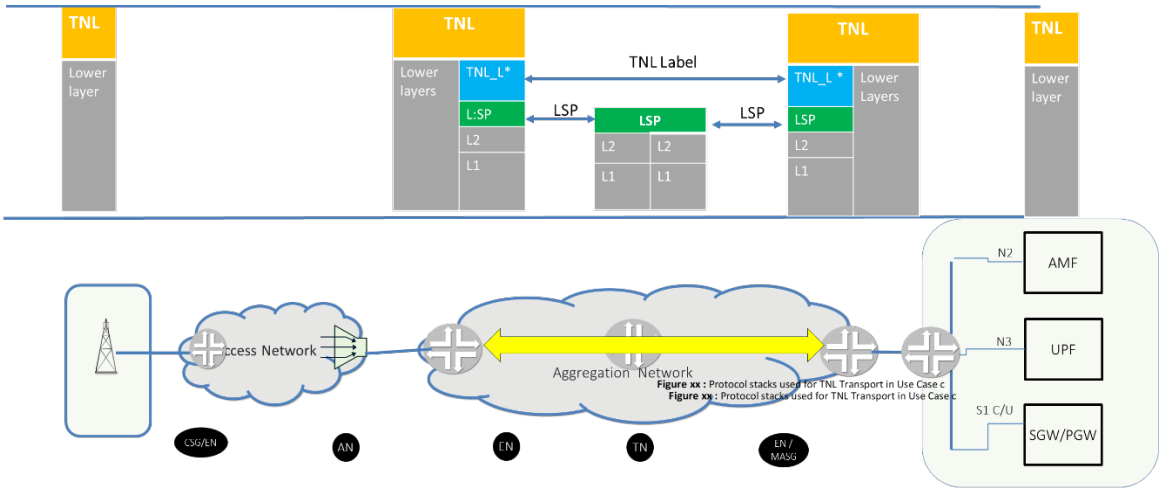
The Xn user plane (Xn-U) interface is defined between two NG-RAN nodes. The Xn-U interface provides nonguaranteed delivery of user plane PDUs between two NG-RAN nodes.

The transport network layer is built on IP transport. For the reliable transport of signaling messages, SCTP is added on top of IP. The application layer signaling protocol is referred to as XnAP (Xn Application Protocol).

The protocol stack for Xn-U and Xn-C is shown in Figure 6.9 case of IP –TNL the CSG will transfer either IP TNL I.E only the IP layer or in case of ETH-TNL the Ethernet part as well.

6.1.2.2 MPLS protocol stack

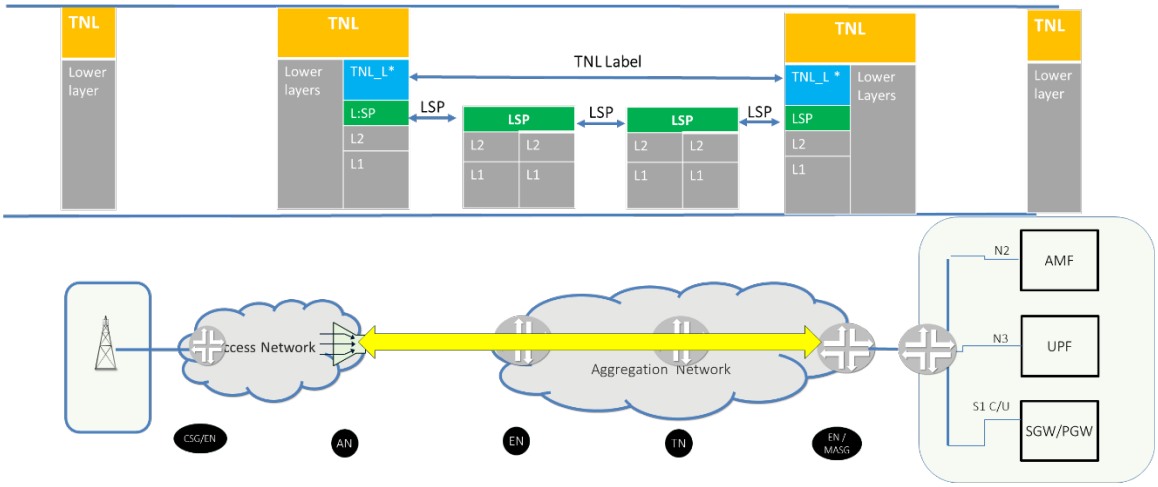
This section shows the protocol stacks used in the access and aggregation network nodes to transport the TNL for each MPLS deployment scenario.



TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label
for IPoMPLS – no label(empty)

Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

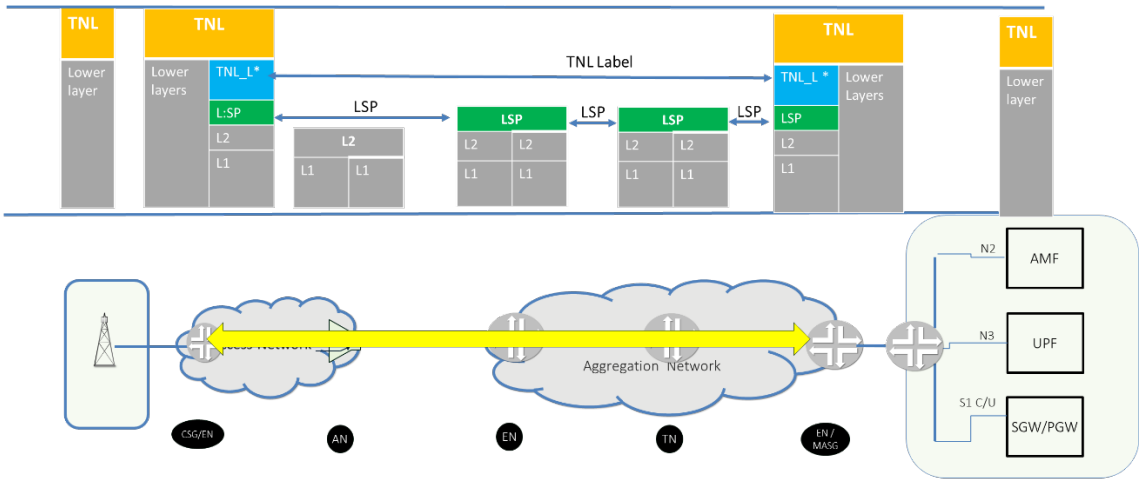
Figure 6.10: Protocol stacks used for TNL Transport in Use Case a



TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label
for IPoMPLS – no label(empty)

Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

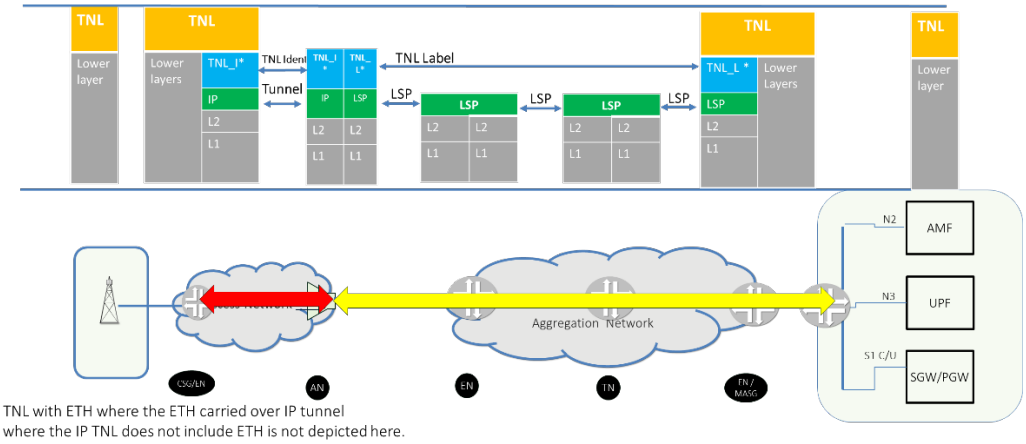
Figure 6.11: Protocol stacks used for TNL Transport in Use Case b



TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label
for IPoMPLS – no label(empty)

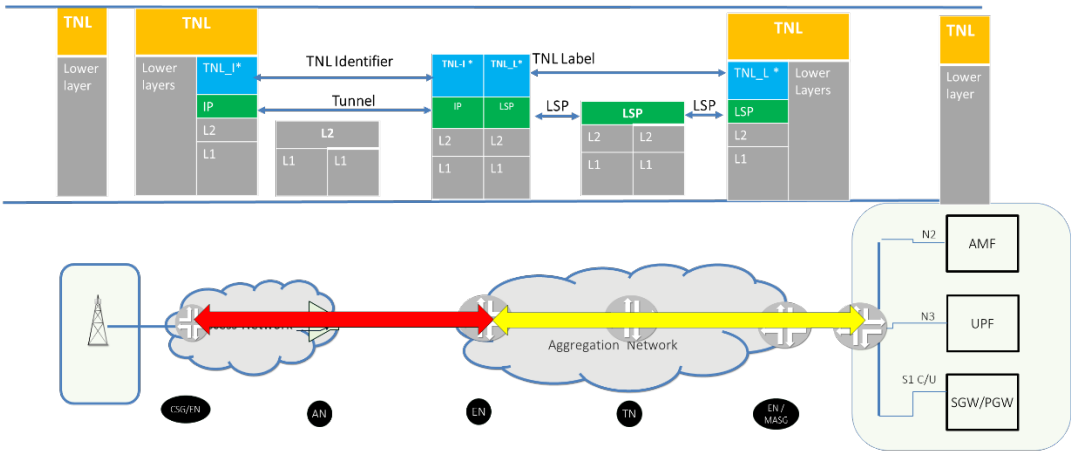
Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

Figure 6.12: Protocol stacks used for TNL Transport in Use Case c



The figure depicts a case of IP TNL with ETH where the ETH carried over IP tunnel
Note : the case of IP over ETH where the IP TNL does not include ETH is not depicted here.
TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label- No label empty
for IPoMPLS – no label(empty)
TNL-I : TNL Identifier per tunnel technology
LSP - stack of labels
Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

Figure 6.13: Protocol stacks over IP access and MPLS aggregation used for TNL Transport in Use Case d



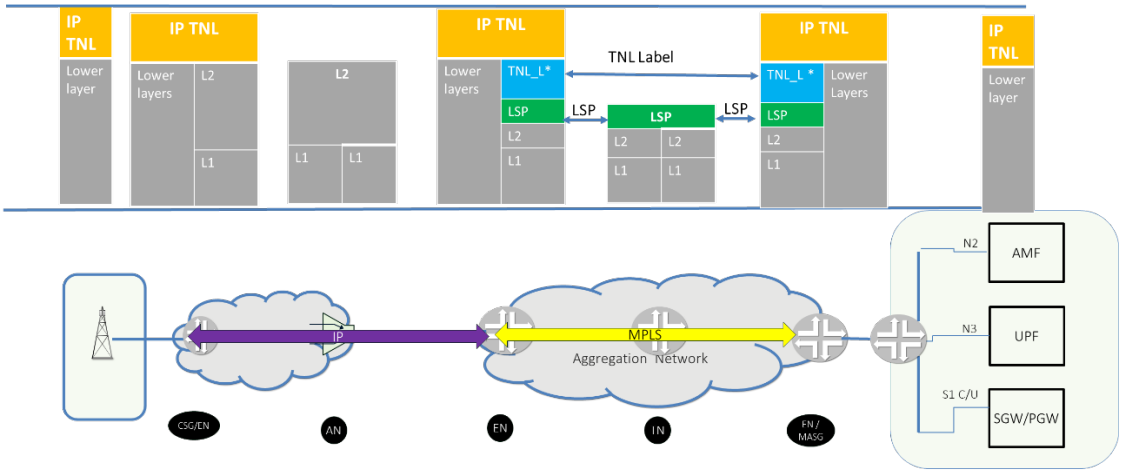
The figure depicts a case of IP TNL with ETH where the ETH carried over IP tunnel
Note : the case of IP over ETH where the IP TNL does not include ETH is not depicted here.
TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label- No label empty
for IPoMPLS – no label(empty)
TNL-I : TNL Identifier per tunnel technology
LSP - stack of labels
Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

Figure 6.14: Protocol stacks over IP access and MPLS aggregation used for TNL Transport in Use Case e

6.1.2.3 IP protocol stack

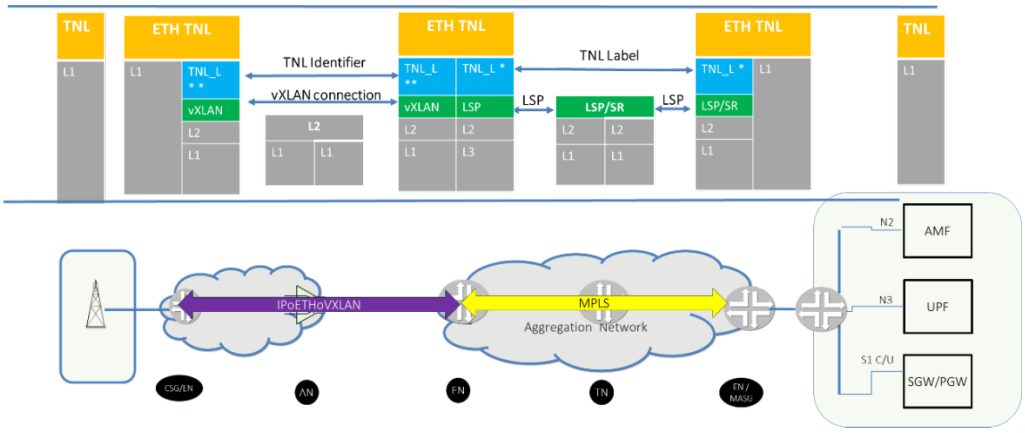
The CSG only can carry TNL over IP with 2 use cases either the TNL includes only the IP part or the TNL includes also the Ethernet part.

The following drawing depicts the 2 encapsulations:



TNL-L* means TNL specific label (if any) for Ethernet PW
for L3 VPN- label
for IPoMPLS – no label(empty)
Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1

Figure 6.15: Protocol stacks over Ethernet at the access network used for TNL that includes IP only Transport



TNL-L* means TNL specific label (if any) for Ethernet PW
TNL-L ** TNL specific Label in vXLAN (VNI)
Lower Layer means layers carrying TNL For Ethernet – L1
For IP L2 + L1
ETH TNL – TNL that include the gNB Ethernet frame

Figure 6.16: Protocol stacks over IP at the access network used for TNL that includes Ethernet Transport

7 Generic specification (Equipment Specifications/Requirements)

7.1 Requirements over MPLS (L2VPN, L3VPN, EVPN) connectivity

7.1.1 Signaling and Routing

[R-1] If the PE supports EVPN it must support requirements in section 11 of TR-350 Issue 2 [5].

7.1.1.1 PSN Tunnel LSP signaling

[R-2] PE and P routers supporting MPLS TE and non-TE LSPs as well as MPLS SR MUST support one or both of the following methods:

- Static provisioning
- Dynamic signaling

[R-3] Both of the following methods MUST be supported by PE and P routers for dynamically signaled PSN tunnel LSPs.

- LDP is used to set up, maintain and release LSP tunnels per IETF RFC 5036 [25].
- RSVP-TE is used to set up, maintain and release LSPs for traffic engineered tunnels per IETF RFC 3209 [26] and RFC 5151 [46]. When traffic engineering is needed on the LSP, RSVP-TE MUST be used.
- If RSVP-TE is used, the encoding MUST comply with Encoding of Attributes for MPLS LSP Establishment Using Resource Reservation Protocol Traffic Engineering (RSVP-TE) as described in RFC 5420 [94]

[R-4] If segment routing is supported then the PE routers MUST support IETF RFC 8666 [42] for LSP signaling

[R-5] If segment routing is supported then the PE routers MAY support IETF RFC 8667 [43] for LSP signaling

[R-6] If segment routing is supported then the PE SHOULD support IETF RFC 8661 [85] for segment routing MPLS interworking with LDP

[R-7] When co-routed bidirectional LSPs are required, GMPLS-RSVP-TE as per IETF RFC 3473 [27] MAY be supported by PE and P routers.

7.1.1.2 Multi-area LSP Signaling

Section 5.1 of TR-221 [1] domain TE LSPs. The following text provides different options of RSVP-TE LSPs and LDP LSPs Multi-area signaling support.

7.1.1.2.1.1 Multi-area RSVP-TE Signaling

Inter-domain TE LSPs can be supported by the following option as specified in RFC 5151 [46]: contiguous LSPs.

A contiguous TE LSP is a single TE LSP that is set up across multiple domains using RSVP-TE signaling procedures described in Section 5.1.1/ TR-221 [1].

7.1.1.2.1.2 Multi-area LDP Signaling

RFC 5283 [28] facilitates the establishment of Label Switched Paths (LSPs) that would span multiple IGP areas in a given Autonomous System (AS).

[R-8] PE and P routers SHOULD support establishment of inter-area LSPs using LDP s per RFC 5283 [28].

[R-9] If GMPLS is support, OSPF extensions in support of GMPLS as per RFC 4203 [92] MUST be supported.

[R-10] If GMPLS is supported, ISIS extensions in support of GMPLS as per RFC 5307 [93] MAY be supported.

.

7.1.1.3 PSN Tunnel LSP routing

[R-11] One or both of the following methods MUST be used when dynamic signaling is supported by PE and P routers:

- Static routing
- Dynamic routing

[R-12] If dynamic routing is supported, all of the following methods MUST be supported by PE and P routers to exchange routing information to facilitate dynamic LSP signaling:

- OSPFv2 (IETF RFC 2328 [29])
- OSPFv3 (IETF RFC 5340 [30])
- IS-IS (IETF RFC 1195 [31])
- IS-IS for IPv6 (IETF RFC 5308 [32])

[R-13] Traffic engineering extensions of OSPF and IS-IS are used to exchange traffic attributes for RSVP-TE tunnels. If TE is supported, both of the following methods MUST be supported by PE and P routers:

- OSPF-TE (IETF RFC 3630 [33])
- OSPF-TEv6 (IETF RFC 5329 [34])
- OSPF-TE metric extension (IETF RFC 7471 [86])
- IS-IS-TE (IETF RFC 5305 [35])
- IS-IS-TE metric extension (IETF RFC 8570 [87])

[R-14] If segment routing is supported, then the PE routers MUST support IETF RFC 8666 [42] for routing.

[R-15] If segment routing is supported, then the PE routers MAY support IETF RFC 8667 [43] for routing.

[R-16] If segment routing is supported, then the PE routers MAY support IETF RFC 8669 [89] for routing.

[R-17] If segment routing is supported, then the PE routers MUST support IETF RFC 8491 [89] for advertisement of MSDs (maximum SID depth) using IS-IS extensions.

7.1.1.4 PW signaling

[R-18] One or both of the following methods MUST be used for PWs:

- Static provisioning
- Dynamic signaling

[R-19] PE routers MUST support Single Segment Pseudowire (SS-PWs) as per IETF RFC 3985 [36].

[R-20] PE and P routers SHOULD support static provisioned Multi-Segment Pseudowire (MS-PW) as per IETF RFC 6073 [37]

When PE and P routers support Dynamic signaled PWs the following apply: MUST support pseudowire setup, maintenance and release of PWs as per IETF RFC 4447 [38]with FEC 128

[R-21] SHOULD support pseudowire setup, maintenance and release of PWs as per IETF RFC 4447 [38] with FEC 129

If an implementation supports IP-MPLS 22.0.0 [7] “BGP auto-discovery and signaling for VPWS-based VPN services” which provides specification for setup of VPWS pseudowires with BGP the following requirements apply.

[R-22] PE routers SHOULD support one or more of the following encapsulation type values from IP-MPLS 22.0.0 [7]

- For Ethernet over MPLS (IETF RFC 4448 [41]) the Encapsulation Type is 4 or 5 as per IP-MPLS 22.0.0 [7] Section 8.5.
- For TDM TNL (RFC 4553 [47] or RFC 5086 [48]) the Encapsulation Type is per IP-MPLSF 22.0.0 [7] Section 8.5

Any difference from the above requirements for specific TNLs is identified in the specific TNL PW signaling section and takes precedence on these requirements.

7.1.2 Forwarding

[R-23] The PE MUST support IPv4/IPv6 dual stack functionality.

[R-24] The PE MUST support forwarding IPv4traffic.

[R-25] The PE MUST support forwarding IPv6 traffic.

[R-26] If segment routing is supported then PE routers MUST support Segment Routing with MPLS data plane as per IETF RFC 8402 [51].

7.1.3 OAM

7.1.3.1 LSP OAM

As defined in TR-221 [1] section 5.2.1. See clarification on TR-221 Corrigendum 1 [3] section 3.2.

7.1.3.2 PW OAM

As defined in TR-224 [82] section 8.2.3.

7.1.3.3 Packet Loss and Delay Measurement

As defined in TR-221 [1] section 5.2.4 and TR-224 [82] Section 8.2.4.

7.1.3.4 MEF Service OAM

As defined in TR-224 [82] Section 8.1.2.

7.1.4 Resiliency

TR-221 [1] section 5.3 defines resiliency in the mobile networks.

7.1.4.1 Link Resiliency at Layer 2

As defined in TR-221 [1] section 5.3.2.

7.1.4.2 LSP Resiliency

As defined in TR-221 [1] section 5.3.3.

Loop free alternates (LFA) As defined in TR-221 Amendment 2 [2] section 3.3

7.1.4.3 Pseudowire resiliency

As defined in TR-221 Amendment 1 [4] section 3.4.

VRRP protection as per TR-221 [1] section 5.3.4.1.

7.1.5 QoS

As defined in TR-221 [1] section 5.4 and TR-224 [82] Section 9.

7.1.5.1 Tunnel CoS Mapping and marking

As defined in TR-221 [1] section 5.4.1 and TR-224 [82] Section 9.1.

7.1.5.2 PW CoS Mapping and marking

As defined in TR-221 [1] section 5.4.2 and TR-224 [82] Section 9.2.

7.1.6 Security requirements

As defined in TR-221 [1] section 5.6 and TR-224 [82] Sections 3.3, 11.1.10, 12.1.14, and 13.1.14.

7.2 Requirements over IP connectivity

IP connectivity can be implemented in several ways:

- IP or Ethernet over IP tunnel (VXLAN, GRE.)
- IP over VLAN
- IP over Ethernet

7.2.1 QoS

The MPLS mobile backhaul network has to provide QoS and service level agreements. The QoS capabilities must be end to end, which includes both ACs and mobile BH domains. In this case the access domain is IP and the Aggregation and Core domains are MPLS. Usually, a mobile backhaul network will support guaranteeing sufficient bandwidth is available to support new and existing connections conforming to all SLA metrics including protection mechanisms.

[R-27] The PE(CSG) MUST support a configurable mechanism to ensure CoS starvation prevention.

7.2.2 Connectivity over IP Tunnel

As shown in Figure x3, the CSG and AN/EN can be IP Tunnel End Points, performing the encapsulation/decapsulation of mobile traffic in IP tunnel.

7.2.2.1 Connectivity over VXLAN tunnel

If the IP tunnel is VXLAN IETF RFC 7348 [39] then, a unique VXLAN Network Identifier (VNI) is assigned per CSG by the service provider and used in the VXLAN tunnel encapsulation between the CSG and the AN/EN. While using a control plane for VXLAN (e.g., EVPN) is possible and even highly desirable in some environments, using VXLAN in the access network focusses on point-to-point.

7.2.2.2 Connectivity over VLAN

Each VLAN represents VRF #. In case of CSG connection to the PE via aggregator 2 VLANS might be used one to designate the CSG and the other to designate the VRF.

7.2.2.3 IP over Ethernet

In case of direct connection between the PE to the CSG the interface can be Ethernet Tagged or untagged. In case there is an aggregator between the CSG and the PE.

Each CSG might be connected with a different VLAN to the PE port.

8 Specification for ETH TNL scenario

The architecture and requirements for the ETH TNL support are specified per TR-224 [82] for VPLS and per TR-350 Issue 2 [5] for EVPN. These detail how to provide an Ethernet service such as EPL or EVPL.

9 Specification for IP TNL scenario

9.1 IP connectivity

From 3GPP R5, IP can be used as TNL. IP can be carried over different types of L2 protocols: Ethernet, ML-PPP, etc. Currently RAN equipment vendors are implementing Ethernet ports on RAN and mobile Core equipment (e.g., Gigabit Ethernet), so Ethernet will be largely deployed to support IP TNL. IP TNL can be directly transported on L3VPN or routed IP over LSPs when L3 transport solutions are used in the mobile backhaul network.

For 5G, IP is the unique Transport Network Layer specified to transport mobile flows between gNBs and mobile Core nodes in order to support logical mobile interfaces defined by 3GPP. Details on the IP connectivity requirements for specific 3GPP interfaces, e.g., N3, 2, 6, 4, and N9, are given in Figure 5.1. Different Solutions MPLS based or none MPLS based, can be used to transport IP TNL in the mobile backhaul network and its different segments: L2VPN MPLS (e.g., VPWS, VPLS, H-VPLS), L3VPN MPLS and RSVP-TE MPLS LSP, EVPN, Pure IP connectivity that are described hereafter.

9.2 Specification for IP TNL over MPLS L2VPN/L3VPN EVPN and IP over MPLS

9.2.1 IP and Ethernet QoS

As defined in TR-221 [1] section 8.2.

9.2.2 L2VPN MPLS solutions

As defined in TR-224 [82] section 9.

9.2.3 EVPN MPLS solutions

As defined in TR-350 Issue 2 [5] section 7.14.

9.2.4 L3VPN MPLS solutions

As defined in TR-221 [1] section 8.4.

9.2.5 IP over LSPs

As defined in TR-221 [1] section 8.5.

9.2.6 IPV6 Requirements

9.2.6.1 IPv6 TNL support in an IPv4 MPLS MBH network

As defined in TR-221 [1] section 5.5.1.

9.2.6.2 IPv6 TNL support in an IPv6 MPLS MBH network

As defined in TR-221 [1] Section 5.5.2.

9.2.6.3 IPv4 TNL support in an IPv6 MPLS MBH network

As defined in TR-221 [1] Section 5.5.2.

9.3 Specification for IP TNL over IP connectivity

9.3.1 IP and Ethernet QoS

As defined in TR-221 [1] section 8.2.

9.3.2 IP and Ethernet over IP tunneling

Due to the fact that the access network is defined as Layer 2 network, the following applies:
If the PE supports IP TNL over IP connectivity then:

[R-28] The PE MUST support Ethernet over IP tunnel

[R-29] The PE MAY support IP over IP tunnel.

9.3.2.1 Routing

[R-30] One or both of the following methods MUST be used by PE and P routers:

- Static routing
- Dynamic routing

[R-31] If dynamic routing is supported, all of the following methods MUST be supported by PE and P routers to exchange routing information:

- OSPFV2 (IETF RFC 2328 [29])
- IS-IS (IETF RFC 1195 [31])
- OSPFv3 (IETF RFC 5340 [30])
- IS-IS for IPv6 (IETF RFC 5308 [32])
- BGP-4 (IETF RFC 4271 [40])

9.3.2.2 QoS

QoS as defined in section 7.2.1.

9.3.2.3 Tunnel CoS Mapping and marking

[R-32] The PE MUST support CoS marking in the DSCP bits of the IP tunnel.

[R-33] The PE MUST support CoS mapping between the QoS of TNL and DSCP bits of the IP tunnel.

9.3.2.4 Ethernet and IP over VXLAN tunnel

Virtual Extensible LAN (VXLAN) is a network virtualization technology that uses a VLAN-like encapsulation technique to encapsulate Ethernet in IP. As a result, IP over VXLAN is effectively IP over Ethernet over IP.

The following requirements apply to the CSG when using VXLAN IETF RFC 7348 [39] tunnels for IP connectivity:

[R-34] The CSG MUST support VXLAN tunnels

[R-35] The CSG MUST support VXLAN tunnels using IPv4 encapsulation.

[R-36] The CSG SHOULD support VXLAN tunnels using IPv6 encapsulation.

[R-37] The CSG MUST support bridging Ethernet frames into a VXLAN tunnel.

[R-38] The CSG MUST support using the tunnel settings in Table 9.1.

[R-39] The CSG MUST support static provisioning of VXLAN tunnel settings

[R-40] Upon receiving downstream encapsulated traffic from the AN/EN, the CSG MUST:

- Decapsulate VXLAN
- If the Protocol Type in IP header is UDP (0x11) and the UDP Destination Port is 4789, then it must process the 802.3 frame following the VXLAN header.
- The frame should be forwarded per the MAC forwarding table, if matching the VNI configured for the VXLAN tunnel.

The following requirements apply to the AN/EN when using VXLAN tunnels for the IP connectivity:

[R-41] The AN/EN MUST support stateless VXLAN tunnels

[R-42] The AN/EN MUST support stateless VXLAN tunnels using IPv4 encapsulation.

[R-43] The AN/EN SHOULD support stateless VXLAN tunnels using IPv6 encapsulation.

[R-44] The AN/EN MUST support bridging Ethernet frames into a VXLAN tunnel.

[R-45] The AN/EN MUST support using the tunnel settings in Table 9.1.

[R-46] The AN/EN MUST support static provisioning of VXLAN settings.

[R-47] The AN/EN SHOULD support dynamically learning the VXLAN tunnel settings from encapsulated packets received from the CSG. Learned encapsulation is then used on downstream traffic to the CSG.

[R-48] Upon receiving upstream encapsulated traffic from the CSG, the AN/EN MUST:

- Decapsulate VXLAN
- If the Protocol Type in IP header is UDP (0x11) and the UDP Destination Port is 4789, then it must process the 802.3 frame following the VXLAN header.
- The frame should be forwarded to the selected AN/EN for this CSG, based on the VNI.

Table 9.1 describes the values that should be set in each of the headers of the VXLAN encapsulation in the VXLAN tunnel.

Table 9.1: VXLAN tunnel settings

Header Field	Value
Source IP address	**CSG to AN/EN**: CSG WAN IP **AN/EN to CSG**: AN/EN WAN IP
Destination IP address	**CSG to AN/EN**: AN/ENWAN IP **AN/EN to CSG**: CSG WAN IP
IP Protocol Type / Next-Header	UDP (0x11)
Source UDP Port	Configurable (4789 recommended)
Destination UDP Port	4789
VXLAN Network Identifier	Configurable (one per enterprise)
Source MAC address	**CSG to AN/EN: CSG MAC Address** **AN/EN to CSG: AN/EN MAC address**
Destination MAC address	**CSG to AN/EN: AN/EN MAC address** **AN/EN to CSG: CSG MAC address** **In both cases, the broadcast MAC is used for broadcast traffic, e.g., for ARPs**

9.3.2.5 IP Over VXLAN Tunnel

Routing as defined in section 9.3.2.1.

QoS as defined in section 9.3.2.2.

The IP packet is carried over VXLAN by encapsulating the packet with an Ethernet Header inside a VXLAN header added by the VXLAN ingress device.The Ethernet header is removed at the VXLAN Egress device.

[R-49] The PE MUST use the Ethernet source address that is associated with the VXLAN ingress device in the Encapsulating Ethernet Header.

[R-50] The PE MUST use The Ethernet destination address that is associated with the VXLAN egress device in the Encapsulating Ethernet Header.

9.3.2.6 Ethernet over VXLAN

Routing as defined in section 9.3.2.1.

QoS as defined in section 9.3.2.2.

9.3.2.7 Qos

The following capabilities are to be supported by the PEs (CSGs) supporting IP connectivity for IP TNL using Ethernet:

[R-51] The PE(CSG) MUST support ingress bandwidth profile based on MEF 10.3 [19].

[R-52] The PE(CSG) MUST support at least 4 CoS and associated service metrics (e.g., delay, delay variation, packet loss) as defined in MEF 22.3 “EVC Requirements” [20].

[R-53] The PE(CSG) SHOULD support Connection Admission Control to guarantee sufficient bandwidth is available to support new connection conforming to all SLA metrics defined in MEF 22.3 [20] Section 10.3 [19].

Section 4.7/ IETF RFC 4448 [41]specifies the QoS considerations.

[R-54] The ingress PE(CSG) MUST map the PCP (in the PRI field of the IEEE 802.1Q [8] VLAN tag) into DSCP field of the IP tunnel.

[R-55] For support of PTP synchronization over the Ethernet, the network MUST support the synchronization performance metrics defined in “Performance for Synchronization Traffic Class” by MEF 22.3 [20].

It is assumed that QoS markings are mapped from higher layers to lower or encapsulation layers.

Note: Mapping based on higher layer QoS settings (e.g., DSCP, etc.) may be also used.

9.3.2.8 OAM

9.3.2.8.1 Underlay OAM

9.3.2.8.1.1 Continuity check

The CSG monitors the state of its connectivity to the access node / Edge node, as depicted in cases d and e, based on BFD RFC 5880 [44] mechanism.

[R-56] The CSG MUST support monitoring the status of the underlay network using BFD.

[R-57] The CSG MUST support single-hop BFD per RFC 5881 [45] [3x] mandatory features.

[R-58] The CSG MUST support BFD asynchronous mode per RFC 5880 [44].

[R-59] The CSG MUST support a single BFD session per to a specific Access node / PE at the POP/CO IP address.

9.3.2.8.1.2 Performance monitoring

Mobile services normally have SLAs. Hence support for Performance Monitoring is mandatory.

The CSG MUST support measuring the performance between the CSG and the Access node or the Edge node as depicted in

[R-60] Figure 5.3 cases d and e. The CSG MUST support measuring the performance between a CSG and other CSG.

TWAMP Light (TWL), an IP OAM tool described in RFC 5357 [49], Appendix I, shall be used for measuring the performance between any two CSGs, as well as between a CSG and the edge node.

[R-61] The CSG MUST support acting as a TWL Session-Reflector as per Section 6.1/TR-390 [6].

[R-62] The CSG MUST support static provisioning of the TWL Session-Reflector as defined in section 5/TR-390 [6].

[R-63] The CSG MUST support acting as a TWL Session-Sender as defined section 6.2/TR-390 [6].

[R-64] The CSG MUST be able to mark the DSCP field in the IP packet per the class of service measured.

9.3.2.8.2 Overlay OAM

The mobile operator may use Ethernet Services to connect the CSG and the MASG. In that case, the mobile operator must be able to manage this form of Mobile Backhaul using Service OAM, and the following requirements apply:

[R-65] [The CSG MUST support MEF service OAM as defined in TR-221 [1] section 5.2.5 and TR-224 [82] Section 8.1.2.

9.3.2.9 Resiliency

For mobile networks, resiliency is the ability to maintain the required levels of service for both inelastic and elastic traffic when there are temporary or permanent failures in that network. This section describes requirements to ensure resiliency over the access network between the CSG and the Access node / Edge node for the case of transferring Ethernet over IP tunnel.

While the traffic is inherently bidirectional, failures may be related to a specific traffic direction. In the following we will generally discuss traffic in the CSG to Access Node / Edge node direction, and the reader will understand that the opposite direction needs to be similarly addressed.

9.3.2.10 Scope of resiliency

In this section “resiliency” means protection switching (IP tunnel (underlay network), or L2 link protection) between the Access Node / Edge Node and the CSG, Resiliency in this specification does not cover L1 protection switching.

If protection mechanisms are available at multiple layers, careful consideration should be given to setting of the relevant timer values. For such cases, guidance can be derived from Section 3.5/RFC 3386 [50], which

states: “Multilayer interaction is addressed by having successively higher multiplexing levels operate at a protection / restoration time scale greater than the next lowest layer".

Hence, if L1 or L2 protection is available in addition to IP protection, the PE must be able to delay its actions sufficiently for lower layer protection methods to succeed. Whenever possible, protection switching at the layers underneath the tunnel should be transparent to the IP layer. The specific algorithm of protection switching implemented at each node is beyond the scope of this specification.

9.3.2.10.1 Link resiliency at layer 2

As per TR-221 [1] section 5.3.2.

9.3.2.10.1.1 Connectivity monitoring by the CSG

The CSG needs to monitor the underlay network as per section 9.3.2.8.1.1 “Continuity check”.

9.3.2.10.1.2 Protection mechanism

As per failure detection

[R-66] The CSG MUST support re-establishing the path continuity over a backup access link.

[R-67] The CSG SHOULD restore traffic flow within 250 milliseconds after receipt of failure notification.

When the failed access link comes back online, and is once again capable of providing underlay path continuity, it is a matter of policy whether to re-establish the tunnel over the primary access link or to keep using the backup.

[R-68] The CSG MUST support resiliency revertive mode.

[R-69] The CSG MUST support resiliency non-revertive mode.

[R-70] The CSG MUST support setting of the resiliency revert mode based on configuration and/or policy.

9.3.2.11 Security

[R-71] The PEs MUST support the following capabilities for VPN security:

- General VPN security per Section 4.5/RFC 3809 [76] and RFC 4111 [80].
- L2VPN security per Section 6/RFC 4761 [22] and Section 14/RFC 4762 [21].
- L3VPN security per Section 13/RFC 4364 [24].
- Encapsulation MPLS in IP (for the IP part) Section 8/RFC 4023 [84]

If the PE supports VXLAN tunnel

[R-72] The PE MUST support Section 7/ RFC 7348 [39]

9.3.2.12 IPSEC Requirements

[R-73] The PE MAY support peer to peer IPSec VPN, as defined in IETF RFCs 4301 [77], 4303 [79], 7296 [81].

[R-74] If the PE supports IPSec VPN, it MUST support encapsulating security payload (ESP), as defined in IETF RFC 4303 [79].

[R-75] If the PE supports IPSec VPN, it MUST support the IKEv2 key exchange protocol as defined in RFC 7296 [81].

[R-76] If the PE supports IPSec VPN, it MUST support IPSec VPN in tunnel mode, which is defined in section 3.2 of RFC 4301 [77].

[R-77] If the PE supports IPSec VPN, it MUST support dead peer detection (DPD), which is defined in RFC 7296 [81].

[R-78] If the PE supports IPSec VPN, it MUST support that the destination address in the IPSec is configured to be either an IP address or a dynamic domain name.

[R-79] If the PE supports IPSec VPN, it MUST support querying the status of child security associations (SA) from the Controller extension.

[R-80] The PE MUST support the following encryption types:
- AES_CBC Encryption
- AES_GCM_16 Encryption
- No Encryption (NULL)

as per RFC 8221 [90] section 5

[R-81] The PE SHOULD support the following encryption types:
- AES_CCM_8
- CHAHA20_POLY1305

as per RFC 8221 [90] section 5.

[R-82] The PE MUST support the following authentication types:
- SHA_256_2 SHA1_96 authentication

as per RFC 8221 [90] section 6.

[R-83] The PE SHOULD support the following authentication types:
- SHA2_521_256 authentication

as per RFC 8221 [90] section 6

[R-84] The PE MUST NOT support authentication using Message Digest 5 (MD5) IP over Ethernet No tunnel

9.3.2.13 IP over VLAN

Routing as defined in section 9.3.2.1.

QoS as defined in section 9.3.2.2.

9.3.2.14 CoS Mapping and marking

[R-85] The PE MUST support CoS marking in the PCP (in the PRI field of the IEEE 802.1Q [8] VLAN tag) VLAN of the VRF VLAN and Provider VLAN if (exist).

[R-86] The PE MUST support CoS mapping between the QoS of TNL and the PCP (in the PRI field of the IEEE 802.1QVLAN tag [8]) VRF VLAN and provider VLAN (if exist).

9.3.2.15 OAM

9.3.2.15.1 Continuity check

The CSG monitors the state of its connectivity to the access node / PE at the POP/CO based on BFD RFC 5880 [44] mechanism.

[R-87] The CSG MUST support monitoring the status of the IP network using BFD.

As required in section 9.3.2.8.1.1, the CSG needs to support requirements R50 – R53.

9.3.2.15.2 Performance monitoring

Mobile services normally have SLAs. Hence support for Performance Monitoring is mandatory.

As required in section 9.3.2.8.1.2 the CSG needs to support requirements [R-60] - [R-64]

9.3.2.16 Resiliency

For mobile networks, resiliency is the ability to maintain the required levels of service for both inelastic and elastic traffic when there are temporary or permanent failures in that network. This section describes requirements to ensure resiliency over the access network between the CSG and the Access node / Edge node for the case of transferring N3 interface over IP network.

While the traffic is inherently bidirectional, failures may be related to a specific traffic direction. In the following we will generally discuss traffic in the CSG to Access Node / Edge node direction, and the reader will understand that the opposite direction needs to be similarly addressed.

9.3.2.16.1 Scope of resiliency

In this section, “resiliency” means protection switching (IP network or L2 link protection) between the Access Node / Edge Node and the CSG, Resiliency in this specification does not cover L1 protection switching.

If protection mechanisms are available at multiple layers, careful consideration should be given to setting of the relevant timer values. For such cases, guidance can be derived from Section 3.5/RFC 3386 [50], which states: “Multilayer interaction is addressed by having successively higher multiplexing levels operate at a protection / restoration time scale greater than the next lowest layer".

Hence, if L1 or L2 protection is available in addition to IP protection, the PE must be able to delay its actions sufficiently for lower layer protection methods to succeed. Whenever possible, protection switching at the

layers underneath the tunnel should be transparent to the IP layer. The specific algorithm of protection switching implemented at each node is beyond the scope of this specification.

9.3.2.16.2 Link resiliency at layer 2

As per TR-221 [1] section 5.3.2.

9.3.2.16.3 Connectivity monitoring by the CSG

The CSG needs to monitor the tunnels as per section 9.3.2.8.1.1 “continuity check”.

9.3.2.16.4 Protection mechanism

As per failure detection

[R-88] The CSG MUST support re-establishing the path continuity over a backup access link.

[R-89] The CSG SHOULD restore traffic flow within 250 milliseconds after receipt of failure notification.

When the failed access link comes back online, and is once again capable of providing IP network path continuity, it is a matter of policy whether to re-establish the IP connection over the primary access link or to keep using the backup IP connection.

[R-90] The CSG MUST support resiliency revertive mode.

[R-91] The CSG MUST support resiliency non-revertive mode.

[R-92] The CSG MUST support setting of the resiliency revert mode based on configuration and/or policy.

9.3.2.17 Security

[R-93] The PEs MUST support the following capabilities for VPN security:
- General VPN security per Section 4.5/RFC 3809 [76] and RFC 4111 [80].
- L3VPN security per Section 13/RFC 4364 [24].

9.3.2.18 IPSEC Requirements

As per section 9.3.2.12 in this document.

9.3.3 Flat IP no tunneling

Routing as defined in section 9.3.2.1.

QoS as defined in section 9.3.2.2.

9.3.3.1 OAM

9.3.3.1.1 Continuity check

The CSG monitors the state of its connectivity to the access node / PE at the POP/CO based on BFD RFC 5880 [44] mechanism.

As required in section 9.3.2.8.1.1, the CSG needs to support requirements [R-56] [R-59].

9.3.3.2 Performance monitoring

Mobile services normally have SLAs. Hence support for Performance Monitoring is mandatory.

As required in section 9.3.2.8.1.2 the CSG needs to support requirements R54 - R58

9.3.3.3 Resiliency

As defined in section 9.3.2.9 Security

[R-94] The PEs MUST support the following capabilities for VPN security:

- General VPN security per Section 4.5/RFC 3809 [76] and RFC 4111 [80].
- L3VPN security per Section 13/RFC 4364 [24].

9.3.3.4 IPSEC Requirements

As per section 9.3.2.12 in this document.

10 Auto configuration (Zero touch)

In order to automate the deployment process, the CSG should support Auto configuration / zerotouch process. For zerotouch (IETF RFC 8572 [83]) a CSG needs to use Dynamic Host Configuration Protocol (DHCP) to determine the IP address of an EMS or SDN controller. The CSG then connects to this IP address and an exchange of configuration information occurs between the CSG and an EMS or SDN controller.

If Zero touch is supported then:

[R-95] The CSG MUST support Zero touch process as defend in IETF RFC 8572 [83].

11 Network Slicing

From the perspective of the CSG/MASG, which is not aware of mobile slices, only the transport slices exist. The CSG/MASG needs to classify traffic and map it to a specific transport slice matching the correct SLA. This mapping can be provided either by a management interface to the CSG/MASG or by a signaling protocol. The interfaces between the 3GPP Management System and the Transport Network (TN) is out of scope for this document. This document assumes that networks are capable of providing per slice service behavior bounds, including confidence in delivering those bounds, all dependent on careful design of the network traffic.

It should be noted that the relationship between the network slice and the transport is not necessarily a 1:1 relationship. For example, MEF 22.3.1 [54] indicates that this mapping of mobile slices to an EVC (i.e., transport slice in this document) can by N:1 or 1:1.

As described in IETF draft-ietf-teas-ietf-network-slices [91], the IETF network slice (i.e., transport slice in this document) is an abstract topology connecting a set of endpoints, with shared or dedicated resources to satisfy customer's SLO requirements. The transport slice is technology agnostic, but to realize it in underlying network should be technology specific. The requirements for realization of network slice may include: (1) path computation to create network topology as customer's intent (e.g., low-latency, high-bandwidth, high-reliability, etc.); (2) necessary network resource reservation (including network, computing and storage resource); (3) network abstraction for exporting abstract network topology to upper layer, (4) network performance measuring, etc.

This document specifies the following MPLS-based transport methods with or without Segment Routing:

- L2VPN,
- L3VPN,
- E-VPN,
- IP over MPLS

and the following IP-based transport methods:

- IP and Ethernet over IP tunneling – VXLAN
- IP over Ethernet / VLAN no tunnel

The technologies listed above may be used to address the general requirements below.
VPN can provide separate services as overlay, the underlay network which can be divided into separate virtual networks using some protocols (such as MPLS-TE, RSVP-TE, SR, SR-TE, etc.), but the network topology with SLO (e.g., guaranteed latency, guaranteed bandwidth, etc.) requirements and dedicated or shared network resource reservation requirements for transport slice, may not be satisfied for all use cases. The extension to existing IGP or MPLS, SR technology may be needed, and deterministic technology (e.g., DetNet) may be used in combination.

The requirements for CSG:

[R-96] The CSG MUST be able to accept classification for F1-U or N3 packets from its EMS.

[R-97] The CSG SHOULD be able to accept classification for F1-U or N3 packets from a signaling protocol.

[R-98] The CSG MUST be able to map frames accepted from F1-U and N3 interfaces to the transport network based on the above methods.

12 Network Synchronization

12.1 Frequency Distribution Scenarios over mobile backhaul networks

This section provides frequency distribution solutions required for mobile networks. The base station air interface synchronization requirements are specified in 3GPP (UE to BS interface). If the synchronization reference is provided by the network, the related network synchronization requirements are defined in ITU-T. IP/MPLS.20.0.0 [7], Section 7.11.1.1, presented three prevalent scenarios for frequency distribution in mobile networks. The remainder of this section expands on those scenarios and how they may be deployed. Unless specifically stated, the rest of the text will focus on supplying the base-station required frequency reference accuracy to meet its RF transmission requirements. Another distinction that will also be made in the following text is between physical-layer frequency distribution methods and packet-based (higher-layer) distribution methods. The first uses the physical-layer symbol-rate to distribute the frequency information while the latter does it using a dedicated flow of packets. The frequency distribution scenarios were devised based on the following principals:

(1) When a mixture of physical-layer and packet-based methods is used, the packet-based frequency distribution always extends the physical-layer frequency distribution and never the other way around.
(2) The only exceptions to (1) are:
    (i) At the last-mile (link between the access node and the CSG) where a packet-based to physical-layer frequency conversion is possible in order to support various lastmile frequency distribution technologies (such as NTR in DSL or downstream frequency distribution in xPON).
    (ii) At the, usually short distance, link between the CSG and the BS where various short-distance or intra-office frequency distribution connections might be used (e.g., a 2.048MHz physical clock over a coax cable).
(3) The frequency reference is generally a PRC complying to ITU-T G.811 [62].
(4) The fundamentals and specifics of the physical-layer or packet-based frequency distribution are outside the scope of this document.

12.2 Distribution using physical-layer methods

The fundamentals and specifics of the physical-layer frequency distribution are outside the scope of this document. For examples of End Distribution using physical-layer methods please refer to Appendix B TR-221 [1].

12.2.1 Distribution using packet-based methods

All mobile radio networks such as GSM, WCDMA, and LTE etc. require frequency synchronization to maintain spectral efficiencies and seamless handover characteristics over the air interface. Transport of frequency information using packets provides an alternative way to distribute frequency information when physical-layer frequency distribution means are not possible. All together three different major technologies of packet-based frequency distributions can be identified: TDM PW supporting frequency distribution, the Network Time Protocol (NTP) and the Precision Time Protocol (PTP). These methods use the principles of adaptive clock recovery techniques, which take into account the packet's time-of-arrival. For NTP and PTP transition time is also needed.

Furthermore, packet-based frequency transfer depends on the characteristics of the network affecting packet delay variation (PDV) performance (e.g., network load, number of hops, speed of the links, re-routing). In general anything that affects delay variation of the packets) and the clock recovery function in the end equipment (e.g., the specific local oscillator used, timestamp accuracy). Generally speaking, the frequency information is always distributed from a frequency distribution function towards a frequency recovery

function. The frequency distribution function is referred to as source IWF, Master or Server for TDM PW, PTP or NTP respectively. For PTP or NTP, the frequency distribution function is referred to as packet master clock and the frequency recovery function is referred to as packet slave clock.

12.2.1.1 Frequency distribution requirement

[R-99] An MASG or other PE that complies with this specification MAY support frequency distribution function. Note: The frequency distribution function may be incorporated within the MASG or other PE or implemented externally to it.

[R-100] A CSG or other PE that complies with this specification MAY support frequency recovery function. Note: In some cases the PE may also support a frequency recovery function. These cases are for further study.

12.2.1.2 TDM PW Frequency Distribution Methods

These methods are used to support a TDM PWE (TDM-TNL) service as per TR-221 [1] by distributing the original TDM frequency information end-to-end over the packet network. Two TDM PWE frequency distribution methods are the Adaptive Clock Recovery (ACR) and Differential Clock Recovery (DCR). ACR is addressed in ITU-T G.8261 [63], Clause 8.3. DCR is addressed in ITU-T G.8261 [63] Clause 8.2. The **frame** format as described in section 6.2 in TR-221 [1]. Note: The use of support of Differential Clock Recovery (DCR) in mobile backhaul is for further study. If TDM PW is used for clock distribution then PW over MPLS applies per section 6.2 TR-221 [1].

12.2.1.3 PTPv2 (IEEE 1588 v2)

The Precision Time Protocol is a time distribution protocol which can be used also to transfer frequency synchronization over packet networks. PTP version 2 can be used, for instance in the case of RAN equipment with IP TNL (including LTE), to distribute frequency information to the radio base-station from which its air interface transmission frequency would be derived. PTP is considered a viable packet based method for frequency distribution in G.8261 [63]. Being a higher-layer frequency distribution protocol, PTP is sensitive to the network introduced PDV. PTP is defined in IEEE 1588-2008 [66]. The architecture and requirements for packet-based frequency distribution in telecom networks is described in ITU-T G.8265 [64]. A telecom profile has been specified by the ITU in Recommendations G.8265.1 [65] for interoperability. This Profile concerns the frequency distribution, in a scenario where the network does not provide any timing support such as Boundary Clocks or Transparent Clocks.

[R-101] The synchronization distribution network architecture MUST be per G.8265 [64].

[R-102] The CSG or other PE that implements a PTPv2 slave function SHOULD support a packet slave clock function comply with the PTP Telecom Profile as defined in the ITU-T Recommendations G.8265.1 [65].

12.2.1.4 NTP

The Network Time Protocol is another dedicated time distribution protocol which can be used also to transfer frequency synchronization over packet networks. NTP can be used, for instance in the case of RAN equipment with IP TNL (including LTE), to distribute frequency information to the radio base-station from which its air interface transmission frequency would be derived. NTP is considered as a viable packet based method for frequency distribution in G.8261 [63]. Being a higher-layer frequency distribution protocol, NTP is sensitive to the network introduced PDV. NTP is defined in RFC 1305 (v3) [74] and RFC 5905 (v4) [75].

[R-103] The synchronization distribution network architecture MUST be per G.8265 [64].

[R-104] If a CSG or other PE supports NTP to deliver reference frequency signal to the base station equipment in order to meet its air-interface transmission frequency accuracy requirements , then only packet format and protocol MUST be according to RFC 5905 (v4) [75].

12.2.2 Encapsulation

The timing protocol mapping might depend on the specific transport layer. (e.g., in case of PTP this is specified in G.8265.1 [65], i.e., IEEE 1588 [66] Annex D).

[R-105] A PE SHOULD support transport of timing packets as specified in section 8 of t TR-221 [1]. The encapsulation for the TDM PW is described in section 6.2 (TDM TNL Encapsulation) TR-221 [1].

Note: TDM-PW encapsulations are out of scope of this document. Appendix A TR-221 [1]provides some examples of encapsulations for timing packets in the Mobile Backhaul Environment.

[R-106] A PE supporting G.8265.1 [65] MUST support PTP mapping per G.8265.1 [65], section 6.4 with the following change: “A master or a slave compliant with the profile described in this Recommendation must be compliant with Transport of PTP over User Datagram Protocol over Internet Protocol Version 4 IEEE 1588 [66] and must be compliant with Transport of PTP over User Datagram Protocol over Internet Protocol Version 6 IEEE 1588 .”

12.3 Time and phase synchronization

12.3.1 Time and phase distribution requirements

Stringent time/phase synchronization is needed for some mobile networks, such as TD-SCDMA and LTE TDD and 5G TDD and FDD. Though GNSS (e.g., GPS) can provide accurate timing, they may not be available to the base station in all circumstances. For example, GNSS is vulnerable to jamming and spoofing. Service providers need a mechanism to deliver phase/time in high precision over their MPLS networks in an interoperable way. Depending on the location of the Primary Reference Time Clock (PRTC), a Distributed PRTC method or a Packet-based method can be used.

12.4 Distributed PRTC based time and phase distribution

In this case, the PRTC function is located directly at the base station or the edge of the mobile network (e.g., CSG); typically a GNSS receiver is connected to the base station or the CSG. Therefore, the time synchronization reference is directly delivered from the PRTC to the base station or the CSG. For example, APTS and Sync_E may be used to keep time/phase if GNSS fails.

12.5 Packet based time and phase distribution

12.5.1 Time and phase distribution with full timing support from the network

It can further be classified into the following 3 cases:

Case A: centralized PRTC co-located with Primary Reference Clock (PRC) In case A, the PRTC is co-located with the PRC in the aggregation network (e.g., MASG), and may receive a frequency reference from the PRC (the two functions may be integrated within the same equipment). The time synchronization reference is then delivered from the PRTC via the packet master (T-GM) all along the mobile backhaul network, down to the base station, using a time protocol such as IEEE 1588 PTPv2 [66].

Case B: centralized PRTC not co-located with PRC In case B, the PRTC is located in the aggregation network (MASG), but not co-located with the PRC. The PRTC may receive the frequency reference from the PRC. The time synchronization reference is then delivered from the PRTC via a packet master (T-GM) all along the mobile backhaul network, down to the base station, using a time protocol such as IEEE 1588 PTPv2 [66].

Case C: PRTCs in access networks In case C, the PRTC is located in an access network; typically a GNSS receiver is added to an access device. The PRTC may receive the frequency reference from the PRC. The time synchronization reference is then delivered from the PRTC via a packet master (T-GM) all along the mobile backhaul network, down to the base station, using a time protocol such as IEEE 1588 PTPv2 [66]. These packet based time and phase synchronization cases can be fulfilled by the mechanism and PTP profile as defined in G.8275.1 [73]. The specific architecture is described in G.8275 [72] which allows the distribution of phase/time with full timing support from the network, and is based on the second version of PTP defined in IEEE 1588v2 [66]. That is, all of the nodes in the transmission path will provide timing support by participating in the timing protocol, and the assumption is all the intermediate nodes are Telecom Boundary Clocks (T-BC) with physical layer frequency support. The network limits are specified in G.8271.1 [67]. Note: work is ongoing concerning the inclusion of Telecom Transparent Clocks (T-TC) into the network reference chain (T-TC is being defined in G.8273.3 [69]). The following requirements are needed to support packet based time and phase synchronization:

[R-107] Time and phase distribution architecture MUST be per G.8275 [72]. Note: The PRTC function may be incorporated within the MASG or other PE or implemented externally to it.

[R-108] A PE or P device that implements Telecom Boundary Clock (T-BC) function MUST support T-BC timing characteristics as defined in the ITU-T Recommendations G.8273.2 [68].

[R-109] A CSG or other PE that implements Telecom Time Slave Clock (T-TSC) function MUST support T-TSC timing characteristics as defined in the ITU-T Recommendations G.8273.2 [68].

[R-110] A CSG, PE or P device that implements packet based time and phase distribution MUST support G.8275.1 [73] PTP protocol profile.

12.5.2 Time and phase distribution with partial timing support from the network

For some mobile backhaul networks, many nodes may not have timing synchronization capabilities. ITU-T specifies synchronization architecture for a use case (case E in G.8275 Amendment 1 [71]) where intermediate nodes do not provide timing support, but timing support is provided by GNSS at the network edge, with PTP acting as a backup. This is called Assisted Partial Timing Support (APTS). The node providing support at the edge of the network is called an Assisted Partial Timing Support Clock (APTSC). The mechanism and PTP profile for time and phase distribution with partial timing support are further defined in G.8275.2 [61]. Work is ongoing concerning the performance aspects. In particular, the network limits are being addressed in G.8271.2 [60]and clock specification in G.8273.4 [70]. The following requirements are needed to support time and phase synchronization with partial timing support from the network:

[R-111] Time and phase distribution architecture MUST be per G.8275 [72]case E. Note: The PRTC function may be incorporated within the MASG or implemented externally to it.

[R-112] A MASG MUST support the T-BC-P with PTP protocol profile function as defined in G.8275.2 [61]. Note: the performance of the clock to be used with the G.8275.2 [61]profile is under study (G.8273.4 [70])

A CSG or other PE MUST support T-TSC-A with PTP protocol profile function as defined in the ITU-T Recommendations G.8275 amd2 [61] . Specifically, section A.3.2 MUST be supported with the following change: “A.3.2 Transport mechanisms required, permitted, or prohibited In this profile, a permitted transport mechanism is Transport of PTP over User Datagram Protocol over Internet Protocol Version4 UDP/IPv4 as per Annex D in IEEE 1588 V2 [66]. Bit 0 of the transportSpecific field defined in IEEE 1588 [66] must be set to "0"; that field does not exist in IEEE 1588 [66]. In this profile, the required transport mechanism is Transport of PTP over User Datagram Protocol over Internet Protocol Version 6 UDP/IPv6 as per Annex E in IEEE 1588 [66].”

13 Network Virtualization

As depicted in Figure 5.1 of this document the scope of the document includes:

1. N3, N2 from the RAN to data and control networks
2. N6, N4 and N9 in case the UPF resides in the aggregation network
3. F1 interface DU-CU split option 2.

In addition, the scope is also covering only eMBB use only where the transport SLA requirements are not so stringent.

Since the interfaces listed above are not changing regardless if virtualization is used or not, using virtualization will not impact the transport.

14 4G to 5G migration scenarios

Following are 4G to 5G migration options:

14.1 Stand Alone options

In the Stand Alone options each base station connects to the core from its own generation.

Following are the Stand Alone options:

For completeness, “Option 1” representing today’s 4G deployments is included.

Option 1. (SA) Current 4G network operation that connects LTE device to EPC
Option 2. (SA) Connects 5G NR device to 5G Core as defined in 3GPP R15
Option 5. (SA) Connects LTE device to 5G Core

From Transport perspective options 2 and 5 will require handling much higher rates for data interfaces. Control and data interfaces will be carried as IP TNLs.

Option 2 is generally preferred by the industry e.g., as indicated by MEF 22.3.1 – Transport Services for Mobile Networks [20].

14.2 gNB to EPC

Most of the initial 5G deployments will be **N**on**S**tand**A**lone access, wherein 4G LTE network components are utilized.

Option 3. (NSA) LTE and 5G NR devices connect into EPC

As depicted in figure 13.3.2.2.-1 and figure 13.3.2.2-2 in TS 38.912 [96].

The most important NSA option in the near term is called option 3 which collocates a gNB next to an eNB to obtain the advantages of the NR air interface but without (yet) upgrading the core to the 5GC. This option provides higher data rates for eMBB but not full 5G capabilities. In option 3 there is no direct connection between the gNB and EPC, instead user and control data flow through the eNB via X2-U and X2-C interfaces. Since this will overload the user plane capabilities of the collocated eNB, option 3A provides an S1-U connection from gNB to EPC, obviating the X2-U but with the control traffic still over the X2-C. Option 3X has both X2 and S1 to enable load balancing.

Option 3x is generally preferred by the industry e.g., as indicated by MEF 22.3.1 – Transport Services for Mobile Networks [20].

From Transport perspective both control and data interfaces will be carried as IP TNLs. The underlying connectivity may be different between the collocated and non-collocated cases. For the collocated case the X2 interface may be directly transported on a link connecting the eNB or ng-eNB and the gNB, or a CSG may be used as a L2 switch or L3 router to provide this connectivity.

In option 3 and 3X the X2 interface will be used for control and also for data all in 4G rates.

14.3 LTE to 5GC

For the future there will be options 4 and 7 that only utilize a 5GC (the EPC having been retired) but provide support for 4G legacy UEs via upgraded ng-eNBs. Once again there is collocation of 4G and 5G components, but their interconnection will be via 5G Xn interfaces.

Option 4. (NSA) 5G NR and LTE devices connect into 5GC

As depicted in figure 13.3.3.3.-1 and figure 13.3.3.3-2 in TS 38.912 [96]

Option 7. (NSA) LTE and 5G NR connect into 5G C

As depicted in figure 13.1.3.4.-1 and figure 13.1.3.4-2 in TS 38.912 [96]

In option 4 gNB is the master and ng-eNB connects via Xn interface.

In option 7 ng-eNB is the master and gNB connects via Xn interface. These too have variations (4, 4A, 7, 7A, and 7X).

From Transport perspective both control and data interfaces will be carried as IP TNLs. The underlying connectivity may be different between the collocated and non-collocated cases. For the collocated case the X2 interface may be directly transported on a link connecting the eNB or ng-eNB and the gNB, or a CSG may be used as a L2 switch or L3 router to provide this connectivity.

In option 4 and 7 the CSG needs to support higher BW since it carries more than one gNB/ng-eNB interfaces.

15 Network Management YANG Model Requirements

This section provides the network management related equipment model requirements for the transport network nodes providing 5G transport support.

> **Note:** This is not an exhaustive list of models. It is assumed that there is a complete network management framework that these fit into.

To set the tone for the models being referenced, YANG 1.1 and NMDA are useful and SHOULD be supported:

YANG and NETCONF related

- IETF RFC 7950: The YANG 1.1 Data Modeling Language
- IETF RFC 8342: Network Management Datastore Architecture (NMDA)
- IETF RFC 8526: NETCONF Extensions to Support the Network Management Datastore Architecture
- IETF 8407: Guidelines for Authors and Reviewers of Documents Containing YANG Data Models
- IETF 8819: YANG Module Tags

The PE SHOULD support the following network management models according to the Category noted (e.g., If the PE supports the Sync Category, the corresponding models (i.e., IETF RFC 8575 ietf-ptp.yang) SHOULD be supported as well):

Req#	Standard	Category	Title	YANG Modules
[R-113]	IETF RFC 8343	Interface	A YANG Data Model for Interface Management	ietf-interface.yang
[R-114]	IETF RFC 8348	Hardware	A YANG Data Model for Hardware Management	ietf-hardware.yang ietf-hardware-state.yang
[R-115]	IETF RFC 8561	Microwave	A YANG Data Model for Microwave Radio Link	ietf-microwave-radio-link.yang ietf-microwave-types.yang
[R-116]	IETF RFC 8575	Sync	YANG Data Model for the Precision Time Protocol (PTP)	ietf-ptp.yang
[R-117]	IEEE 802.3.2-2019	Ethernet	IEEE Standard for Ethernet	ieee802-ethernet-interface-half-duplex.yang ieee802-ethernet-interface-interface.yang ieee802-ethernet-interface-link-oam.yang ieee802-ethernet-interface-pon.yang ieee802-ethernet-interface-pse.yang
[R-118]	IEEE 802.1Q-2018 (and amendments)	Bridging	IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks	ieee802-types.yang ieee802-dot1q-ats.yang ieee802-dot1q-bridge.yang ieee802-dot1q-cfm-alarm.yang ieee802-dot1q-cfm-bridge.yang ieee802-dot1q-cfm-types.yang

				ieee802-dot1q-cfm.yang ieee802-dot1q-pb.yang ieee802-dot1q-stream-filters-gates.yang ieee802-dot1q-tpmr.yang ieee802-dot1q-tsn-types.yang ieee802-dot1q-types.yang
[R-119]	IEEE 802.1X-2020 (and amendments)	Bridging	IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks	• ieee802-dot1x-types.yang • ieee802-dot1x.yang

Related to topology, the following provides a base set of topology related models:

- RFC 8345: A YANG Data Model for Network Topologies
  - ietf-network.yang
  - ietf-network-state.yang
  - ietf-network-topology.yang
- RFC 8795: YANG Data Model for Traffic Engineering (TE) Topologies
  - ietf-te-topology.yang
  - ietf-te-topology-state.yang

Basic models needed for system management:

- System Management
  - RFC 7317: A YANG Data Model for System Management
    - ietf-system
- Security
  - RFC 8341: Network Configuration Access Control Model
    - ietf-netconf-acm
- Alarm Management
  - RFC 8632: A YANG Data Model for Alarm Management
    - ietf-alarms
- Notification Management
  - RFC 8639: Subscription to YANG Notifications
    - ietf-subscribed-notifications
  - RFC 8640: Dynamic Subscription to YANG Events and Datastores over NETCONF
  - RFC 8641: Subscription to YANG Notifications for Datastore Updates
    - ietf-yang-push
- Monitoring of Management Protocol
  - RFC 6022: YANG Module for NETCONF Monitoring
    - ietf-netconf-monitoring
- YANG Library
  - RFC 8525: YANG Library
    - ietf-yang-library

End of Broadband Forum Technical Report TR-521