TECHNICAL REPORT

TR-221
Technical Specifications for MPLS in Mobile Backhaul Networks

Issue: 1
Issue Date: October 2011

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

This Broadband Forum Technical Report is provided AS IS, WITH ALL FAULTS. ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY:

(A) OF ACCURACY, COMPLETENESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE;
(B) THAT THE CONTENTS OF THIS BROADBAND FORUM TECHNICAL REPORT ARE SUITABLE FOR ANY PURPOSE, EVEN IF THAT PURPOSE IS KNOWN TO THE COPYRIGHT HOLDER;
(C) THAT THE IMPLEMENTATION OF THE CONTENTS OF THE TECHNICAL REPORT WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

By using this Broadband Forum Technical Report, users acknowledge that implementation may require licenses to patents. The Broadband Forum encourages but does not require its members to identify such patents. For a list of declarations made by Broadband Forum member companies, please see http://www.broadband-forum.org. No assurance is given that licenses to patents necessary to implement this Technical Report will be available for license at all or on reasonable and non-discriminatory terms.

ANY PERSON HOLDING A COPYRIGHT IN THIS BROADBAND FORUM TECHNICAL REPORT, OR ANY PORTION THEREOF, DISCLAIMS TO THE FULLEST EXTENT PERMITTED BY LAW (A) ANY LIABILITY (INCLUDING DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES UNDER ANY LEGAL THEORY) ARISING FROM OR RELATED TO THE USE OF OR RELIANCE UPON THIS TECHNICAL REPORT; AND (B) ANY OBLIGATION TO UPDATE OR CORRECT THIS TECHNICAL REPORT.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Issue Date	Issue Editors	Changes
1	October 2011	Doug Hunt, ALU Ron Isler, RAD Santosh Kolenchery, Ericsson Fabien Le Clech, FT Ed Sierecki, AT&T	Original

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

Editors	Doug Hunt	ALU
	Ron Isler	RAD
	Santosh Kolenchery	Ericsson
	Fabien Le Clech	FT
	Ed Sierecki	AT&T
IP/MPLS&Core WG Chair	Rao Cherukuri	Juniper
Vice Chairs	Drew Rexrode	Verizon
	David Sinicrope	Ericsson
Chief Editor	Michael Hanrahan	Huawei Technologies

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

With the increase of the bandwidth demand per mobile user combined with the decrease of the average revenue per user, mobile operators and transport providers need to evolve their mobile backhaul networks to be faster and more efficient thereby lowering the cost per bit in the backhaul network. One way to address this is to converge multiple backhaul technologies into one unified technology and converge multiple backhaul networks into a single network making more efficient use of network resources and reducing operational costs.

MPLS, with its support for TDM, ATM, Ethernet and IP services, is the unique technology that allows this convergence. TR-221 defines the use of MPLS in Mobile Backhaul access and aggregation networks and provides solutions for the transport of traffic in 2G, 3G and LTE mobile networks.

Specifically, TR-221 provides reference architectures for MPLS in Mobile Backhaul networks and includes specifications for the various transport scenarios that are depicted in the reference architecture. TR-221 describes transport architectures applicable to all mobile networks (e.g. 2G, 3G and LTE) and also specifies the equipment requirements for the control, user and management planes to provide unified and consistent end-to-end transport services for mobile backhaul.

1 Purpose and Scope

1.1 Purpose

TR-221 provides technical architecture and equipment requirements for MPLS based mobile backhaul networks. It provides solutions and end-to-end reference architectures for transport services addressing control, user and management traffic in mobile networks. It also includes specifications for various transport scenarios that are depicted in this reference architecture. The intent of TR-221 is to promote the multi-vendor interoperability for equipments used in mobile backhaul networks based on MPLS. TR-221 may be used as a basis for conformance testing.

1.2 Scope

There is a range of services that may be used to transport wireless traffic in the access and aggregation networks. For example, choices can include IP, TDM, ATM, and Ethernet.

TR-221 focuses on the application of MPLS technology in these networks with regards to encapsulation, signaling and routing, QoS, OAM, resiliency, security and synchronization. At the same time, it is recognized that portions of the network based upon MPLS may interface with portions based on other technologies such as IP, TDM, ATM or Ethernet. However, details of the use of other technologies in the network are outside of the scope of this document.

Expected services over the backhaul network include: real-time voice, multimedia services, data traffic and multicast traffic e.g. MBMS (Multimedia Broadcast and Multicast Services). As such, the solution and architecture must provide the requisite quality of service (QoS) and traffic engineering (TE) capabilities to support these services.

The scope of TR-221 includes the following:

- The use of MPLS technology to backhaul mobile traffic (user, control and management planes) over access and aggregation networks. While MPLS is widely used for the transport in the mobile core network, the use of MPLS technology in the core network is not within the scope of TR-221.

- The scope is to consider several 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.

- The following Transport Network Layers (TNLs as defined by 3GPP in TS 25.401 [100] and TS 25.933 [101] are within scope of TR-221: TDM TNL (e.g. for 2G), ATM TNL (e.g. for 3G R3/R4/R5) and IP TNL (e.g. for 3G R5 and beyond, and LTE R8 and beyond).

- 3GPP and 3GPP2 networks such as 2G, 2.5G, 3G and LTE.

- Generic QoS requirements for mobile backhaul services.

- Requirements for supporting clock distribution to the base stations, including frequency. Time/phase synchronization requirements are for further study.

- Resiliency requirements taking into account failover times appropriate for mobile backhaul networks.

- OAM requirements and capabilities for the MPLS network.

- RAN equipment with a range of physical interfaces (e.g. T1/E1, STM1/OC3, Fast Ethernet, Gigabit Ethernet, etc.) and technologies (e.g. PDH, SDH, ATM, PPP, Ethernet, IP, etc.), connected through intervening access and aggregation networks.

- Support for different kinds of access transmission technologies: point-to-point access (xDSL, microwave, Fiber), point-to-multipoint access (e.g. xPON).

- MPLS facilities in the access and/or aggregation networks which may be leased from a third party.

TR-221 approaches the mobile backhaul architecture from the point of view of the transport network. Mobile traffic is considered as application data of the respective TNL and is transparent to the transport network. Different MPLS solutions can be used to transport the TNLs of mobile networks: L2VPN, (e.g. VPWS, VPLS, H-VPLS), L3VPN (e.g. BGP L3VPN), and IP routing over MPLS (e.g. IP over LSPs). Other technologies are not precluded but are out of scope of TR-221 (e.g. Provider Bridging, Provider Backbone Bridging).

TR-221 assumes that an MASG (Mobile Aggregation Site Gateway) and a CSG (Cell Site Gateway) are MPLS PE nodes. When the MASG and CSG are not MPLS nodes, their requirement specifications are outside the scope of TR-221.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [9].

MUST This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.

MUST NOT This phrase means that the definition is an absolute prohibition of the specification.

SHOULD This word, or the adjective “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.

MAY This word, or the adjective “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.1.1 Requirements table

In some sections of the document the requirements differ depending on the role of the equipment, e.g. different for MASG vs. CSG. In these cases the requirement is listed in a table and the status of the requirement given for each equipment role as illustrated in the example below.

MASG (PE router)	**CSG (PE router)**	**P router**	**Requirement**
MUST	SHOULD	N/A	[R] Router equipment requirement XYZ

Table 1 – Example Requirement Table

2.2 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.

2.2.1 Normative References

Document		Title	Source	Year
[1]	AF-AIC-0178.001	*ATM-MPLS Network Interworking v2.0*	ATM Forum	2003
[2]	802.1AX-2008	*Link Aggregation*	IEEE	2008
[3]	802.1Q	*IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*	IEEE	2005
[4]	802.3ah	*Ethernet in the other first mile: North American case studies for IEEE 802.3ah in applications beyond FTTH*	IEEE	2006
[5]	1588v2	*Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*	IEEE	
[6]	RFC 1195	*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*	IETF	1990
[7]	RFC 1305	*Network Time Protocol Specification, Implementation and Analysis, Version 3*	IETF	1992
[8]	RFC 1981	*Path MTU Discovery for IP version 6*	IETF	1996
[9]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[10]	RFC 2328	*OSPF Version 2*	IETF	1998
[11]	RFC 2545	*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*, March 1999.	IETF	2001
[12]	RFC 2460	*Internet Protocol Version 6 (IPv6) Specification*	IETF	1998
[13]	RFC 3032	*MPLS Label Stack Encoding*	IETF	

[14]	RFC 3209	*RSVP-TE: Extensions to RSVP for LSP Tunnels*	IETF	2001
[15]	RFC 3270	*Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*	IETF	2002
[16]	RFC 3386	*Network Hierarchy and Multilayer Survivability*	IETF	2002
[17]	RFC 3471	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*	IETF	2003
[18]	RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*	IETF	2003
[19]	RFC 3478	*Graceful Restart Mechanism for Label Distribution Protocol*	IETF	2003
[20]	RFC 3630	*Traffic Engineering (TE) Extensions of OSPF Version 2*	IETF	2003
[21]	RFC 3623	*Graceful OSPF Restart*	IETF	2003
[22]	RFC 3809	*Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)*	IETF	2004
[23]	RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*	IETF	2004
[24]	RFC 3916	*Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*	IETF	2004
[25]	RFC 4090	*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*	IETF	2005
[26]	RFC 4111	*Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)*	IETF	2005
[27]	RFC 4364	*BGP/MPLS IP Virtual Private Networks*	IETF	2006
[28]	RFC 4365	*Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)*	IETF	2006
[29]	RFC 4379	*Detecting Multi-protocol Dataplane*	IETF	2006
[30]	RFC 4385	*Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*	IETF	2006

[31]	RFC 4443	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6) Specification*	IETF	2006
[32]	RFC 4446	*IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*	IETF	2006
[33]	RFC 4447	*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*	IETF	2006
[34]	RFC 4448	*Encapsulation Methods for Transport of Ethernet over MPLS Networks*	IETF	2006
[35]	RFC 4553	*Encapsulation Methods for Transport of Ethernet over MPLS Networks over Packet (SAToP)*	IETF	2006
[36]	RFC 4659	*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*	IETF	2006
[37]	RFC 4717	*Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks*	IETF	2007
[38]	RFC 4760	*Multiprotocol Extensions for BGP-4*	IETF	2007
[39]	RFC 4761	*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*	IETF	2007
[40]	RFC 4762	*Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*	IETF	2007
[41]	RFC 4798	*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*	IETF	2007
[42]	RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*	IETF	2007
[43]	RFC 4875	*Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*	IETF	2007
[44]	RFC 5036	*LDP Specification*	IETF	2007
[45]	RFC 5085	*Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*	IETF	2007

[46]	RFC 5086	*Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*	IETF	2006
[47]	RFC 5151	*Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*	IETF	2008
[48]	RFC 5254	*Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)*	IETF	2008
[49]	RFC 5287	*Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*	IETF	2008
[50]	RFC 5305	*IS-IS Extensions for Traffic Engineering*	IETF	2008
[51]	RFC 5308	*Routing IPv6 with IS-IS*	IETF	2008
[52]	RFC 5329	*Traffic Engineering Extensions to OSPF Version 3*	IETF	2008
[53]	RFC 5340	*OSPF for IPv6*	IETF	2008
[54]	RFC 5549	*Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop*	IETF	2009
[55]	RFC 5659	*An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*	IETF	2009
[56]	RFC 5798	*Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*	IETF	2010
[57]	RFC 5880	*Bidirectional Forwarding Detection (BFD)*	IETF	2010
[58]	RFC 5881	*BFD for IPv4 and IPv6 (Single Hop)*	IETF	2010
[59]	RFC 5883	*Bidirectional Forwarding Detection (BFD) for Multihop Paths*	IETF	2010
[60]	RFC 5884	*Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*	IETF	2010

[61]	RFC 5885	*Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*	IETF	2010
[62]	RFC 5905	*Network Time Protocol Version 4: Protocol and Algorithms Specification*	IETF	2010
[63]	RFC 5994	*Application of Ethernet Pseudowires to MPLS Transport Networks*	IETF	2010
[64]	RFC 6073	*Segmented Pseudowire*	IETF	2011
[65]	RFC 6074	*Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*	IETF	2011
[66]	RFC 6119	*IPv6 Traffic Engineering in IS-IS*	IETF	2011
[67]	RFC 6310	*Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*	IETF	2011
[68]	RFC 6374	*Packet Loss and Delay Measurement for MPLS Networks*	IETF	2011
[69]	draft-ietf-l3vpn-2547bis-mcast-10.txt	*Multicast in MPLS/BGP IP VPNs*	IETF	2010
[70]	Draft-ietf-l3vpn-2547bis-mcast-bgp-08.txt	*BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*	IETF	2009
[71]	draft-ietf-l3vpn-mvpn-considerations-06	*Mandatory Features in a Layer 3 Multicast BGP/MPLS VPN Solution*	IETF	2010
[72]	draft-ietf-mpls-ldp-p2mp-15	*Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*	IETF	2011
[73]	draft-ietf-pwe3-static-pw-status-06.txt	*Pseudowire Status for Static Pseudowires*	IETF	2011

[74]	IP/MPLS Forum 4.1.0	*TDM Transport over MPLS using AAL1 Technical Specification*	IP/MPLS Forum	2008
[75]	IP/MPLS Forum 20.0.0	*MPLS in Mobile Backhaul Networks Framework and Requirements Technical Specification*	IP/MPLS Forum	2008
[76]	G.704	*Synchronous Frame Structures Used at 1544, 6312, 2048, 8448 and 44 736 kbit/s Hierarchical Levels*	ITU-T	1998
[77]	G.707	*Network Node Interface For The Synchronous Digital Hierarchy (SDH)*	ITU-T	2003
[78]	G.811	*Timing Characteristics of Primary Reference Clocks*	ITU-T	1997
[79]	G.823	*The Control Of Jitter and Wander Within Digital Networks Which are Based on the 2048 Kbit/S Hierarchy*	ITU-T	2000
[80]	G.824	*Control of Jitter and Wander Within Digital Networks Which are Based on the 1544 kbit/s Hierarchy*	ITU-T	2000
[81]	G.825	*Control of Jitter and Wander Within Digital Networks Which are Based on the Synchronization Digital Hierarchy (SDH)*	ITU-T	1993
[82]	G.8261	*Timing and Synchronization Aspects in Packet Networks*	ITU-T	2007
[83]	G.8262	*Timing characteristics of synchronous Ethernet equipment slave clock (EEC)*	ITU-T	2007
[84]	G.8265	*Architecture and requirements for packet based frequency delivery*	ITU-T	
[85]	G.8265.1	*Precision time protocol telecom profile for frequency synchronization*	ITU-T	2010
[86]	I.150	*B-ISDN Asynchronous Transfer Mode Functional Characteristics*	ITU-T	1999
[87]	I.610	*B-ISDN Operations and Maintenance Principles and Functions*	ITU-T	1999
[88]	Y.1411	*ATM-MPLS Network Interworking - Cell Mode User Plane Interworking*	ITU-T	2006
[89]	MEF 4	*Metro Ethernet Network Architecture Framework - Part 1: Generic Framework*	MEF	2004

[90]	MEF 6.1	*Ethernet Services Definitions - Phase 2*	MEF	2008
[91]	MEF 10.2	*Ethernet Services Attributes - Phase 2*	MEF	2009
[92]	MEF 11	*User Network Interface (UNI) Requirements and Framework*	MEF	2004
[93]	MEF 12.1	*Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer - Base Elements*	MEF	2010
[94]	MEF 13	*User Network Interface (UNI) Type 1 Implementation Agreement*	MEF	2005
[95]	MEF 20	*User Network Interface (UNI) Type 2 Implementation Agreement*	MEF	2008
[96]	MEF 22.1	*Mobile Backhaul Implementation Agreement - Phase 1*	MEF	2009
[97]	MPLS and Frame Relay Alliance 8.0.0	*Emulation of TDM Circuits over MPLS Using Raw Encapsulation Implementation Agreement*	MPLS and Frame Relay Alliance	2004

2.2.2 Informative References

[98]	C.S0084	*Overview for Ultra Mobile Broadband (UMB) Air Interface Specification, Version 2.0*	3GPP2	2007
[99]	TS 23.002	*Network Architecture*	3GPP	
[100]	TS 25.401	*UTRAN overall description (Release 8)*	3GPP	
[101]	TS 25.933	*IP Transport in UTRAN (Release 5)*	3GPP	
[102]	TS 25.999	*High Speed Packet Access (HSPA) evolution; Frequency Division Duplex (FDD) (Release 7)*	3GPP	2008
[103]	TS 32.107	*Quality of Service (QoS) Concept and Architecture*	3GPP	
[104]	TS 36.300	*Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2*	3GPP	
[105]	RFC 4026	*Provider Provisioned Virtual Private Network (VPN) Terminology*	IETF	2005

2.3 Definitions

The following terminology is used throughout this Technical Report.

Abis Interface between the BTS and BSC (TNL is TDM)

ATM TNL The Transport Network Layer defined in this document as the transport bearer for 3G ATM traffic.

CSG Cell Site Gateway – Node at the cell site that presents the transport network interface to the Base Station equipment. For purposes of this document this device is an MPLS capable node.

Iub Interface between the NB and RNC (TNL is ATM or IP)

IP TNL The Transport Network Layer defined in this document as the transport bearer for LTE and 3G IP traffic. It should also be noted that there is a possible difference between the TNL and what is transported over MPLS. For example, when carrying the ATM TNL using TDM over MPLS or when carrying IP TNL using Ethernet over MPLS.

MASG Mobile Aggregation Site Gateway - Node at the radio controller, MME or serving gateway site that presents the transport network interface to the mobile equipment. For purposes of this document this device is an MPLS capable node.

S1 interface Interface between the eNB and the MME or S-GW

TDM TNL The Transport Network Layer defined in this document as the transport bearer for 2G TDM traffic.

X2 interface Interface between two neighboring eNBs

2.4 Abbreviations

This Technical Report uses the following abbreviations:

3GPP	3rd Generation Partnership Project
AC	Access Circuit
aGW	Access Gateway (MME, S-GW/P-GW)
AN	Access Node
ATM	Asynchronous Transfer Mode
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
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
EPS Bearer	Evolved Packet System Bearer
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVC	Ethernet Virtual Connection
FDD	Frequency Division Duplex
FEC	FEC Forwarding Equivalence Class
GPRS	General Packet Radio Service
GSM	Global Standard for Mobile Communication
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
OAM	Operations, Administration and Management
P	Provider
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
QoS	Quality of Service
RAN	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
S-GW	Serving – Gateway
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

3 Technical Report Impact

3.1 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) 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.

3.2 IPv6

To support the smooth transition from IPv4 to IPv6 for the MPLS Mobile Backhaul (MBH) networks, this document specifies IPv6 use with MPLS. IPv6 support covers the data plane support of IPv6 for the IP TNL, the control plane support of IPv6 routing, signaling and management plane. It should be noted that IPv6 can be implicitly supported in any MPLS L2VPN solution since the IPv6 packets are transparently transported over the Ethernet PWs. In addition, with L3VPN there is a technology defined to carry IPv6 over MPLS in a transparent way without having to support IPv6 on the P nodes. This mechanism is the 6PE defined in RFC 4798 [41].

The evolution to IPv6 can be step by step depending on the service providers' needs. For example, the RAN may be evolved to use IPv6 first and then MBH follows, or vice versa. This means that the mobile backhaul network should accommodate IPv6 transport. This means the IPv6 RAN is supported, while the MPLS mobile backhaul network internally remains IPv4. The final stage of the IPv6 evolvement for carriers could be based on a full IPv6 MPLS MBH network.

3.3 Security

Security requirements above the transport level are specified by 3GPP. It is assumed that security risks on the 2G and 3G RAN are negligible because the traffic is encrypted between the Base Station and the Network Controller. For LTE, traffic between eNB and MME or S-GW may be encrypted using IPsec if the deployment scenario demands it.

Security risks on the mobile backhaul network (e.g. securing the MPLS control plane) are addressed by the security requirements described further in the document in Section 5.6.

3.4 Privacy

Any issues regarding privacy are not affected by TR-221.

4 Reference Architecture

4.1 Supported technologies and TNL types

The reference architecture shows various scenarios that are based on the type of the Transport Network Layer (TNL) carried over the MPLS network. Four types of TNL are considered in the TR-221 (TDM, ATM and IP) according to the mobile network generation as shown in Table 2 that presents different TNL scenarios using MPLS technology in the access and aggregation networks to transport all these kinds of TNLs.

Network	Specification	TNL
GSM/GPRS/EDGE (2G/2.5G)		TDM IP
UMTS	R3, R99/R4	ATM
	R99/R5, R6, R7	ATM
		IP
CDMA 1x-RTT	IS-2000	TDM
CDMA 1x EV-DO	IS-856	IP
LTE	R8,R9,R10	IP

Table 2 – RAN Access Technologies

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

1. TDM TNL
2. ATM TNL
3. IP TNL

For details regarding each TNL scenario, refer to Section 5 of IP/MPLS Forum 20.0.0 [75]

For each supported TNL scenario, the MPLS transport network may extend from the MASG to various nodes in the mobile access/aggregation network as indicated by cases (a) through (f) in Figure 1. These are referred to as Deployment Scenarios.

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

4.2 Deployment Scenarios

Figure 1 provides a reference architecture, depicting the access, aggregation and core parts of the mobile backhaul network considering all current types of TNL used in 2G, 3G and LTE mobile networks.

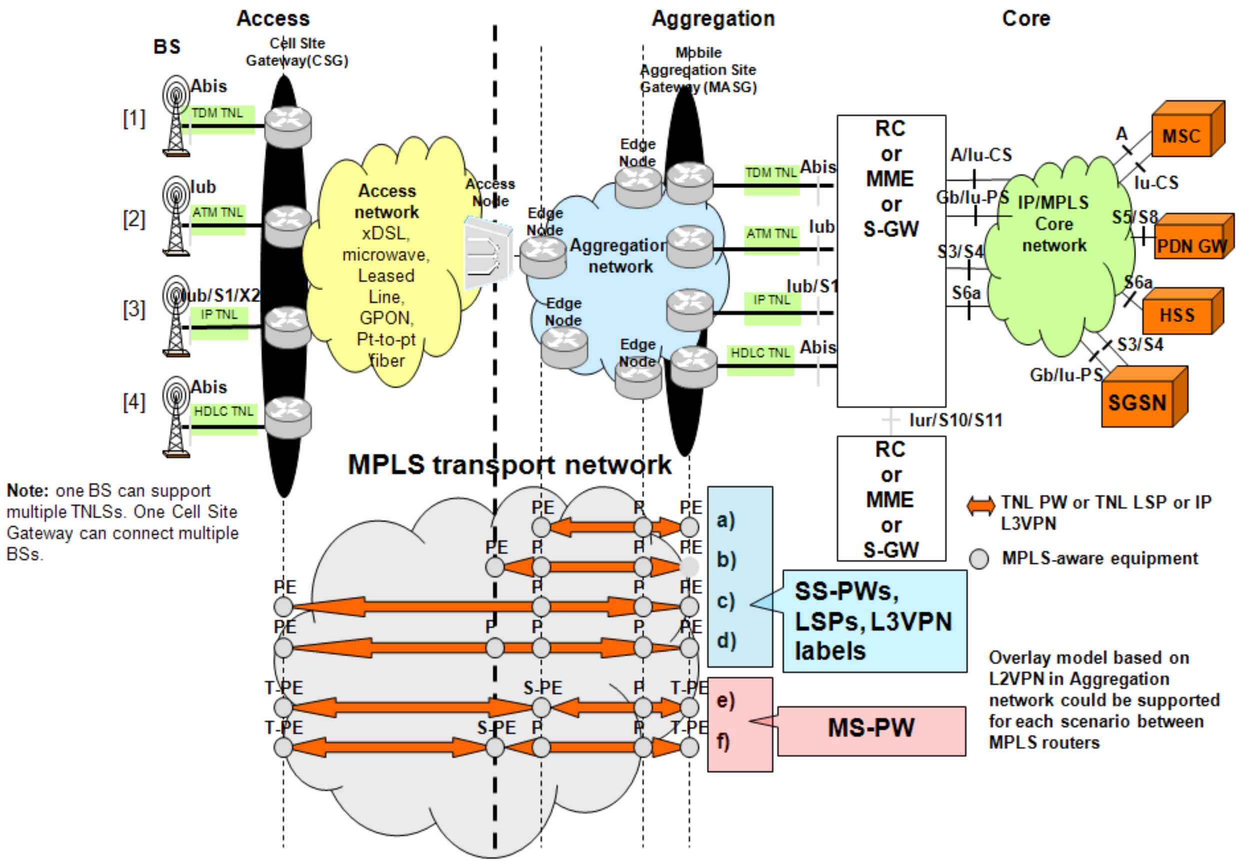


Figure 1: Reference Architecture for mobile backhaul network using MPLS Transport in the Access, Aggregation, and Core Networks

All encapsulations over MPLS solutions performed in the CSG require suitable adaptation mechanisms at the MASG to provide a compliant interface Iub for interconnection to the BSC/RNC. Figure 1 depicts an MPLS-based mobile backhaul network in the Access and Aggregation networks connecting Base Stations to RC/MME/S-GW. MPLS in the core networks connecting RC/MME/S-GW to MSC 2G/3G and P-GW is out of scope of the document. In the reference architecture, the location of MPLS functions for the various TNL scenarios is flexible; i.e. the MPLS 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.

Various Deployment Scenarios arise based on the location of MPLS functions and the extent of MPLS in the mobile backhaul network. Cases (a) through (f) in Figure 1 depict these deployment scenarios through the access and aggregation networks:

a. MPLS transport is used between the EN and the MASG via a Single Segment Pseudowire (SS-PW) or LSP or L3VPN carrying a TNL.
b. MPLS transport is used between the AN and the MASG via a SS-PW or LSP or L3VPN carrying a TNL.
c. MPLS transport is used between the CSG and the MASG, with the AN transparent to MPLS. A SS-PW or LSP or L3VPN 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.

d. MPLS transport is used between the CSG and the MASG, with an AN that is MPLS-aware. A SS-PW or LSP or L3VPN 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.

e. A Multi-Segment Pseudowire (MS-PW) carrying a TNL is established between the CSG and the MASG, which act as T-PE devices, while the EN acts as a S-PE device.

f. A MS-PW carrying a TNL is established between the CSG and the MASG, which act as T-PE devices, while the AN acts as a S-PE device.

For each MPLS use case, an overlay model based upon L2VPN could be used between any MPLS routers. L2VPN can be based upon VPWS or VPLS in the aggregation network, and even down to the AN. 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 the Ethernet layer is carried over L2VPN in the aggregation network (including AN 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.

Note that in scenarios e and f, the PW segments in the access network are built between equipment that is directly connected (i.e. there is no intervening MPLS-aware equipment). These PW segments are between the CSG and EN (scenario e) or between the CSG and AN (scenario f). These PW segments may be carried over a physical layer with constrained bandwidth, such as a leased line or microwave connection. To support efficient transport for these bandwidth-constrained PW segments, an implicit null PSN tunnel label may optionally be used in these scenarios. MS-PW is still work in progress within the IETF. Although this architecture references MS-PW and MS-PW architecture is defined in RFC 5659 [55]and RFC 6073 [64] specific support of dynamically signaled MS-PW in this document is for further study.

There are different types of solutions based upon MPLS 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. MPLS architectures described in this section have to support IP connectivity requirements between BS and MME or S-GW/P-GW on one hand and between BSs on the other hand. Appendix C provides use cases of different LTE mobile node’s (e.g. MME, S-GW, P-GW) location in the transport network.

When an Ethernet service is used at both endpoints of the RAN backhaul, this service is an MEF EVC demarced by MEF UNIs that is realized with a L2VPN. Specifically, TR-221 realizes the E-Line, E-LAN and E-Tree* (see Appendix F) services described by the MEF 22.1 [96] and MEF 6.1 [90]. Also see Section 4.3.2.1.

4.3 MPLS connectivity

4.3.1 L2VPN MPLS connectivity for TDM and ATM TNL

This section addresses the MPLS architecture for providing TDM and ATM emulation to transport the TDM and ATM TNLs for mobile backhaul.

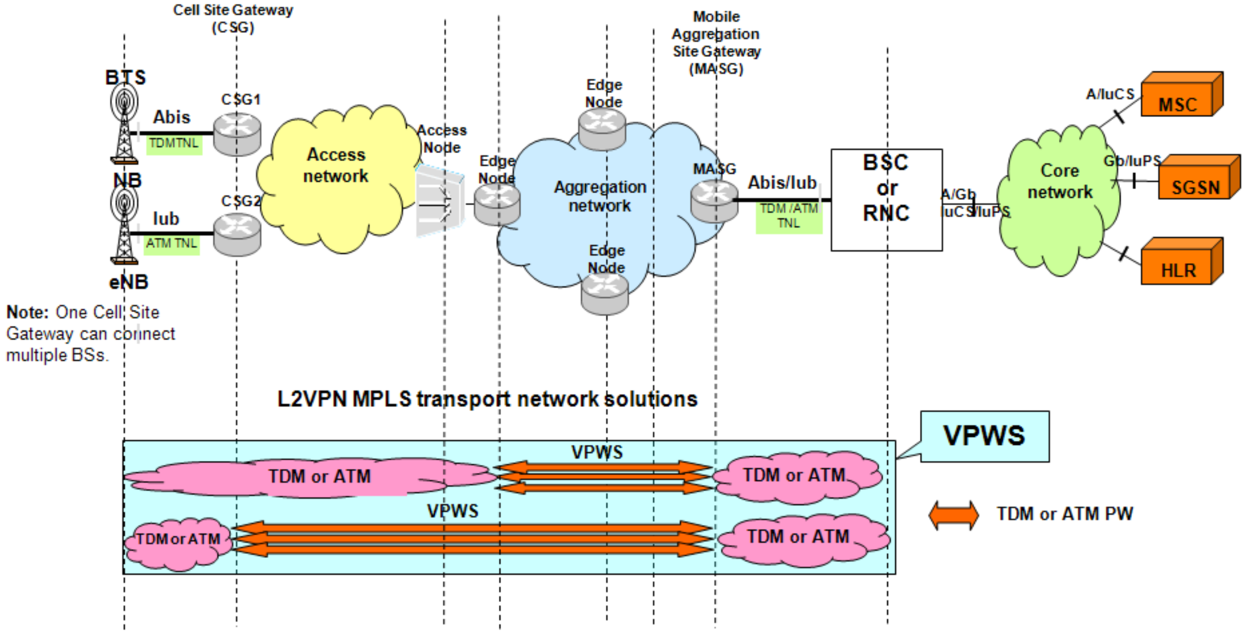


Figure 2: Reference Architecture of L2VPN MPLS connectivity for TDM and ATM TNL

4.3.1.1 TDM TNL

The mobile technologies identified in the Table 2 using the TDM TNL use the following interfaces:

- T1 or E1 links as per the G.704 [76] interface
- T3 or E3 links as per the G.704 [76] interface
- OC3 or STM-1c links as per the ITU-T G.707 [77] interface

These interfaces are point-to-point interfaces and their content may be emulated by VPWS using a TDM PW.

4.3.1.2 ATM TNL

The mobile technologies identified in Table 2 using the ATM TNL require ATM VPC and VCC connections defined per ITU-T I.150 [86].

These connections are point-to-point and are emulated by VPWS using ATM PWs.

Note: ATM TNL can also be carried using TDM emulation. Impacts of carrying ATM TNL using TDM emulation in conjunction with IMA and SATOP are outside the scope of this document.

4.3.2 L2VPN MPLS connectivity for IP TNL using Ethernet

The mobile technologies identified in Table 2 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 RC/MME/S-GW sites, MEF compliant EVC based services and attributes as specified in MEF 22.1 [96] are used. MEF services are supported as VPWS or VPLS across the domain that uses MPLS for transport. Specifically, this document realizes the E-Lineand E-LAN services described by the MEF mobile backhaul IA (MEF 22 and MEF 6.1). 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 22.1 [96] describes how mobile backhaul can be supported by Carrier Ethernet Services in MEF 6.1 [90], using Service Attributes defined in MEF 10.2 [91] and MEF 22.1. The additional service attributes focus on availability, resiliency performance, COS and synchronization.

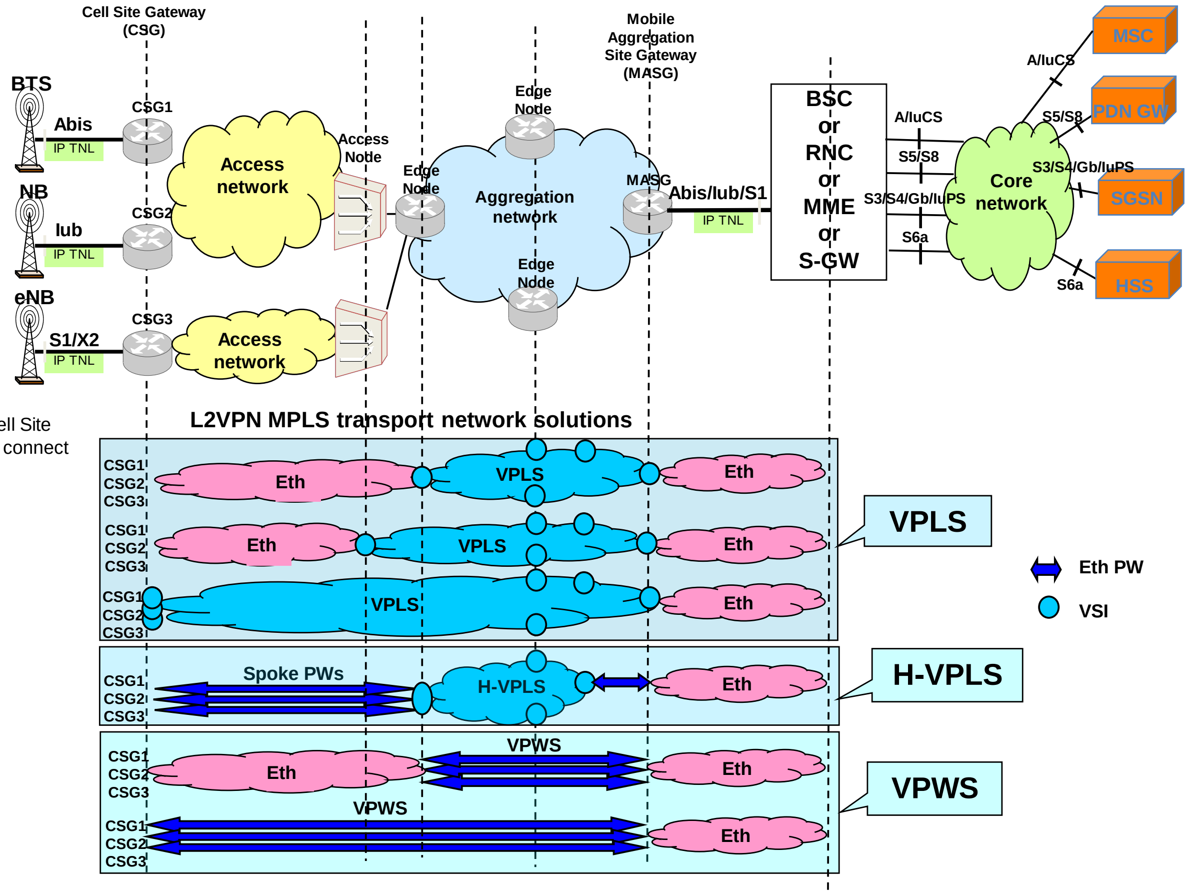
In the mobile backhaul network, d Ethernet VLAN tagging as per IEEE 802.1Q [3], may be used for traffic separation, for example to separate management from user traffic, to separate traffic between operators in case of RAN sharing or to separate 2G, 3G and LTE traffic in case of traffic aggregation.

Figure 3 provides the reference architecture for L2VPN solutions as VPLS (e.g. RFC 4762 [40] and/or RFC 4761 [39]), H-VPLS option of RFC 4762 and VPWS in the mobile backhaul network for 2G/3G using IP TNL or LTE, 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 both S1 and X2 interfaces in order to get a converged and efficient network solution for LTE.

VPLS 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.



Note: One Cell Site Gateway can connect multiple BSs.

Figure 3: Reference Architecture of L2VPN MPLS connectivity for IP TNL using Ethernet

Note: The diagram in Figure 3 shows progression of VPLS from the aggregation to the access. This diagram represents one logical diagram and does not preclude others.

4.3.2.1 Relationship to MEF 22.1 Mobile Backhaul

This section introduces key MEF service constructs and shows the relationship to TR-221. MEF 22.1 [96] "*Mobile Backhaul Implementation Agreement, Phase 2*" identifies the requirements for MEF defined Ethernet Services and MEF defined External Interfaces (EIs such as UNIs) for use in Mobile Backhaul networks based on MEF specifications. The services and requirements on the Metro Ethernet Network (MEN) are based on the services defined in MEF 6.1 [90] as well as the attributes defined in MEF 10.2 [91], in MEF 10.2.1 and MEF 22.1 [96].

Note: When the CSG is not an MPLS node its requirements are out-of-scope in this document.

4.3.2.1.1 EVC

The Ethernet Virtual Connection (EVC) is defined in Section 5/MEF 4 [89] and further augmented by Section 6/MEF 10.2 [91]. Per Section 5/MEF 4:

> *"The Ethernet Virtual Connection (EVC) is the architecture construct that supports the association of UNI reference points for the purpose of delivering an Ethernet flow between subscriber sites across the MEN. There may be one or more subscriber flows mapped to a particular EVC (e.g. there may be more subscriber flows identified by the flow classification rules at the ingress point to a network than EVCs). The mapping of Ethernet flows to EVCs is service specific and specified in the MEF Ethernet Service Model specification…"*

4.3.2.1.2 UNI

The MEF User Network Interface (UNI), is defined in Section 7.1/MEF 4 [89] and Section 6.3/MEF 10.2 [91] and specified in MEF 13 [94], and MEF 20 [95]. As per MEF 4:

> *"The UNI is the interface used to interconnect a MEN subscriber to its MEN service provider(s). The UNI also provides a reference point for demarcation between the MEN operator's equipment that enables access to the MEN services and the subscriber access equipment. Therefore, the demarcation point indicates the location where the responsibility of the service provider ends, and the responsibility of subscriber begins. The specific location of the UNI reference point (T) is specified in the MEF UNI document."*

In this document MEF UNI refers to the physical demarcation point between the responsibility of the MEN Operator ("Service Provider") and the responsibility of the Mobile Operator ("Subscriber"). The UNI requirements might not be uniform for all UNIs in the Mobile Backhaul. For example MASG UNI requirements might be different than the CSG UNI requirements.

The UNI-C, as defined in Section 7.1.1/MEF 4 [89] and MEF 12.1 [93] Section 8.1, as per MEF 4:

> *"The UNI-C is a compound architectural component of a MEN that represents all of the functions required to connect a subscriber to a MEN …"*

For purposes of this document the UNI-C is managed by the Mobile Operator (called "Subscriber"), i.e. at RAN sites.

The UNI-N, as defined in Section 7.1.2/MEF 4 and MEF 12.1, as per MEF 4:

> *"The UNI-N is a compound architectural component of a MEN that represents all of the functions required to connect a MEN to a MEN subscriber. The individual functions in a UNI-N are entirely in the service provider/network operator domain."*

For the purposes of this document the UNI-N is managed by the MEN Operator ("Service Provider").

Based on MEF 11 [92], this document assumes that the UNI-C or UNI-N functions can be distributed across one or more NEs in such a manner that all the required UNI functions are performed on all ingress and egress Service Frames at the UNI reference point.

4.3.2.1.3 Realization

The Broadband Forum's MBH reference architecture and equipment requirements specified in this Technical Report support MEF MBH services and constructs. Specifically Technical Report supports three cases:

- Provides MEF Service: the MPLS Network provides the MEF Ethernet service using VPWS and VPLS to transport IP TNL for which the MEF EVC concept can be mapped. That is, an MEF EVC used for mobile backhaul can be realized with an MPLS network as described in this document.
- Uses a MEF service: the MPLS network provides any service while some portion of the MPLS network uses a MEF Ethernet service.
- Does both: above scenarios can be combined, where the MPLS network both provides and uses MEF Ethernet service.

The following figures show the mappings between TR-221 architecture and MEF 22.1 architecture. The distinction between the figures is the location of the MEF UNIs. The location depends on whether or not the MPLS network (i) provides MEF Service (as in Figure 4), (ii) uses a MEF Service (as in Figure 5) or (iii) both (as in Figure 6). The scope of MEF service constructs in a Broadband Forum's MBH architecture is shown as an EVC being an association of MEF UNIs.

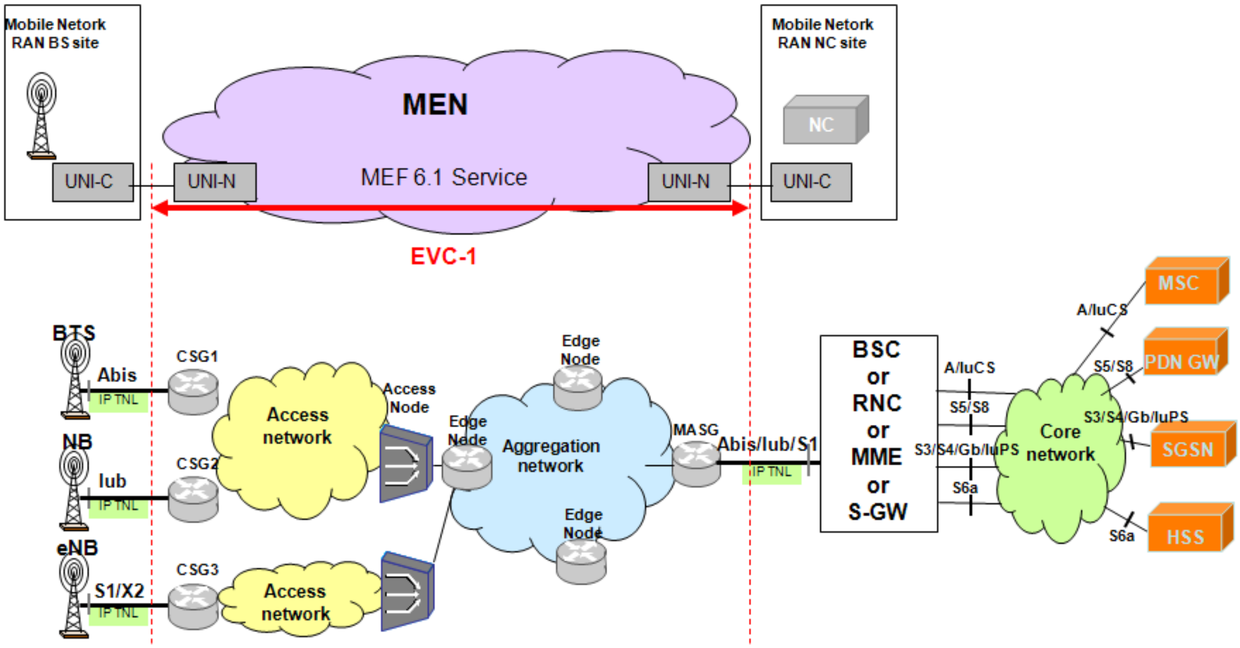


Figure 4: MPLS Networks provides MEF Service

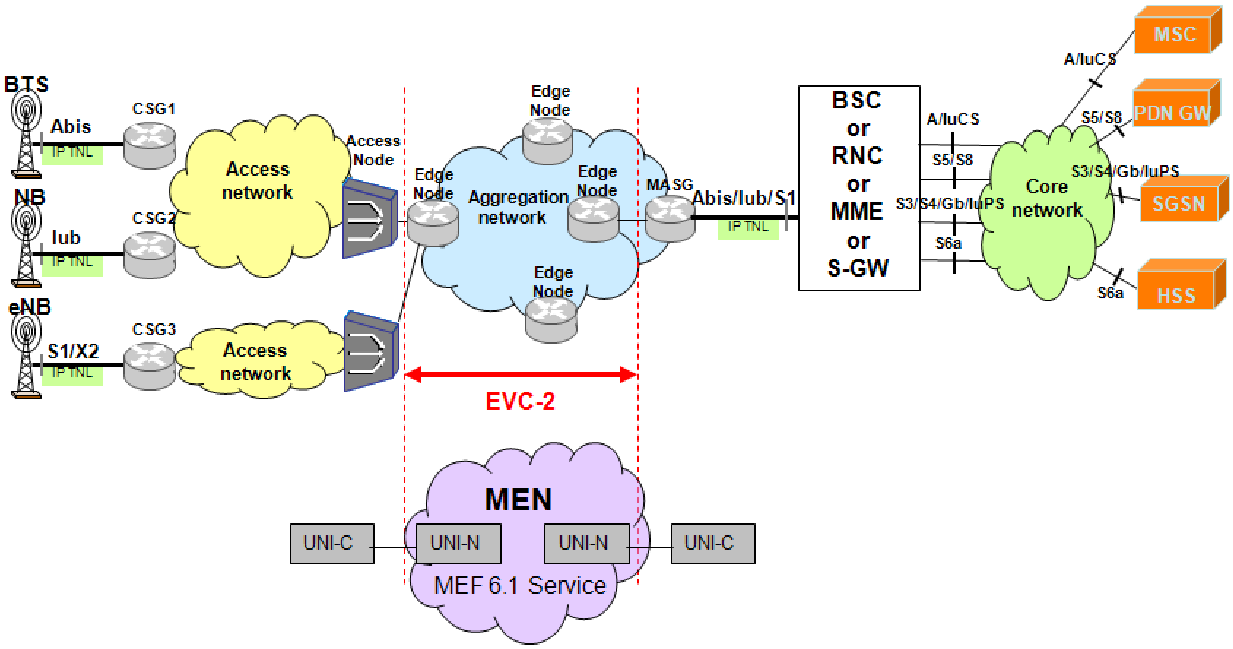


Figure 5: Example of an MPLS Networks uses MEF Service

Figure 5 provides an example of an MPLS network that uses a MEF Ethernet Service for some parts of the network. In the case where the MEN is implemented using MPLS, this is the overlay model as defined in Section 4.2, Figure 16 and Section 5.2.5.

Note: Figure 5 depicts an example of the UNI placement. The EVC-2 can reach up to the back of the CSG or to any point in between. The remainder of the connectivity from the termination of the UNI-C to the CSG is beyond the scope of the document. E.g. the UNI-C in the Figure 5 may terminate at an AN and the remainder of the connectivity to the CSG is provided with a DSL or xPON service or a microwave link.

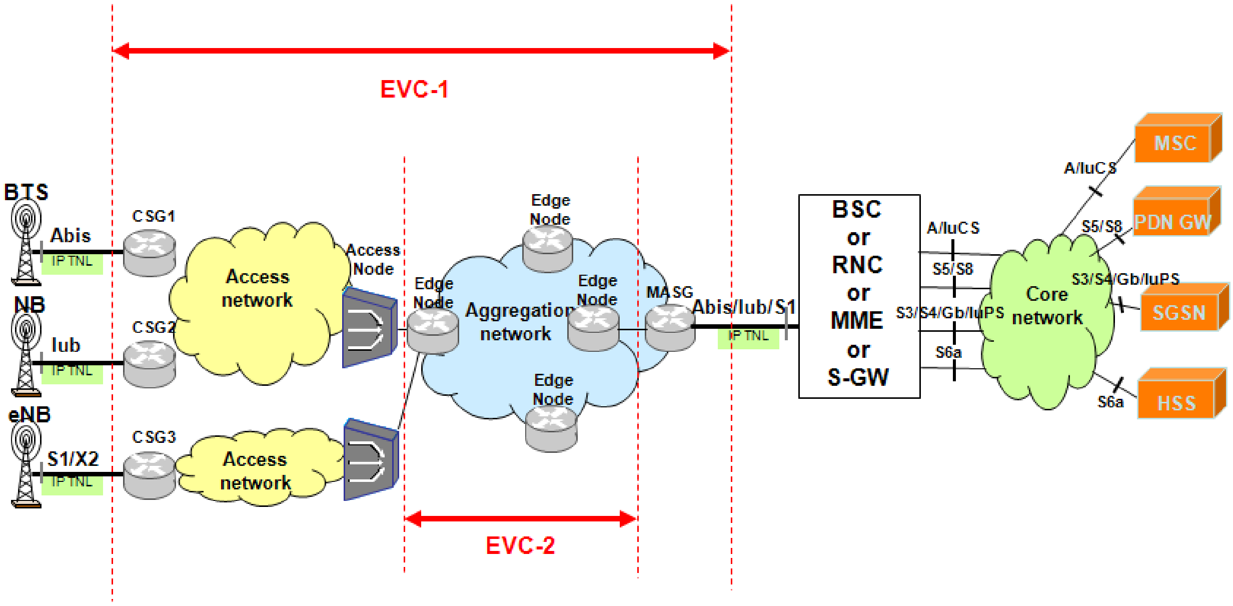


Figure 6: MPLS Networks Provide and Use MEF Service Simultaneously

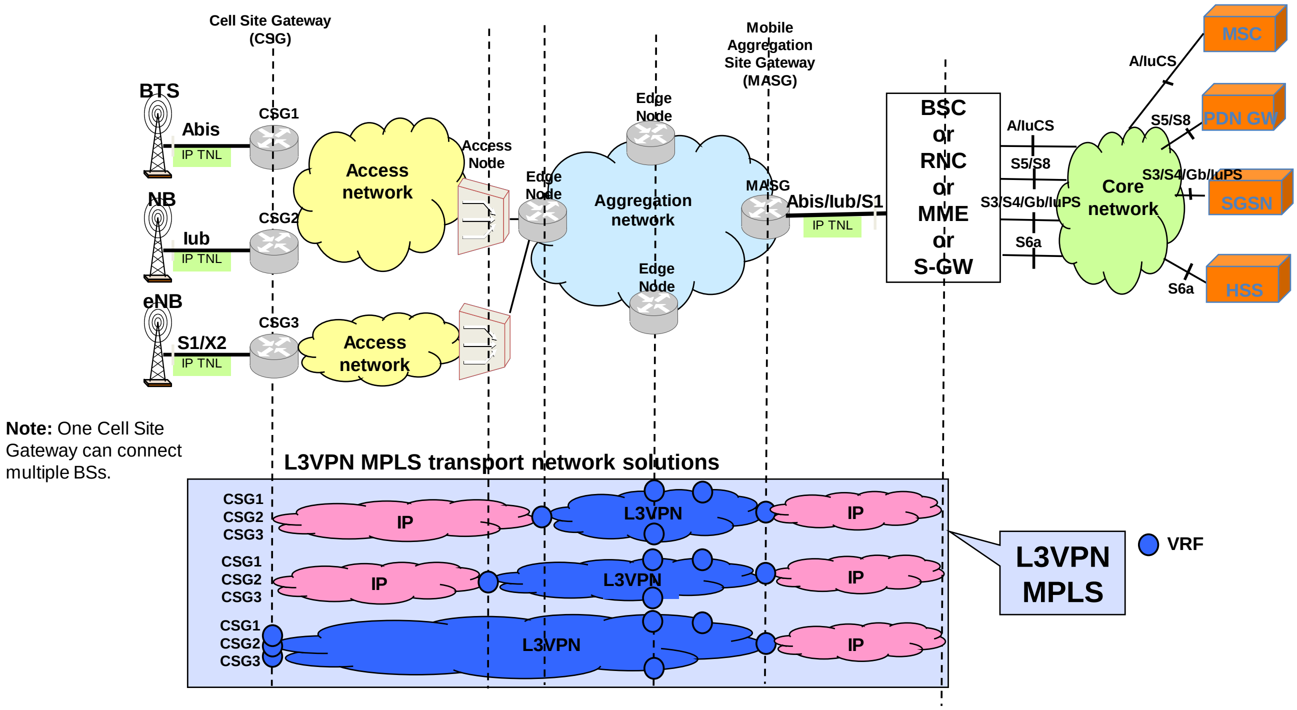
4.3.3 L3VPN MPLS connectivity for IP TNL

Figure 7 provides the reference architecture for L3VPN solutions RFC 4364 [27] in the mobile backhaul network for 2G/3G using IP TNL or LTE, 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 unique L3 VPN MPLS transport solution RFC 4364 [27] could be used to backhaul both S1 and X2 interfaces in order to get a converged and efficient network solution for LTE.

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 RFC 4364 [27] and support QoS and Traffic Engineering. The VPNs provide layer 3 connectivity across the backhaul network and provide any to any topology to support both X2 and S1 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.



Note: One Cell Site Gateway can connect multiple BSs.

Figure 7: Reference Architecture of L3VPN MPLS connectivity for IP TNL

The connectivity between the mobile nodes and the L3VPN PE router can be provided by a native layer 2 technology or emulated using VPWS or VPLS, for example.

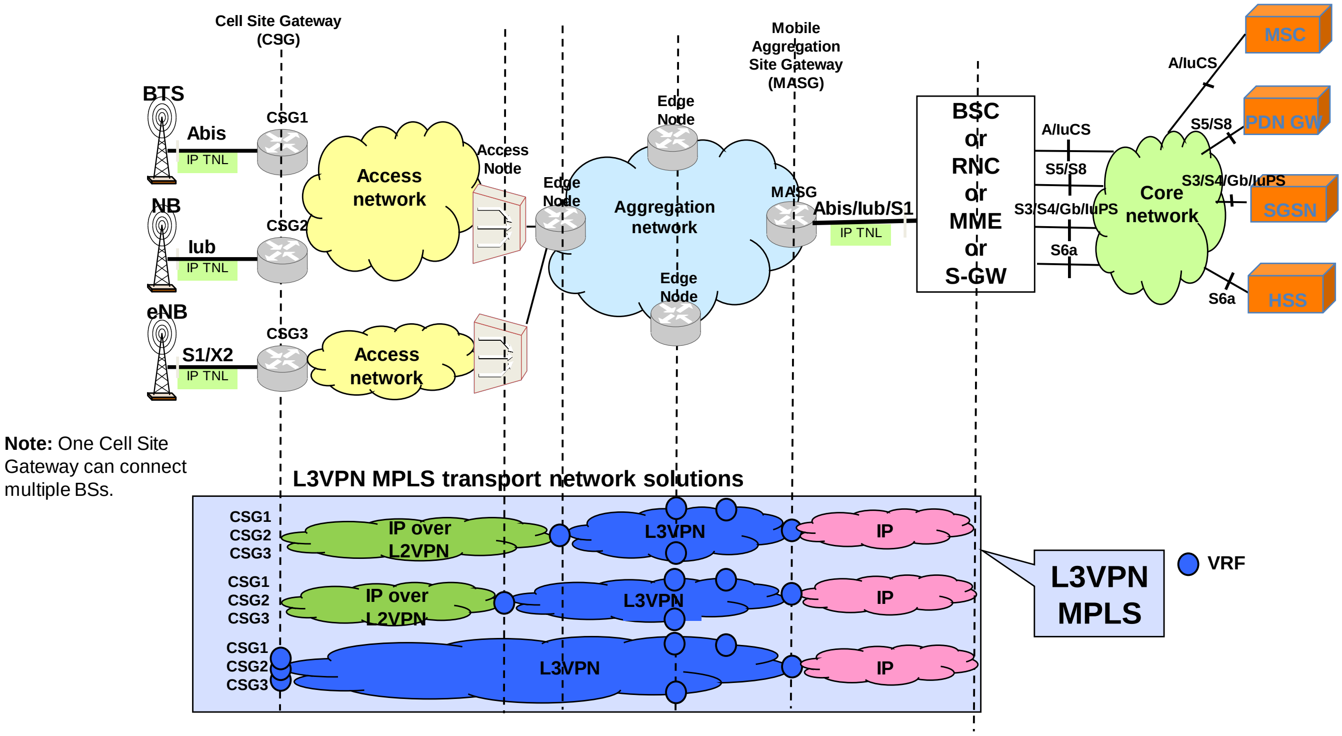
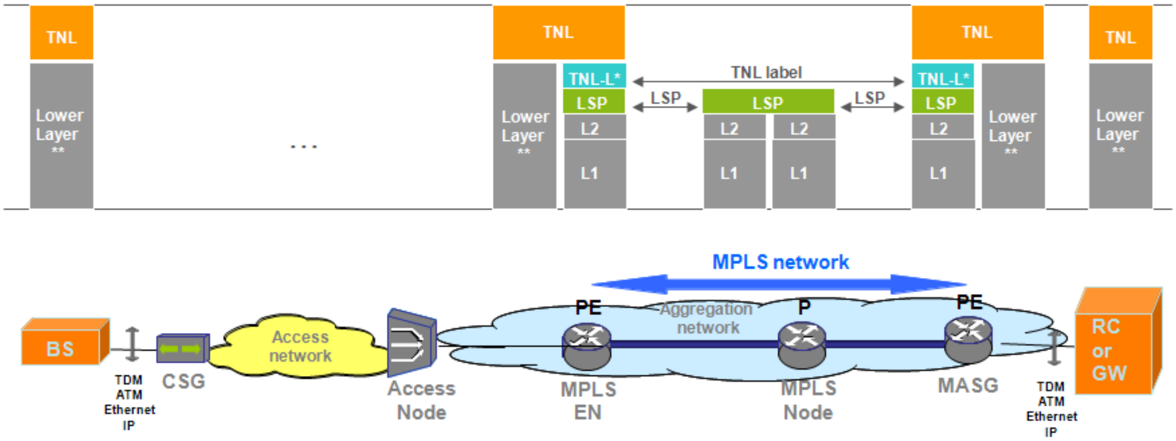


Figure 8: Reference Architecture of L2VPN Access to an L3VPN

4.4 Protocol Stacks

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



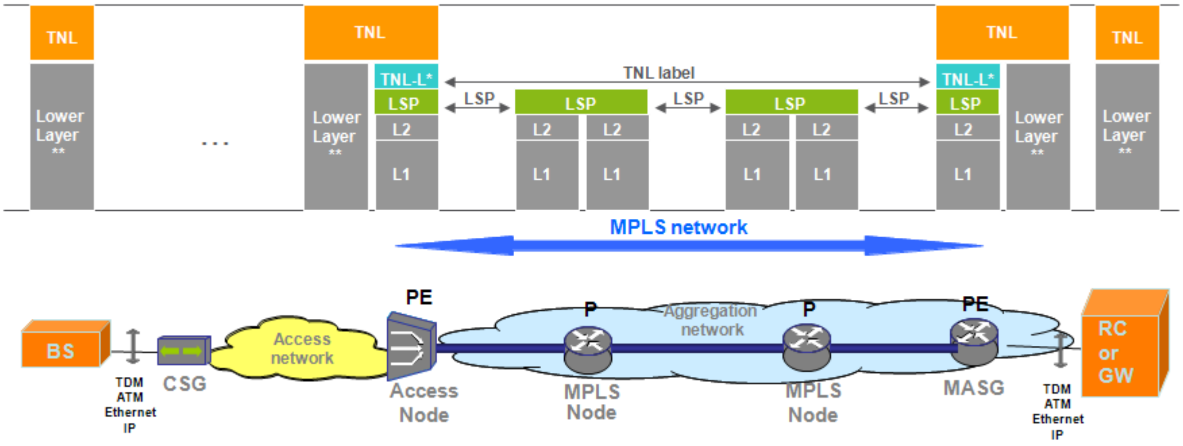
TNL-L* means TNL specific label (if any)

for TDM or ATM or Ethernet – PW label;
for L3 VPN – VPN label;
for IPoLSP – no label (empty)

Lower Layer ** means layers carrying TNL

for TDM or ATM or Ethernet – L1
for IP – L2 + L1

Figure 9: Protocol stacks used for TNL Transport in Use Case a



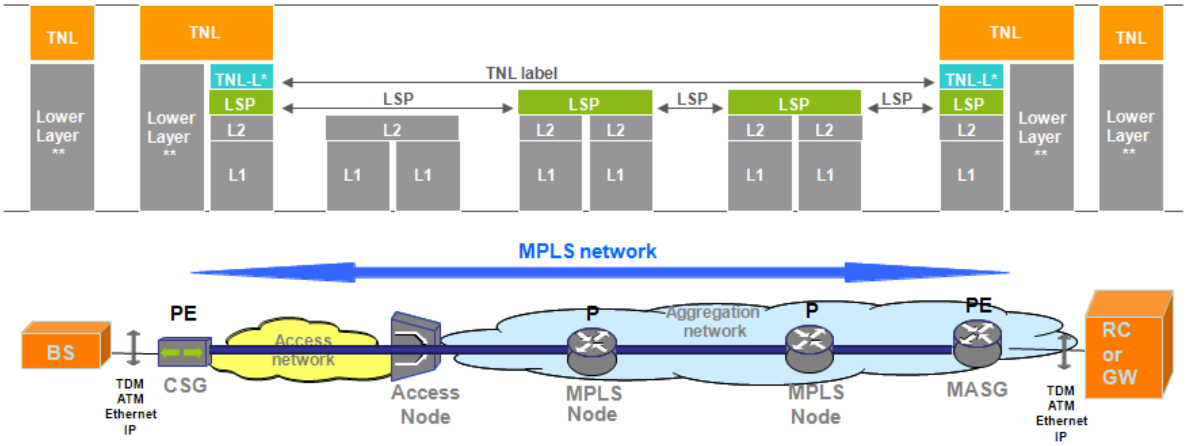
TNL-L* means TNL specific label (if any)

for TDM or ATM or Ethernet – PW label;
for L3 VPN – VPN label;
for IPoLSP – no label (empty)

Lower Layer ** means layers carrying TNL

for TDM or ATM or Ethernet – L1
for IP – L2 + L1

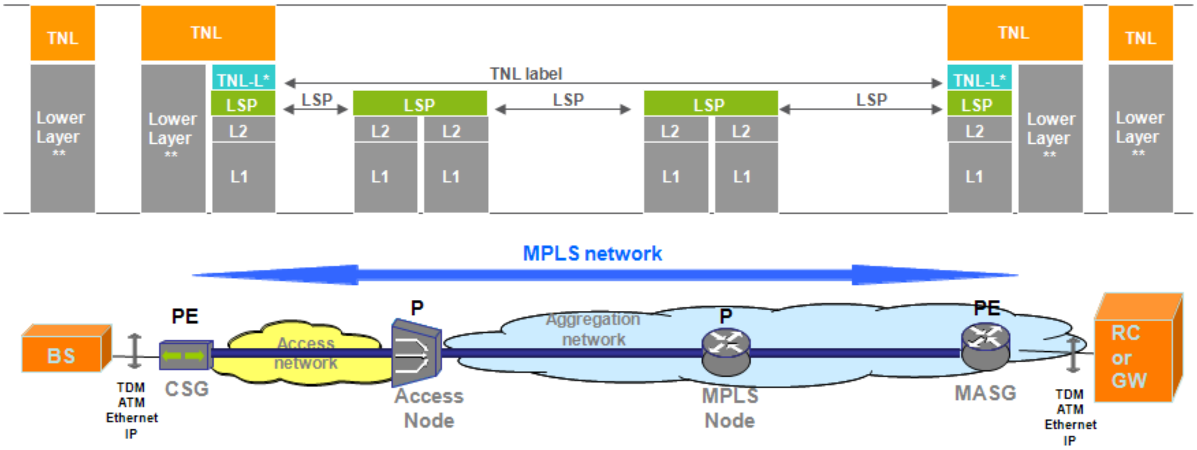
Figure 10: Protocol stacks used for TNL Transport in Use Case b



TNL-L* means TNL specific label (if any) for TDM or ATM or Ethernet – PW label;
for L3 VPN – VPN label;
for IPoLSP – no label (empty)

Lower Layer ** means layers carrying TNL for TDM or ATM or Ethernet – L1
for IP – L2 + L1

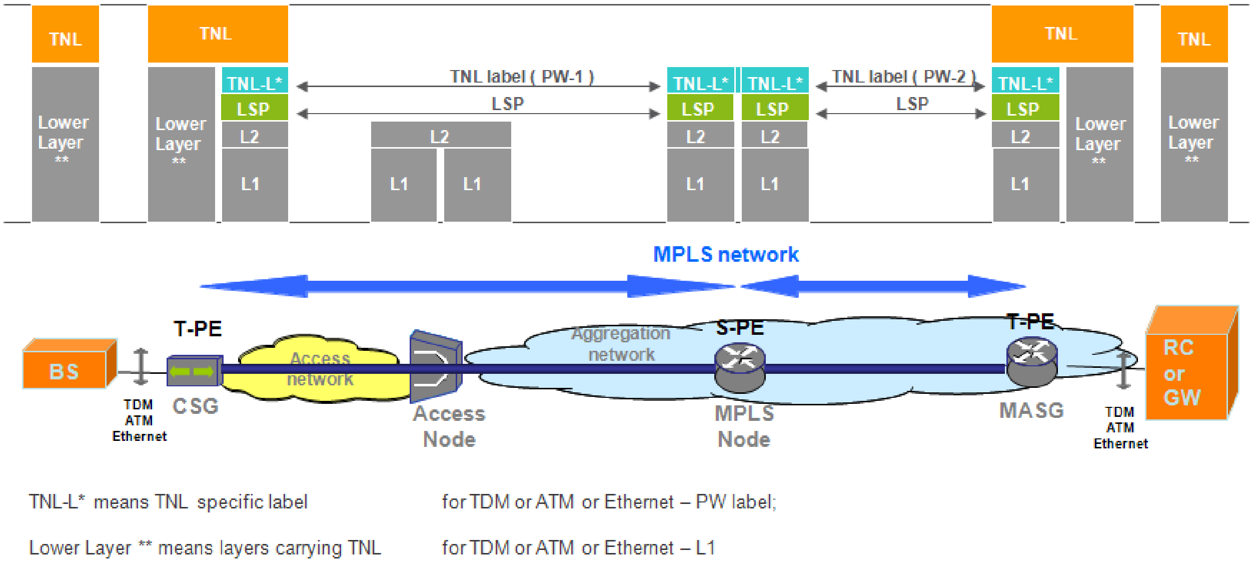
Figure 11: Protocol stacks used for TNL Transport in Use Case c



TNL-L* means TNL specific label (if any) for TDM or ATM or Ethernet – PW label;
for L3 VPN – VPN label;
for IPoLSP – no label (empty)

Lower Layer ** means layers carrying TNL for TDM or ATM or Ethernet – L1
for IP – L2 + L1

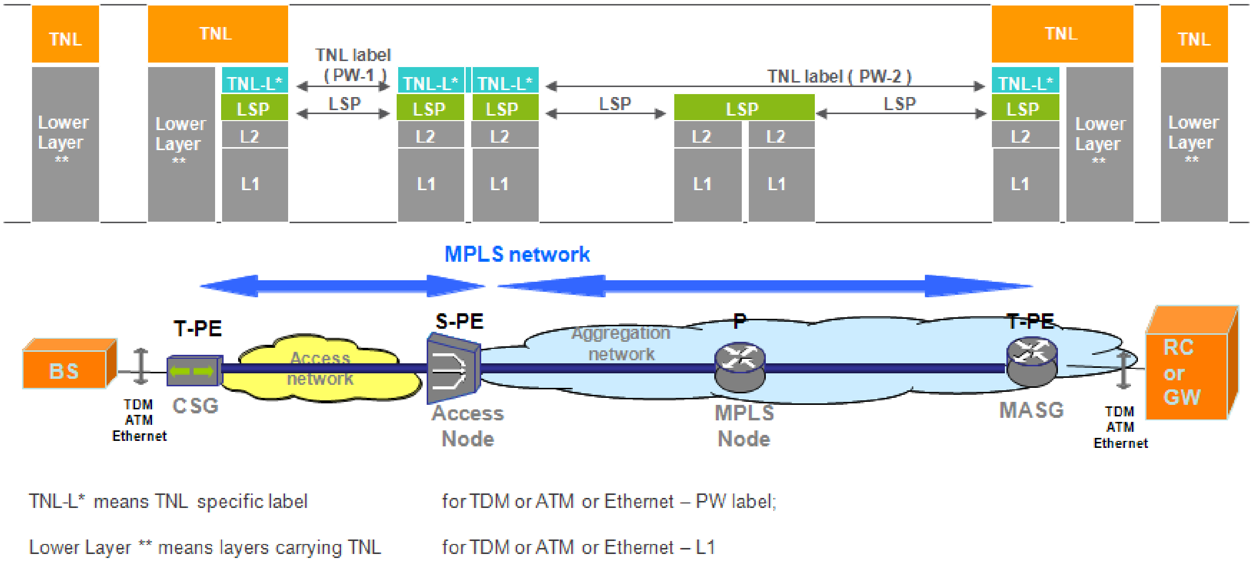
Figure 12: Protocol stacks used for TNL Transport in Use Case d



TNL-L* means TNL specific label for TDM or ATM or Ethernet – PW label;

Lower Layer ** means layers carrying TNL for TDM or ATM or Ethernet – L1

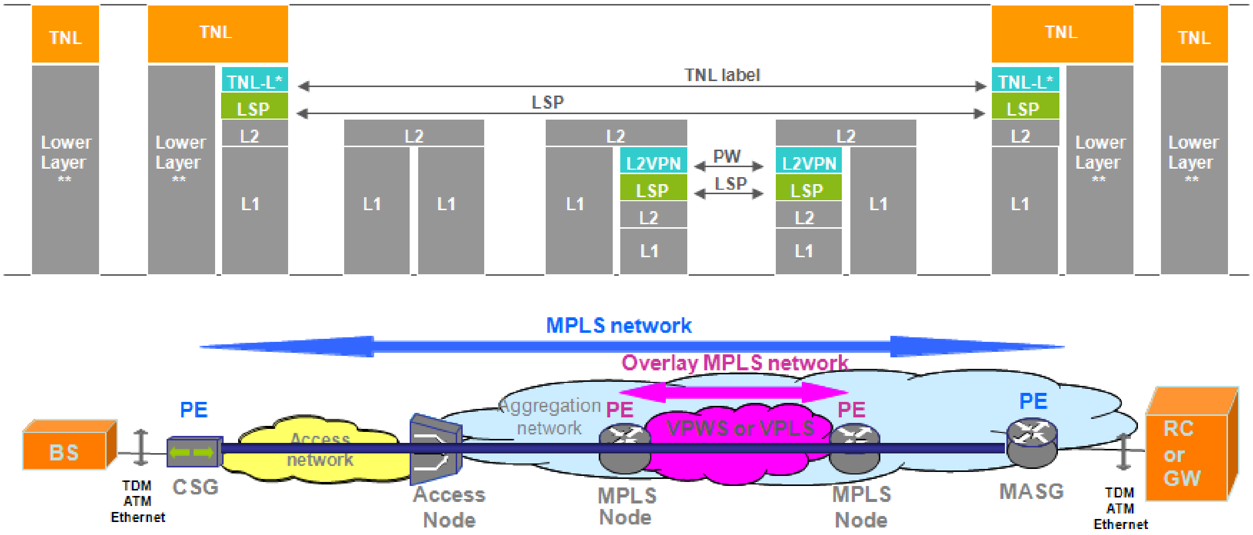
Figure 13: Protocol stacks used for TNL Transport in Use Case e



TNL-L* means TNL specific label for TDM or ATM or Ethernet – PW label;

Lower Layer ** means layers carrying TNL for TDM or ATM or Ethernet – L1

Figure 14: Protocol stacks used for TNL Transport in Use Case f



TNL-L* means TNL specific label for TDM or ATM or Ethernet – PW label;

Lower Layer ** means layers carrying TNL for TDM or ATM or Ethernet – L1

Figure 15: Protocol stacks used for TNL Transport in MPLS Use Case (c) with Overlay Model in Aggregation Network

5 Generic specifications (Equipment Specifications/Requirements)

This section describes specifications, solutions and nodal requirements for MPLS in Mobile Backhaul networks that are common to some or all of the TNL scenarios described in Section 4. The requirements in this section apply to all node roles unless otherwise indicated.

5.1 Signaling and routing

5.1.1 PSN Tunnel LSP signaling

[R1] PE and P routers supporting MPLS TE and non-TE LSPs MUST support one or both of the following methods:

- Static provisioning
- Dynamic signaling

[R2] 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 RFC 5036 [44].
- RSVP-TE is used to set up, maintain and release LSPs for traffic engineered tunnels per RFC 3209 [14] and RFC 5151 [47]. When traffic engineering is needed on the LSP, RSVP-TE MUST be used.
  - For local protection using RSVP-TE see Section 5.3.3.3.

[R3] When co-routed bidirectional LSPs are required, GMPLS-RSVP-TE as per RFC 3473 [18] MAY be supported by PE and P routers.

5.1.2 PSN Tunnel LSP routing

[R4] One or both of the following methods MUST be used when dynamic signaling is supported by PE and P routers:

- Static routing
- Dynamic routing

[R5] If dynamic routing is supported, both of the following methods MUST be supported by PE and P routers to exchange routing information to facilitate dynamic LSP signaling:

- OSPF (RFC 2328 [10])
- IS-IS (RFC 1195 [6])

[R6] 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 (RFC 3630 [20])
- IS-IS-TE (RFC 5305 [50])

5.1.3 PW signaling

[R7] One or both of the following methods MUST be used for PWs:

- Static provisioning
- Dynamic signaling

[R8] PE routers MUST support Single Segment Pseudowire (SS-PWs) as per RFC 3985.

[R9] PE and P routers SHOULD support static provisioned Multi-Segment Pseudowire (MS-PW) as per RFC 6073 [64]

When PE and P routers support Dynamic signaled PWs the following apply:

[R10] MUST support pseudowire setup, maintenance and release of PWs as per RFC 4447 [33] with FEC 128

[R11] SHOULD support pseudowire setup, maintenance and release of PWs as per RFC 4447 [33] with FEC 129

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

5.2 OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels and pseudowires used to transport the various TNLs over MPLS. OAM is an important and fundamental functionality in mobile backhaul networks. OAM contributes to the reduction of operational complexity, by allowing for efficient and automatic detection, localization, handling and diagnosis of defects. OAM functions, in general, may be used for fault-management, performance-monitoring, and used by protection-switching applications.

5.2.1 LSP OAM

This section describes techniques to perform OAM for the underlying MPLS LSPs used in a mobile backhaul application for carrying PWs, L3VPNs and IP services over MPLS.

LSP-Ping (RFC 4379 [29]) and Bidirectional Forwarding Detection (BFD) (RFC 5880 [57]) are OAM mechanisms for MPLS LSPs. The following OAM mechanisms are supported:

BFD for MPLS LSPs

It monitors the integrity of the LSP for any loss of continuity defect. In particular, it can be used to detect a data plane failure in the forwarding path of an MPLS LSP.

[R12] PE and P routers MUST support BFD for MPLS LSPs as per RFC 5884 [60]

Detecting MPLS Data Plane Failures

Used to perform on-demand Connectivity Verification, Route Tracing and Adjacency functions. It provides two modes: “ping” mode and “traceroute” mode.

In "ping" mode (basic connectivity check), the packet should reach the end of the path, at which point it is sent to the control plane of the egress LSR, which then verifies whether it is indeed an egress for the FEC.

[R13] PE and P routers MUST support “ping” mode as per RFC 4379 [29].

In "traceroute" mode (fault isolation), the packet is sent to the control plane of each transit LSR, which performs various checks that it is indeed a transit LSR for this path; this LSR also returns further information that helps check the control plane against the data plane.

[R14] PE and P routers SHOULD support “traceroute” mode as per RFC 4379 [29].

The LSP Ping Reply modes as defined in RFC 4379 Section 3 apply as shown in Table 3

Reply Mode	Echo request	Echo Reply
Reply via an IPv4/IPv6 UDP packet (code value 2)	MUST	MUST
Reply via application level control channel (code value 4)	MAY	MAY

Table 3 – LSP Ping Reply Modes

[R15] The following subsections of RFC 4379 [29] Section 3.2 concerning Target FEC Stack apply as follows:

- When using LDP - LDP IPv4 prefix as defined in Section 3.2.1 MUST be supported.
- When using RSVP - RSVP IPv4 LSP as defined in Section 3.2.3 MUST be supported.
- When using BGP - BGP labeled IPv4 prefix as defined in Section 3.2.11 MUST be supported.
- When using LDP - LDP IPv6 prefix as defined in Section 3.2.2 SHOULD be supported.
- When using RSVP - RSVP IPv6 LSP as defined in Section 3.2.4 SHOULD be supported.
- When using BGP - BGP labeled IPv6 prefix as defined in Section 3.2.12 SHOULD be supported.

5.2.2 Native service OAM

Native service OAM is dependent on the native service being provided and therefore is TNL specific. See each of the individual TNL sections for related native service OAM information.

5.2.3 PW OAM

This section defines the common PW requirements for all TNLs. For requirements on OAM message mapping please see the specific TNL sections below.

5.2.3.1 Single Segment Pseudowire (SS-PW) OAM

[R16] The VCCV Control Channel (CC) Type per RFC 5085 [45] applies as follows:

- VCCV Control Channel Type 1, also known as "PWE3 Control Word with 0001b as first nibble", MUST be supported. This control channel type allows the OAM messages to follow the same forwarding path of the associated traffic even in the case of ECMP hashing.

- VCCV Control Channel Type 3, also known as "MPLS PW Label with TTL == 1", MAY be supported. This type is more compatible with existing deployments if control word is not enabled. But the OAM message may not follow the same forwarding path of the associated traffic in the case of ECMP hashing.

Note: VCCV Control Channel Type 2, also known as “MPLS Router Alert Label”, is not applicable to this document.

[R17] For each of these control channels supported, VCCV profile 1 MUST be supported and VCCV Profile 2 SHOULD be supported as described in Section 3.1 and 3.2/RFC 5994 respectively. Please note that RFC 5994 [63] refers to RFC 5885 [61] for detailed description and usage of Connection Verification (CV) types.

[R18] When the PW is established using static provisioning, fault notification (i.e. status signaling) is supported as follows:

- BFD status signaling using diagnostic codes per the VCCV profile supported SHOULD be used
- Static PW status signaling per draft-ietf-pwe3-static-pw-status [73] MAY be used.

[R19] When LDP is supported for PW establishment, fault notification MUST be supported per RFC6310 [67] by PE routers.

[R20] MPLS LSP Ping (CV type 0x02) SHOULD be supported per RFC 5085 [45].

5.2.3.2 Multi-Segment Pseudowire (MS-PW) OAM

<u>VCCV Control Channel Types</u>

[R21] VCCV control channels types are supported per 5.2.3.1 section above. For additional tools addressing S-PEs, VCCV channels types MUST be supported per RFC 6073 [64].

<u>VCCV-BFD</u>

VCCV-BFD is run end-to-end between T-PEs, similar to the SS-PW application. This operation is transparent to the S-PE.

<u>VCCV Connectivity Verification (Ping) and VCCV Path Verification & Path Trace (Traceroute)</u>

If MS-PW are supported, the following requirements apply in addition to Section 5.2.3.1:

[R22] End-to-end MS-PW connectivity verification SHOULD be supported per Section 9.6/RFC 6073.

[R23] Partial MS-PW connectivity verification SHOULD be supported per Section 9.6/RFC 6073.

[R24] Pseudowire Switching Point PE sub-TLV Type SHOULD be supported as per RFC 6073.

[R25] The S-PE MUST support including the label stack in the Pseudowire Switching Point PE sub-TLV as per the FEC 129 encoding in Section 3.2.10/RFC 4379 [29].

[R26] MS-PW Path Verification MAY be supported as per Section 9.6/RFC 6073 [64], to verify the path of the MS-PW against the actual data path of the MS-PW.

[R27] MS-PW Path Trace MAY be supported as per Section 9.6/RFC 6073. The sending T-PE or S-PE recursively test each S-PE along the path of the MS-PW, exercising the FECs recorded from the Target FEC stack TLV [RFC 4379] returned by S-PEs or T-PEs in an echo reply message. This enables to determine the actual data path of the MS-PW and can be used for both statically configured and signaled MS-PWs.

5.2.4 Packet Loss and Delay Measurement

The ability to monitor performance metrics (i.e. packet loss, one-way and two-way delay) for Label Switched Paths and Pseudowires provides service level measurements to the service provider.

[R28] PE and P routers SHOULD support loss and delay measurement per RFC 6374 [68]

5.2.5 MEF Service 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.

[R29] CSG and MASG supporting this scenario MUST support the requirements in MEF 22.1 [96] Section 8 with the following additions.

- Ethernet Link OAM: when the CSG or the MASG supports being directly connected to the network demarcation point, Link OAM features MUST be supported and the CSG or MASG acts in Slave mode as described in IEEE 802.3ah [4]
- As MEF UNI service is provided by the Carrier, MEF SOAM levels 5 to 7 MUST be supported by the L2VPN. OAM frames are sent as user data and carried transparently over the L2VPN.

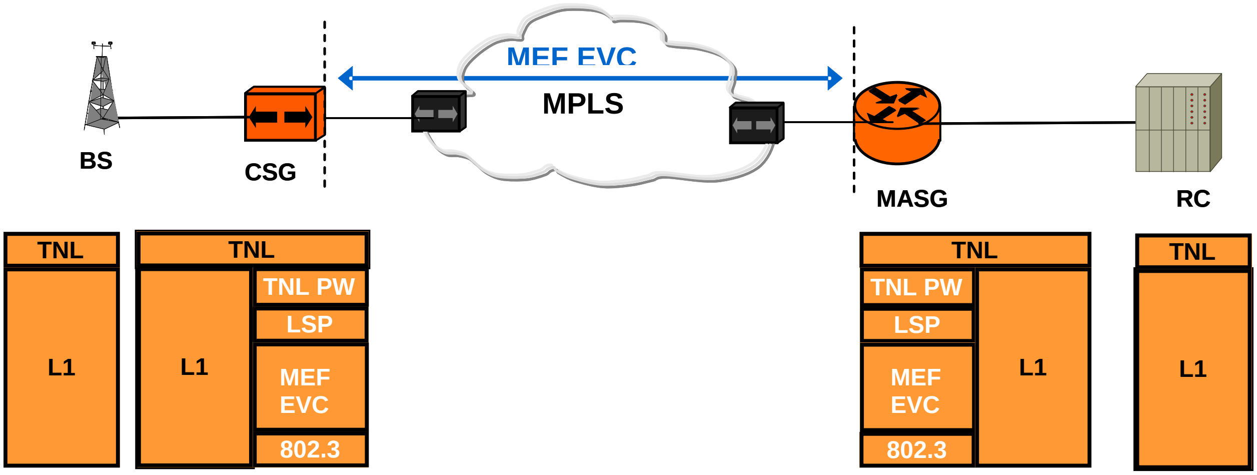


Figure 16: OAM for Ethernet managed services

5.3 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 in the underlying LSPs and pseudowires.

Not all parts of the mobile backhaul network require or support network resiliency; consideration should be given to the physical topology available before a decision on which particular resiliency scheme (or schemes) should be used.

For example, fast service recovery features can be provided by RSVP-TE, including path and local protection schemes. They can be enabled for those parts of the transport network where some form of protection is required.

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 MASG direction, and the reader will understand that the opposite direction needs to be similarly addressed.

Depending on criteria such as provisioning complexity, topology and recovery time, LSP Path protection or local protection may be used across the mobile backhaul network or in part of the mobile backhaul network to facilitate resiliency.

LSP Path protection may be preferred in circumstances where it offers better control of the end-to-end traffic-engineered protection path. It also manages the scenario where a working LSP has a failure in an area where the local protection has not been enabled.

One particular consideration during deployment is that the protected LSPs not share fate with the working LSP, that is to say they are in different shared risk links groups (RFC 3386 [16]). This would imply that the set of LSPs and PWs in the 2 paths (working and protected) would be in different SRLGs. This can be done using different methods such as, alternate route, routing metrics and signaled path specification to the destination.

To detect LSPs failures in a reliable and robust manner, an OAM mechanism such as MPLS BFD (see section 5.2.1 LSP OAM) should be used for LSPs. E.g. this is particularly important to detect end-to-end failure of the LSPs.

For typical mobile backhaul deployment scenario, the following considerations apply:

- In many cases the Cell site doesn’t necessarily need to be protected at the transport level because it is protected at higher layer such as radio or RAN level. These higher protection levels are outside of the scope of the document.
- In many cases the Radio Controller site does need to be protected at the transport level. This would be due to, for example, the concentration of the traffic at one centralized point and the possible lesser presence of protection at the RAN level.
- AC protection mechanisms are technology specific, and are beyond the scope of this specification.

5.3.1 Scope of resiliency

In this specification “resiliency” means protection switching (LSP tunnel, PW, or L2 link protection) between the MASG and the CSG, or between the MASG and another PE acting as an Access node or an Edge node. 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 [16], 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/MPLS or PW 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 MPLS layer. The specific algorithm of protection switching implemented at each node is beyond the scope of this specification.

5.3.2 Link resiliency at Layer 2

The figure below describes existing Mobile Point of Presence (PoP) connectivity with Network Operators. As these PoPs typically aggregate large quantities of NodeB services, it is required that they be protected by at least two disjoint physical links.

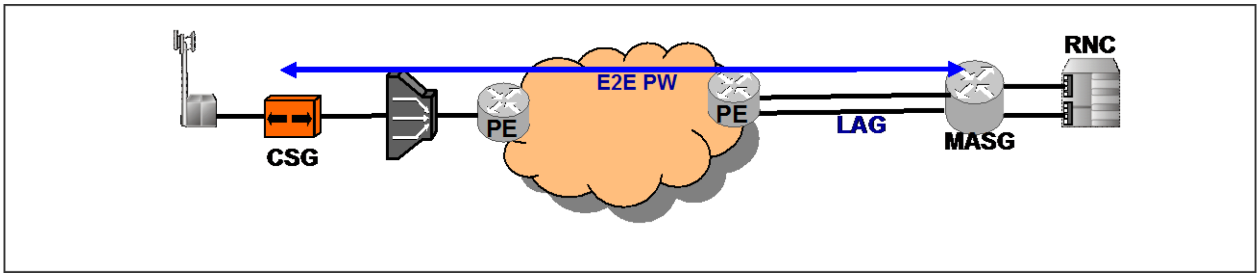


Figure 17: Mobile connectivity with LAG in the overlay model

A PE compliant with this specification that functions as an MASG must support an L2 link protection mechanism. L2 link protection is implemented in the large mobile PoPs. For example protection here is based on L2 link aggregation.

[R30] For Ethernet links between the PE and MASG, both equipments MUST support LAG as defined in IEEE 802.1AX-2008 [2].

Others link aggregation methods used for protection are outside the scope of the document.

5.3.3 LSP resiliency

The aggregation network provides resiliency, and the CSG and MASG need to support either end-to-end LSP protection or segment protection. When supporting segment protection we can identify three segments:

- from the CSG to the aggregation network
- the aggregation network itself
- from the aggregation network to the MASG(s)

It is also possible to combine both end-to-end protection and protection of specific segments (e.g. when an LSP is protected from end to end using working and protecting LSP as well as segment protection between CSG and MASG using FRR). In such cases the setting of the fail over timer values must be carefully considered to coordinate between layers.
If protection switching is required, the protection path may need to be set up ahead of time depending on the recovery time requirement. This can be accomplished by static configuration or by using an appropriate signaling protocol.

[R31] For End to End Tunnel Resiliency the single hop MUST be supported as per RFC 5881 [58]. For the remaining BFD requirement see Section 5.2.1 LSP OAM section.

[R32] For End to End Tunnel Resiliency the Multi-hop Option MUST be supported as per RFC 5883 [59]. For the remaining BFD requirement see Section 5.2.1 LSP OAM section.

Tunnel redundancy can be implemented using single-homed or dual-homed topologies, where in the single-homed case the protected tunnels are terminated at one PE, and in the dual–homed case the tunnels are terminated at two PEs. Dual-homed tunnel resiliency is for further study.

If traffic is to be switched back from protect LSPs to working LSPs it is recommended that enough time be allowed for the working to become stable before the switch back is attempted. Not doing this may result in oscillating failover between the working and protected LSPs.

5.3.3.1 End to End LSP protection

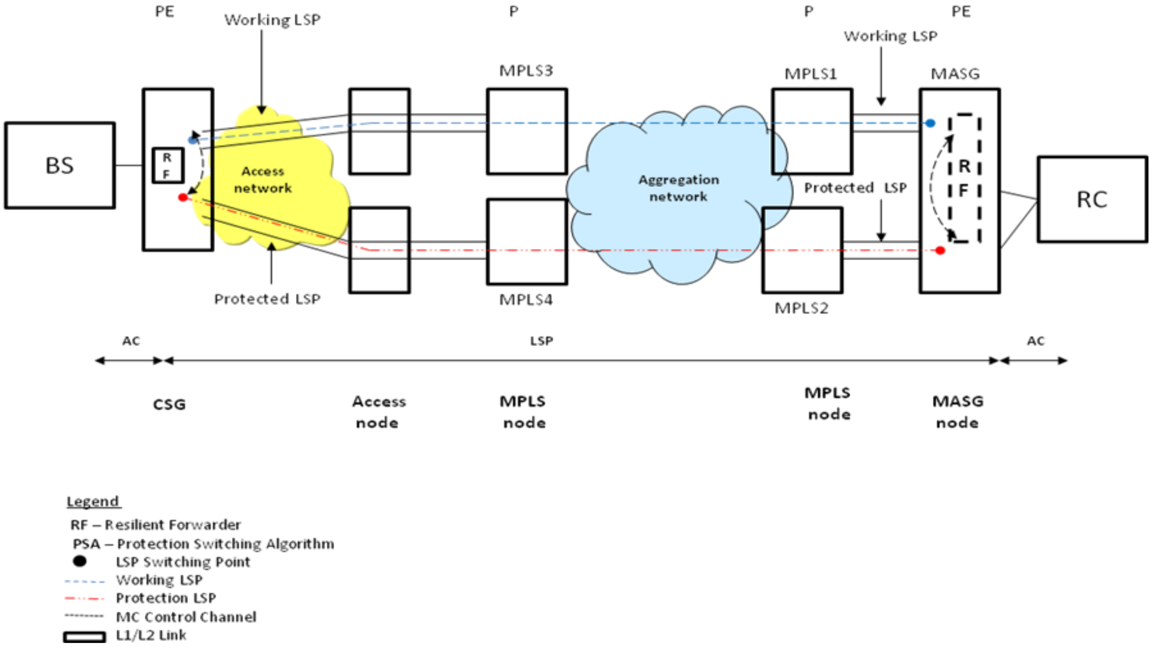


Figure 18: End to End LSP protection – single-homed

`

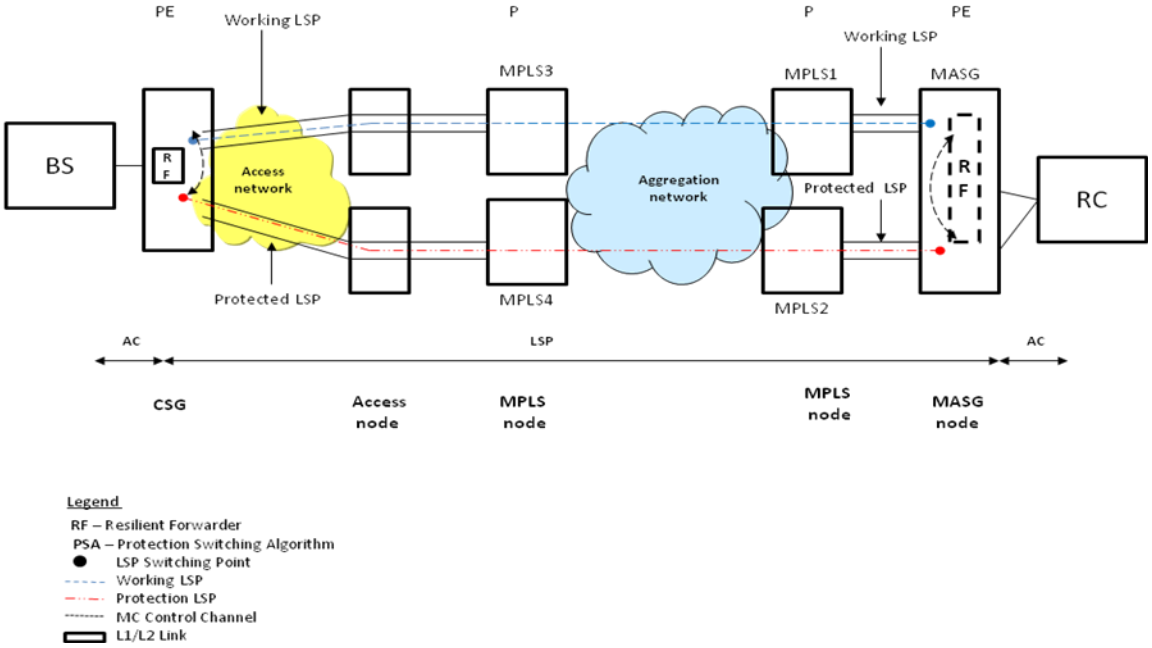


Figure 18 depicts End to End LSP protection when the head-end and tail-end of the LSP reside on the CSG and MASG respectively or vice versa. Any failure in the network, including failure of segment protection, should cause end to end LSP protection switching. In order to maximize survivability, it is desired to ensure that the working and redundant (protection channel) LSPs run over distinct L1/L2 segments. When the CSG or the MASG detects a failure of the working LSP, it must switch over to the redundant LSP and notify its peer.

5.3.3.2 Sub Network Connection Protection (LSP segment protection)

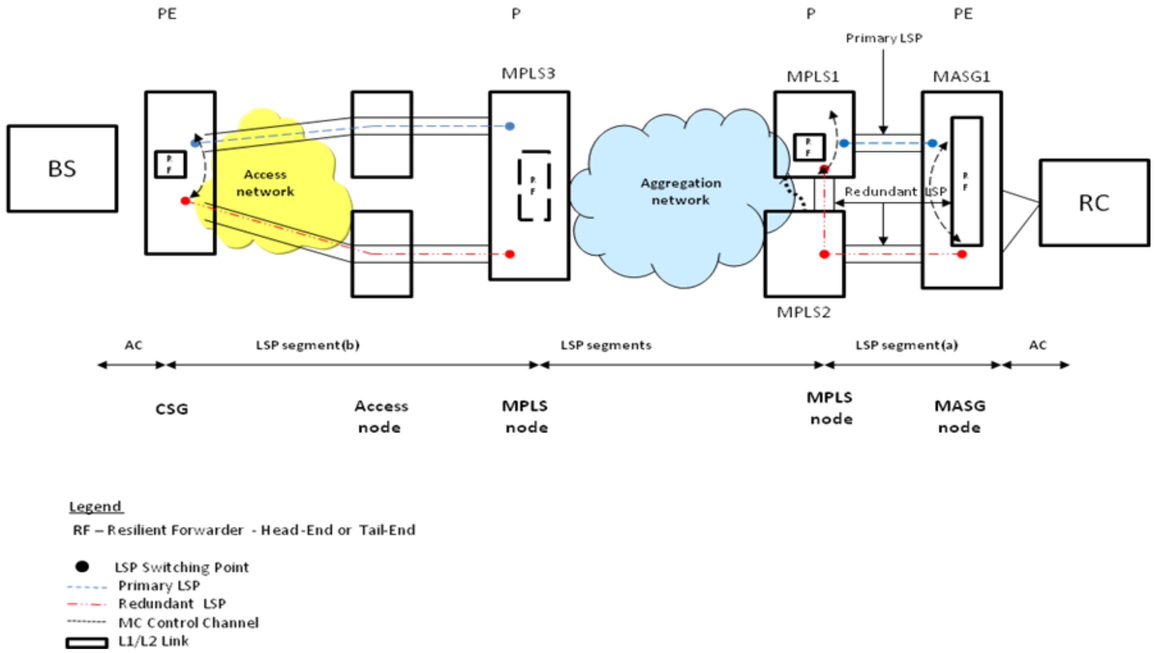


Figure 19: SNCP- Subnet Network Connection LSP Protection (the two P-router cases are depicted) single-homed case

In this case both non-aggregation-network LSP segments are protected. For the first segment (between the CSG and the aggregation network) the working and redundant LSPs run over distinct L1/L2 links over two access nodes (L2 only) and from there to an aggregation network P-router (MPLS3). In the CSG to MASG traffic direction, the head-end of the first segment is the CSG. Its tail-end is the aggregation network P-router. Similarly, for the last segment (between the aggregation network and the MASGs) the working and redundant LSPs run over distinct L1/L2 links from two P-routers towards one PE-router. In order to fully protect this segment against link failures, minimizing out-of-service time, the detours must be preconfigured or signaled.

5.3.3.3 LSP resiliency requirements

A PE compliant with this specification has to support tunnel protection requirements mandated by this section.

[R33] The PE and P routers implementing the LSP resiliency mechanisms of this specification SHOULD restore traffic flow within 250 milliseconds after receipt of failure notification.

Note: The PE routers can support re-optimization on working and protection tunnels.

[R34] PE nodes that implement Linear Protection MUST be capable of assigning Working and Protect roles to LSPs.

[R35] A CSG MAY support LSP protection over two L1/L2 links. E.g. the node may be able to route a working LSP over one L1/L2 link and the protect LSP over a different L1/L2 link.

[R36] An MASG MUST support LSP protection over two L1/L2 links.

Dual homed protection mechanisms are for further study.

In case the tunnels are TE tunnels then the following apply:

MASG (PE router)	**CSG (PE router)**	**P router**	**Requirement**
MUST	MAY	MUST	**[R37]** If local protection switching is required then the router supports Fast ReRoute (FRR) around mobile BH link failure or router node failure as per RFC 4090 [25].
MUST	MAY	MUST	**[R38]** Router supports Facility backup function as defined in Section 3.2/RFC 4090.
SHOULD	MAY	SHOULD	**[R39]** Router supports One to One backup as defined in Section 3.1/RFC 4090.
MUST	MAY	MUST	**[R40]** In order to provide for continuous service when RSVP-TE signaling is used and the router control plane fails, routers support RSVP-TE graceful restart in Section 9/RFC 3473 [18] as well as graceful restart for the routing protocols upon which RSVP-TE path computation depends.
MUST	MAY	MUST	**[R41]** If LDP is used for signaling LSPs, in order to provide for continuous service when the router control plane fails, routers support LDP graceful restart RFC 3478 [19]
SHOULD	MAY	SHOULD	**[R42]** If OSPF is used for routing, in order to provide for continuous service when the router control plane fails, routers support OSPF graceful restart RFC 3623 [21]
SHOULD	MAY	SHOULD	**[R43]** If IS-IS is used for routing, in order to provide for continuous service when the router control plane fails, routers support IS-IS graceful restart RFC 3847 [23]

5.3.3.4 Failure Detection and Notification

MASG (PE router)	CSG (PE router)	P router	Requirement
MUST	MUST	MUST	**[R44]** Router supports detection of LSP failures by the OAM mechanisms as defined in Section 5.2.1

Note: When a PE receives an internal indication that an LSP has gone down, it may trigger protection switching mechanisms internally.

5.3.4 Pseudowire resiliency

This section describes PW resiliency and resiliency requirements.

[R45] A PE compliant with this specification SHOULD support PW protection required by this section.

There are two network scenarios where resiliency on the pseudowire level is supported:

For SS-PW applications: if the working and protect PW terminate on different PE devices, then pseudowire redundancy should be considered as per the ongoing work in the IETF at the time of publication of this document.

For MS-PW applications: these are switched at different S-PE nodes, and hence pseudowire redundancy should be considered as per the ongoing work in the IETF at the time of publication of this document.

In the following, a CE that is connected to a single PE via one AC is referred as a“Single-homed CE”, and a CE that is connected to more than one PE (each AC to a different PE) is referred as a “Multi-homed CE”.

Note: The AC that is connected to a PE might itself be protected using protection native to the AC technology (e.g. LAG for Ethernet). From the PW’s point of view this is a single AC.

5.3.4.1 VRRP Protection

Note: use of VRRP only applies to L2VPN (VPLS) solution for the IP TNL

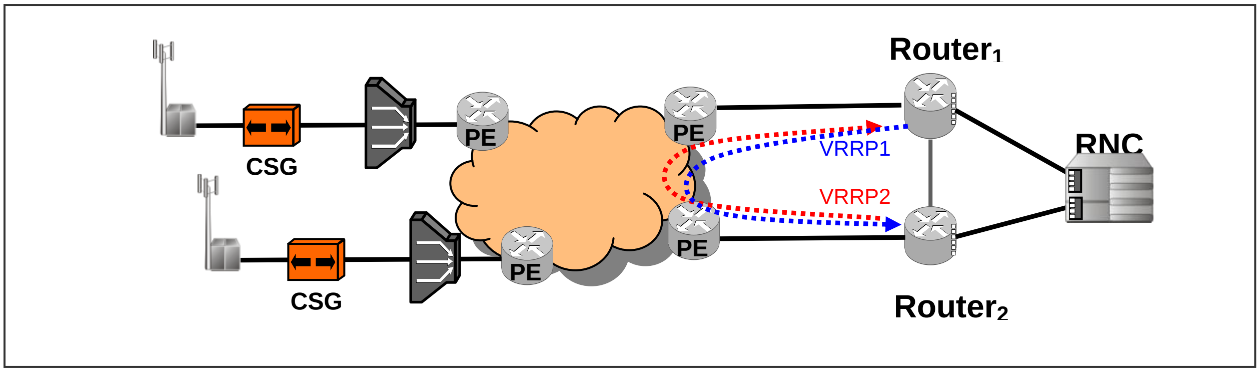


Figure 20: Mobile POP connectivity with direct connect offer and VRRP protection mechanism

The Figure 20 describes a typical Mobile POP configuration for an IP RAN, where two routers are connected to the RNC and a direct connection exists between the routers and the PE's. Virtual Router Redundancy Protocol (VRRP – RFC 5798) may be used to provide PE/Mobile POP protection.

VRRP is a router redundancy protocol that defines a "virtual router", which is actually a master and one or more backup routers, instead of a physical router. At any one time only one physical router, called the master, performs the L3 forwarding. However, if connectivity with the master is lost, the protocol enables a backup router to automatically take over.

As VRRP provides next hop protection, with two VRRP instances, one per NodeB group, over a single LAN, load sharing can be realized. For example in the Figure 20, Router1 is in master mode for the first VRRP instance and Router2 is in master mode for the second instance.

[R46] The MASG SHOULD support the VRRP protocol per RFC 5798 [56].

5.4 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 MPLS domains. 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.

[R47] The PE MUST support a configurable mechanism to ensure CoS starvation prevention.

The following capabilities are to be supported by the PEs supporting L2VPN MPLS connectivity for IP TNL using Ethernet:

[R48] The PE MUST support ingress bandwidth profile based on MEF 10.2 [91].

[R49] The PE MUST support at least 4 CoS and associated service metrics (e.g. delay, delay variation, packet loss) as defined in MEF 22.1 “EVC Requirements” [96].

[R50] The PE SHOULD support Connection Admission Control to guarantee sufficient bandwidth is available to support new connection conforming to all SLA metrics defined in MEF22.1.

Section 4.7/ RFC 4448 [34] specifies the QoS considerations.

[R51] The ingress PE MUST map the PCP (in the PRI field of the 802.1Q VLAN tag [3]) into TC field of the MPLS label stack.

[R52] 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 22.1 [96].

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.

5.4.1 Tunnel COS Mapping and marking

Two types of LSPs are defined in RFC 3270 [15]:

[R53] The PE and P routers MUST support E-LSP as per Section 1.2/RFC 3270: LSPs which can transport multiple Ordered Aggregates, so that the TC field of the MPLS Shim Header conveys to the LSR the PHB to be applied to the packet (covering both information about the packet's scheduling treatment and its drop precedence).

[R54] The PE and P routers MAY support L-LSP as per Section 1.3/RFC 3270: LSPs which only transport a single Ordered Aggregate, so that the packet's scheduling treatment is inferred by the LSR exclusively from the packet's label value while the packet's drop precedence is conveyed in the TC field of the MPLS Shim Header.

Each LSP PHB carries PWs whose services can be met by that PHB.

The internal scheduling of the PWs onto LSP PHBs is out of scope of this specification.

[R55] The PE MUST support COS marking in the TC bits of the LSP labels.

[R56] The PE MUST support COS mapping between the QoS of TNL and TC bits of the LSP labels.

[R57] The PE MUST support the Pipe model as per RFC 3270.

5.4.2 PW COS Mapping and marking

This section is based on AF-AIC-0178.001 [1] and expands on it to handle various PW types.

[R58] The PE SHOULD support mapping of TNL COS to PW label TC bits.

[R59] For multi-segment PW, the PE MUST support mapping of TNL COS to PW label TC bits.

[R60] The PE SHOULD support marking of the PW label TC bits.

[R61] For multi-segment PW, the PE MUST support marking of the PW label TC bits.

5.5 IPv6 requirements

This section discusses both the IPv6 TNL and the IPv6 MPLS MBH network.

5.5.1 IPv6 TNL support in an IPv4 MPLS MBH network

The IPv6 traffic is transported over MPLS. There are two cases either which or both may be supported.

5.5.1.1 IPv6 traffic encapsulated in Layer 2

IPv6 packets are encapsulated in Layer 2 and they are transported as layer 2 VPNs through a MPLS network. IPv6 support is not needed on LER nodes.

In L2VPN solutions, IPv6 TNL is transparently transported over any Layer 2 technologies and then over PWs (e.g. Ethernet PW). It has no impact on the MPLS MBH.

5.5.1.2 IPv6 traffic over MPLS Transport

PE nodes (such as an MASG or any access node connected to an IPv6 eNB) in an IPv4 MPLS MBH network MUST have Dual Stack IPv4/IPv6 capability and be provisioned with at least an IPv4 and IPv6 address. The PEs support IPv6 on the CE facing interfaces. They support IPv4 and MPLS on the core facing interfaces.

[R62] PE nodes MUST support 6PE technology as per RFC 4798 [41] in order to carry IPv6 packets over a MPLS IPv4 only network. 6PE implementations MUST support BGP AFI (Address Family Identifier) value 2, BGP SAFI (Subsequent Address Family Identifier) value 4 and IPv4 Network Address of Next Hop.

The LSPs are setup per section 3/RFC 4798 [41].

For an IPv6 L3VPN MPLS solution, RFC 4659 [36] extends the “BGP/MPLS IP VPN” method for support of IPv6. For this application, an IPv4 backbone with MPLS tunneling is used.

[R63] The PE MUST support transport of IPv6 VPNs over an IPv4 backbone using MPLS LSPs as per RFC 4659 [36]. If supported, the PE MUST support BGP AFI value 2, BGP SAFI value 128 and IPv4 Network Address of the Next Hop.

[R64] MPLS labeled IPv6 packet processing rules per Section 3.5 (*Processing Labeled IPv6 Datagrams which are Too Big*) in RFC 3032 [13] SHOULD be supported in PE.

Differentiated Services over MPLS for IPv6 is handled similar to IPv4, see RFC 3270 [15].

5.5.2 IPv6 TNL support in an IPv6 MPLS MBH network

This section describes the requirements for an IPv6 based IP TNL that is supported by an MPLS Mobile backhaul network where the network is IPv6 based.

5.5.2.1 General IPv6 requirements

All nodes (both PE and P routers) in an MPLS MBH network MUST have the IPv6 capability and be provisioned with at least an IPv6 address. IPv6 forwarding SHOULD be supported.

[R65] IPv6 SHOULD be supported per RFC 2460 [12].

[R66] Neighbor Discovery for IPv6 SHOULD be supported per RFC 4861 [42].

[R67] Internet Control Message Protocol (ICMP) for IPv6 SHOULD be supported per RFC 4443 [31].

[R68] Path MTU Discovery for IPv6 SHOULD be supported per RFC 1981 [8].

To support all IPv6 routing and control protocols in an MPLS MBH network:

[R69] OSPF for IPv6 SHOULD be supported per RFC 5340 [53], OSPF intra-area Traffic Engineering for IPv6 SHOULD be supported per RFC 5329 [52].

[R70] IS-IS for IPv6 SHOULD be supported per RFC 5308 [51], IS-IS intra-area Traffic Engineering for IPv6 SHOULD be supported per RFC 6119 [66].

[R71] BGP for IPv6 SHOULD be supported per RFC 2545 [11].

[R72] RSVP-TE for IPv6 SHOULD be supported per RFC 3209 [14].

[R73] LDP for IPv6 SHOULD be supported per RFC 5036 [44]. Note: additional protocol on LDP for IPv6 is under development in the IETF.

To support IPv6 OAM and protection in an MPLS MBH network:

[R74] BFD for IPv6 MPLS SHOULD be supported per RFC 5884 [60].

[R75] LSP Ping for IPv6 MPLS SHOULD be supported per RFC 4379 [29].

[R76] FRR for IPv6 MPLS SHOULD be supported per RFC 4090 [25].

[R77] VRRP Version 3 SHOULD be supported per RFC 5798 [56].

5.5.2.2 Solution specific IPv6 requirements

In addition to the general IPv6 requirements as specified in Section 5.5.2.1, more solution specific requirements are needed for different solutions:

In L2VPN MPLS solutions, MPLS transport of different kinds of TNLs is the same as specified in respective TNL sections.

[R78] IPv6 PW OAM SHOULD be supported, i.e. IPv6 for VCCV [RFC5085] [45], IPv6 for VCCV BFD, and IPv6 for VCCV LSP Ping.

[R79] In L3VPN MPLS solutions, MPLS transport of IPv6 VPN service over an IPv6 MBH network SHOULD be supported per RFC 4659 [36]. If supported, BGP AFI value 2, BGP SAFI value 128 and IPv6 Network Address of Next Hop MUST be supported per RFC 4659.

[R80] In LSP solutions, MPLS transport of IPv6 service MUST be supported. Using MP-BGP over IPv6 to set up IPv6-signaled LSPs SHOULD be supported per RFC 4760 [38] (i.e. BGP AFI value 2, BGP SAFI value 4 and IPv6 Network Address of Next Hop).

[R81] MPLS labeled IPv6 packet processing rules per Sec. 3.5 (*Processing Labeled IPv6 Datagrams which are Too Big*) in RFC 3032 [13] SHOULD be supported in PE.

Differentiated Services over MPLS for IPv6 is handled similarly as IPv4, see RFC 3270.

5.5.3 IPv4 TNL support in an IPv6 MPLS MBH network

After the transition of the MPLS MBH networks to IPv6, some IPv4 eNB sites may still need to be connected to them. This scenario is for further study.

5.6 Security requirements

[R82] The PEs MUST support the following capabilities for MPLS network security:

- SS-PW per Section 11/RFC 3916 [24].
- MS-PW per Section 7.1/RFC 5254 [48].

[R83] The PEs MUST support the following capabilities for VPN security:

- General VPN security per Section 4.5/RFC 3809 [22] and RFC 4111 [26].
- L2VPN security per Section 6/RFC 4761 [39] and Section 14/RFC 4762 [40].
- L3VPN security per Section 13/RFC 4364 [27].

More detailed security requirements are outside the scope of this document.

6 Specifications for TDM TNL Scenario

This section specifies the use of IP/MPLS in the TDM TNL scenario. For requirements common to all the TNL scenarios, appropriate references are made to the specifications in Section 5.

[R84] A PE compliant with this specification SHOULD support TDM TNL required by this section.

6.1 Signaling and Routing

6.1.1 PSN tunnel LSP Signaling and Routing

Signaling is defined in Section 5.1.1.
Routing is defined in Section 5.1.2.

6.1.2 PW Signaling

PW signaling is defined in Section 5.1.3.

6.2 Encapsulation

This section describes specifications to meet encapsulation requirements in different scenarios (e.g. SATOP and CES with or without RTP).

The following PW encapsulation should be supported for TDM:

[R85] If a PE supports TDM TNL then it SHOULD support SATOP T1 or E1 as per IETF RFC 4553 [35].

- For LDP signaling the PW types per RFC 4446 [32] MUST be used.

[R86] If a PE supports TDM TNL then it SHOULD support CESoPSN as per RFC 5086 [46].

- The PW type for LDP signaling is 0x0015. In addition control protocol extensions described in IETF RFC 5287 [49] MAY be used.

[R87] If a PE supports TDM TNL the following options are supported:

- Control word MUST be used as defined in Section 2.2.1/MFA 8.0 [97].
- TNL TDM Payload Bytes: The default payload size defined for the corresponding service MUST be according to RFC 4553 [35] or RFC 5086 [46].
- TNL then it is default configuration MUST NOT use RTP.

[R88] If RTP is supported:

- The default parameters as specified in Section 4.3.2/RFC 4553 [35] MUST be used.
- The PEs at either end of the PW MUST be configured with the following parameters: Differential Timestamping Mode; Frequency and SSRC.

The BTS and the BSC connection may use either fractional or full E1 or T1.

In the one to one connection the PE may emulate the full T1/E1 without any awareness of its structure.

[R89] PE SHOULD support SATOP emulation as per Section 2.3.2/MFA 8.0 [97].

For either one-to-one or one-to-many (e.g. several TDM PW are connected to one TDM link) cases:

[R90] PE SHOULD support CESoPSN as per Section 2.3.5MFA 8.0.

[R91] PE MAY support TDMoMPLS as per Section 4/MFA 4.1 [74].

6.3 OAM

This section describes OAM techniques used for TDM TNL specific pseudowires.

[R92] PE routers MUST support transparent transfer of TDM native service OAM over the PW as defined in Sections 5 and 9/RFC 6310 [67].

PW OAM is defined in Section 5.2.3.

6.3.1 Encoding of AC condition

[R93] A PE SHOULD map the status of the AC to the PW as defined in Section 2.2.1 Table 2-1/ MFA 8.0.

[R94] A PE MUST support transmission of RDI or AIS towards the local CE as per L and M control word bits combination in the case of one to one connections where structure aware encapsulation is used.

6.4 Resiliency

This section describes ensuring resiliency for TDM TNL specific pseudowires.
Resiliency is defined in Section 5.3.

6.5 QoS

QoS for PW and PSN QOS are defined in Section 5.4.

7 Specifications for ATM TNL Scenario

This section specifies the use of IP/MPLS in the ATM TNL scenario. For requirements common to all the TNL scenarios, appropriate references are made to the specifications in Section 5. The ATM TNL is optional.

7.1 Signaling and Routing

7.1.1 PSN tunnel LSP Signaling and Routing

Signaling is defined in Section 5.1.1.
Routing is defined in Section 5.1.2.

7.1.2 PW Signaling

PW signaling is defined in Section 5.1.3.

[R95] The PW types for ATM n-to-one cell mode MUST be supported as per RFC 4446 [34].

7.2 Encapsulation

7.2.1 Cell Mode Encapsulation

A PE node that implements the ATM TNL supports the following:

[R96] Cell mode MUST be supported according to ATM n-to-one cell mode as described in RFC 4717 [37].

7.2.1.1 Support for multiple connections in a single PW:

[R97] The n-to-one encapsulation method that maps one or more VCCs or VPCs to one PW MUST be supported.

[R98] The MASG and CSG MUST support VCC and VPC cell transport.

<u>Support for cell concatenation:</u>

[R99] The CSG and MASG MUST support concatenation of multiple cells into a single PW packet.

[R100] Each ingress PW endpoint SHOULD concatenate cells based on the MTU limitation of the egress PW endpoint, the MTU limitations of the network, cell transfer delay (CTD) and cell delay variation (CDV) objectives of the multiple ATM connections that are multiplexed into a single PW, and the capabilities of the egress endpoint.

[R101] When using LDP, the maximum cells limit supported by each endpoint MUST be advertised between the LDP peers and the ingress endpoint MUST NOT exceed the advertised limit.

[R102] A timeout mechanism MUST be supported to allow the generation of a PW packet before the maximum configured number of cells has been received.

[R103] For VCC mode MUST support both one cell (N=1) and N cells (N>1) per VCC.

[R104] For VPC mode MUST support one cell (N=1) and MAY support N cells (N>1).

VPI/VCI translation:

As an alternative to keeping the VPI/VCIs unique across all PWs, the PW may be used as a Logical Interface Identifier. The MASG would then map the PW, VPI, and VCI to the egress port, VPI and VCI. This is consistent with Section 8.1/RFC 4717 [37] and Y.1411 [88]. Note that the value of VPI/VCI at the local ATM end point might not be the same as the VPI/VCI value of the far end ATM end point. Supporting VPI/VCI egress translation simplifies Base Station ATM connection provisioning by allowing usage of the same VPI/VCI at all node-Bs.

[R105] The MASG MUST be capable of performing a translation on the PW/VPI/VCI carried in the ATM cell in the PW packet to egress port/VPI/VCI.

[R106] The translation of VPI/VCI MAY be performed at the ingress PW endpoint, the egress PW endpoint or both.

Use of control word:

[R107] The control word SHOULD be used to allow for sequence number support.

[R108] If the control word is supported, the format MUST be as described in Section 8.1/RFC 4717 [37].

[R109] Sequence number SHOULD be supported per RFC 4385 [30] to allow the recognition of reordering or discard problems in the network.

[R110] Each PW endpoint MUST be configurable to support or not support the sequence number in the PW control word.

[R111] When the sequence number is not supported, a value of zero MUST be transmitted in the sequence number bits of the control word.

[R112] When the sequence number is supported, a value of zero MUST be ignored by the receiving endpoint.

7.3 OAM

This section describes OAM techniques used for ATM TNL specific pseudowires.

[R113] PE routers MUST support transparent transfer of ATM native service OAM over the PW as defined in Sections 5 and 7/RFC 6310 [67].

PW OAM is defined in Section 5.2.3.

7.3.1 Cell mode encapsulation

7.3.1.1 VCC Case

As described in Section 7.1/RFC 4717 [37], VCC Case, when configured for ATM VCC service, both PEs act as VC switches, in accordance with the OAM procedures defined in I.610 [87].

[R114] The PEs MUST be able to pass the following OAM cells transparently:

- F5 Alarm Indication Signal (AIS) (segment and end-to-end)
- F5 Remote Defect Indicator (RDI) (segment and end-to-end)
- F5 Loopback (segment and end-to-end)
- F5 Continuity Check (segment and end-to-end)
- Other F5 OAM cells received

[R115] However, if configured to be an administrative segment boundary, the PE MUST terminate and process F5 segment OAM cells.

F4 OAM cells are inserted or extracted at the VP link termination. These OAM cells are not seen at the VC link termination and are therefore not sent across the PSN.

Defects should be handled as follows by PE routers:

AC failure:

[R116] AC receives defect state entry and exit criteria MUST be per RFC 6310 [67], Section 9.1 for single emulated OAM loop mode at F5 level.
AC transmit defect state entry/exit criteria is not applicable.

[R117] AC receives defect consequence action as per RFC 6310 Section 9.3.4 “single emulated OAM loop” MUST support the default option.
AC transmit defect consequence action is not applicable.

PW failure:

[R118] The PE MUST be able to generate F5 AIS on the basis of PW failure per Section 9.3.1/RFC 6310 [67].

[R119] PW receive defect state entry/exit MUST be per Section 9.3.1/RFC 6310 at F5 level.

[R120] PW transmit defect state entry/exit MUST be per Section 9.3.2/RFC 6310 at F5 level.

7.3.1.2 VPC Case

When configured for a VPC cell relay service, both PEs should act as VP cross-connects in accordance with the OAM procedures defined in ITU-T I.610 [87].

[R121] The PEs MUST be able to process and pass the following OAM cells transparently according to I.610:

- F4 AIS (segment and end-to-end)
- F4 RDI (segment and end-to-end)
- F4 Loopback (segment and end-to-end)
- F4 Continuity Check (segment and end-to-end)

[R122] However, if configured to be an administrative segment boundary, the PE MUST terminate and process F4 segment OAM cells.

[R123] The PEs MUST be able to pass the following OAM cells transparently:

- F5 AIS (segment and end-to-end)
- F5 RDI (segment and end-to-end)
- F5 Loopback (segment and end-to-end)
- F5 Continuity Check
- Other F5 OAM cells received

OAM cells may be encapsulated together with other user data cells if multiple cell encapsulations are used.

Defects should be handled as follows:

AC failure:

[R124] AC receives defect state entry and exit criteria MUST be per Section 9.1/RFC 6310 [67]1 for single emulated OAM loop mode at F4 level.
AC transmits defect state entry/exit criteria is not applicable.

[R125] AC receives defect consequence action as per Section 9.3.4/RFC 6310 “single emulated OAM loop” MUST support default option.
AC transmits defect Consequence action is not applicable.

PW failure:

[R126] The PE MUST be able to generate F4 AIS on the basis of PW failure per Section 9.3.1/RFC 6310 [67].

[R127] PW receives defect state entry/exit MUST be per Section 9.3.1/RFC 6310 at F4 level.

[R128] PW transmits defect state entry/exit MUST be per Section 9.3.2/RFC 6310 at F4 level.

7.4 Resiliency

See Section 5.3.

7.5 QoS

See Section 5.4.

7.5.1 Traffic shaping

For ATM TNL, connections are characterized by PCR/CDVT parameters for CBR and by PCR/SCR/MBS/CDVT parameters for VBR connection.

[R129] The PE MUST shape ATM VPC or VCC connections at egress UNI port to maintain the CDVT/PCR and to enforce ATM traffic to be compliant to negotiated SLA.

Note: Due to the presence of a per ATM VPC or VCC shaper on the egress UNI interface of the ATM TNL, increases in CDV within the ATM TNL will lead to increases in CTD across the ATM TNL. Within the capabilities of the egress ATM shaper, increases in CDV will not impact the ability to meet the parameter CDVT at the egress UNI. Bounding of the CDV caused by concatenation of ATM cells from a single ATM VPC or VCC through limiting of the interval of time over which cells are concatenated together will reduce the delay experienced within the egress ATM shaper.

7.5.2 QOS marking

The PE supports marking per Section 5.4.

[R130] In the N to 1 case cell concatenation mode, when N is greater than 1, cells may be concatenated from multiple VCCs or VPCs with different service categories and QoS requirements. In this case, the PSN packet MUST receive appropriate treatment by the PSN to support the highest QoS of the ATM VCCs/VPCs carried.

[R131] In case of 1:1 mapping in VCC or VPC mode, the PE MUST support mapping between ATM COS and PW COS.

[R132] In the N to 1 case cell concatenation mode, when N is greater than 1, cells may be concatenated from multiple VCCs or VPCs with different service categories and QoS requirements. In this case, the PE MUST map the COS of the highest provisioned ATM ATC COS to the PW COS.

8 Specification for IP TNL Scenario

8.1 IP connectivity

From 3GPP R5, IP can be used as TNL. IP can be carried over different types of L2 protocols: Ethernet, ML-PPP, ATM, etc. Currently RAN equipment vendors are implementing Ethernet ports on RAN and mobile Core equipment (e.g. Fast Ethernet or 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 LTE, IP is the unique Transport Network Layer specified to transport mobile flows between eNBs 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. S1 and X2, are given in Appendix D.

Different MPLS based solutions can be used to transport IP TNL in the mobile backhaul network: L2VPN MPLS (e.g. VPWS, VPLS, H-VPLS), L3VPN MPLS and RSVP-TE MPLS LSP that are described hereafter.

8.2 IP and Ethernet QoS

Different kinds of services are expected to be supported over Mobile Backhaul networks, e.g. VoIP, video streaming, instant messaging, mailing and internet. The QoS measures provided must be able to meet the requirements of these different services.

Requirements from Section 5.4 apply.

If the service offered to the mobile equipment is Ethernet, the mobile backhaul network must ensure transparency for transported traffic COS, i.e. no modification of the user provided IEEE 802.1p bits.

[R133] The PE nodes MUST support forwarding of Ethernet packets without modifying the 802.1p received from the mobile equipment.

[R134] The PE nodes MUST support forwarding of IP packets without modifying the DSCP received from the mobile equipment.

Note: if the service offered to the mobile equipment is IP, the mobile backhaul network must ensure transparency for transported traffic COS, i.e. no modification of the user provided DSCP bits.

8.2.1 COS marking

COS Marking are supported as per section 5.4.

8.2.2 Number of COS

Refer to the Section 5.4.

8.3 L2VPN MPLS Solutions

8.3.1 VPWS Solution

This section specifies the use of Ethernet PWs for VPWS service to transport IP TNL carried over Ethernet. The Layer 2 connectivity service is provided using Metro Ethernet Forum E-Line service as defined in MEF 6.1 [90] and MEF 10.2 [91]. Additional service constraints for MBH are defined in MEF 22.1 [96].

8.3.1.1 Signaling and routing

This section specifies the signaling protocol used to establish the underlying MPLS tunnel that carry pseudo-wires. It also specifies the signaling protocol used to setup and control pseudowires of VPWS carrying Ethernet frames encapsulating IP TNL.

In an IP/MPLS network a pseudowire is carried over a MPLS LSP acting as PSN tunnel. Traffic Engineered PSN tunnels must be used when specific path (e.g. for protection purpose), QoS or bandwidth constraints are required.

8.3.1.1.1 LSP signaling

LSP signaling is supported as per Section 5.1.1.

8.3.1.1.2 PW Signaling

PW signaling is supported as per Section 5.1.3.

8.3.1.1.3 Routing

LSP routing is supported per Section 5.1.2.

8.3.1.2 Encapsulation

According to RFC 4448 [34], an Ethernet PW operates in one of two modes: "raw mode" or "tagged mode". For more information on the PW modes of operation see RFC 4448 Sections 4.1 and 4.2.

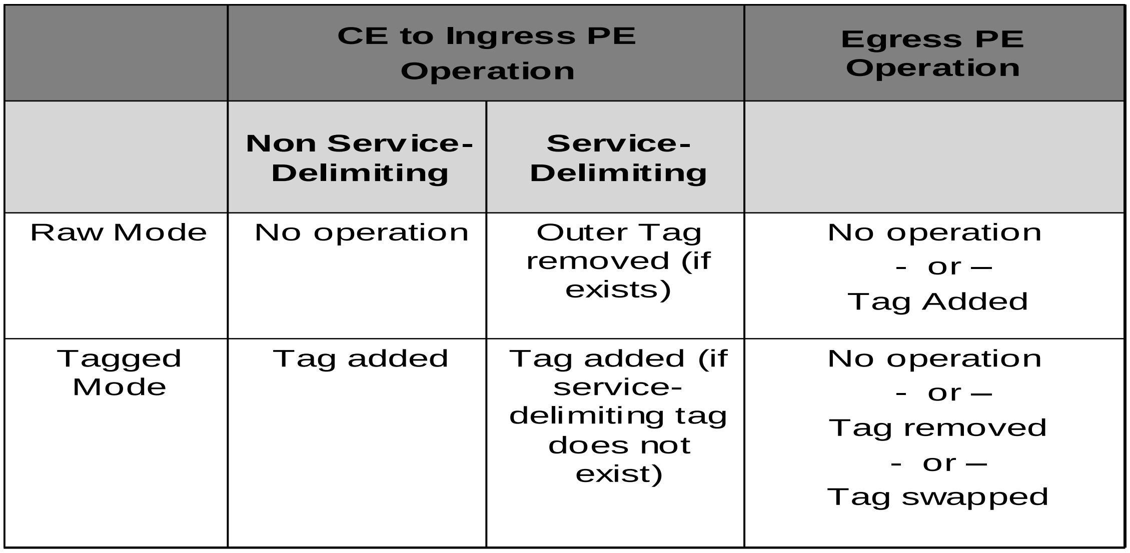
RFC 4448 also defines two modes of operations of using the 802.1Q VLAN tags. When the tags are defined as "service-delimiting" the tags are used by the PE to distinguish the traffic. When the tags are defined as "not service-delimiting" the tags are not meaningful to the PE.

There is an errata that was added to RFC 4448 that tries to clarify the usage of “service delimiting” tags vs. “non service delimiting tags”. This section assumes the intent that is provided by the errata.

8.3.1.2.1 RFC 4448 Mapping Operation

Table 4 below summarizes the operations that can be performed on ingress and egress Ethernet frames associated with the AC for the PW ingress and egress as specified in RFC 4448 [34]. Note that the ingress and the egress frames refer to frames going into the network (ingress) or coming out of the network (egress) at the PE ACs. The PE ACs are configured as either Raw or Tag Modes. The Ethernet frames are designated as either Service-Delimiting or Non Service-Delimiting frames.

Note that the VLAN tag rewrite can be achieved by NSP at the egress PE. A PW only supports homogeneous Ethernet frame type across the PW; both ends of the PW must be either tagged or untagged.



	CE to Ingress PE Operation		Egress PE Operation
	Non Service-Delimiting	Service-Delimiting	
Raw Mode	No operation	Outer Tag removed (if exists)	No operation - or – Tag Added
Tagged Mode	Tag added	Tag added (if service-delimiting tag does not exist)	No operation - or – Tag removed - or – Tag swapped

Table 4 – Raw and Tag Mode Operations for Service Delimiting and Non Service Delimiting Frames

8.3.1.2.2 Mapping between Ethernet and PWs

This specification follows the direction noted in the Errata to RFC 4448 [34] ignoring the distinction between Customers tagged or Service Providers tagged Ethernet frames sent by mobile equipment to the mobile backhaul network, as initially the mapping defined in IETF RFC 4448 imposes some restrictions on the use of "service delimiting tags".

The following requirements specify the configurations, encapsulations and processing required for mapping between Ethernet frames to PWs at the respective ACs of VPWS and VPLS services.

[R135] The PE MUST support the Ethernet encapsulation over PW as specified in RFC 4448.

[R136] The Native Service Processing (NSP) function in a PE MUST support Service Delimiting and Non Service Delimiting functions specified in RFC 4448.

[R137] The NSP function in a PE MUST support Tag Mode specified in RFC 4448 including the operations specified in Table 4.

[R138] The NSP function in a PE MAY support Raw Mode specified in RFC 4448 including the operations specified in Table 4.

The Native Service Processing (NSP) for different use cases are provided in Appendix E.

8.3.1.2.3 Control Word and Frame ordering

Section 4.6 of RFC 4448 [34] specifies the use of the control word for PWs.

[R139] The PE SHOULD support control word.

[R140] The PE SHOULD support Frame Ordering as per Section 4.6 of RFC 4448.

8.3.1.3 OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels and pseudowires used to transport IP TNL over VPWS.

PW OAM requirements as defined in section 5.2.3 apply.

8.3.1.3.1 AC OAM

The PE must transparently transfer received native Ethernet service OAM indications over the PW according to interworking specifications under development in the IETF.

The following defect handling should be supported:

AC failure:

- AC receive defect state entry and exit criteria.
- AC transmit defect state Entry/exit criteria.
- AC receive defect Consequence action.
- AC transmit defect Consequence action.

PW failure:

- PW receive defect entry/exit procedure.
- PW transmit defect entry/exit procedure.

8.3.1.4 Resiliency

The requirements in Section 5.3 apply.

8.3.1.5 QoS and Service Level agreements

The packet based backhaul network has to provide QoS and service level agreements. The QoS capabilities must be end to end, which includes both the Ethernet domain and the MPLS domain.

See Section 5.4.

8.3.1.5.1 QoS mapping

See Section 5.4.

8.3.1.5.2 QoS flexibility

The TC value of one Ethernet PW can be adapted according to the IEEE 802.1p value of the Ethernet frame that is encapsulated into the PW frame. That means that one Ethernet PW is not fixed to only one TC value. This 1:1 mapping allows the automatic transport of the QoS marking from the payload to the TC field (PW/LSP layer) while using a single PW (E-LSP).

8.3.2 VPLS solution

This section specifies the use of VPLS to transport IP TNL carried over Ethernet. Virtual Private LAN Service (VPLS), also known as Transparent LAN Service type, offers a Layer 2 Virtual Private Network (L2VPN) providing multipoint Ethernet LAN connectivity.

8.3.2.1 Signaling and routing

IETF specifies two specifications for VPLS: RFC 4761 [39] "*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signalling*" and RFC 4762 [40] "*Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*".

8.3.2.1.1 Signaling

VPLS can be provisioned and auto discovered with BGP RFC 4761 [39] or provisioned with LDP RFC 4762 [40].

[R141] The PE SHOULD support BGP signaling and Auto-Discovery for VPLS [RFC 4761].

[R142] The PE SHOULD support LDP signaling for VPLS [RFC 4762].

[R143] The PE implementing LDP signaling for VPLS [RFC 4762] MAY also support BGP Provisioning, Autodiscovery and Signaling in Layer 2 VPN networks [RFC 6074] [65].

[R144] The MASG SHOULD support H-VPLS per RFC 4762 as PE-rs in section 10.

In an IP/MPLS network a pseudowire is carried over a MPLS LSP acting as PSN tunnel. Traffic Engineered PSN tunnels must be used when specific path (e.g. for protection purpose), QoS, or bandwidth constraints are required.

PSN tunnel establishment is supported as per Section 5.1.1.

8.3.2.1.2 Routing

PSN tunnel routing is supported as per Section 5.1.2.

8.3.2.2 Encapsulation

For VPLS solutions, the encapsulation used is specified in the RFC 4762 [40] (for LDP based solution) and RFC 4761 [39] (for BGP based solution).

RFC 4762 in Sections 7 and 8 specifies the encapsulation.

```
"While the encapsulation is similar to that described in [RFC 4448], the
functions of stripping the service-delimiting tag and using a "normalized"
Ethernet frame are described [in sections 7 and 8]".
```

Section 7/RFC 4762 specifies for Ethernet PW and Section 8//RFC 4762 specifies for Ethernet VLAN PW.

RFC 4761 [39] in Section 4.1 specifies the encapsulation.
Note: Both VPWS and VPLS use the same encapsulation format. The local functions like NSP, Service-delimiting and Frame forwarding are different. Some of the differences are:

- There are no Tag and Raw modes in RFC 4762 [40]. Section 7 describes Data Forwarding on an Ethernet PW. Section 8 describes Data Forwarding on an Ethernet VLAN PW.
- In Section 7/RFC 4762, it allows mix-and-match of VLAN tagged and untagged services at either end. This is not allowed in VPWS.
- VPLS may have both Ethernet and Ethernet VLAN.

8.3.2.2.1 Control Word and Frame ordering

See VPWS section 8.3.1.2.3 on Control Word and Frame Ordering.

8.3.2.3 OAM

8.3.2.3.1 AC Native Service OAM

See Section 8.3.1.3.1 for requirements.

8.3.2.3.2 Label Switched Paths (LSPs)

LSP OAM is supported as per section 5.2.1.

8.3.2.3.3 Pseudowires (PWs)

PW OAM is supported as per section 5.2.3.

8.3.2.3.4 Packet Loss and Delay Measurement

LSP packet loss and delay measurement is supported as per section 5.2.4.

8.3.2.4 Resiliency

Resilience is supported as per section 8.3.1.4.

8.3.2.5 QoS and Service Level Agreement

QoS is supported as per section 8.3.1.5.

8.3.2.6 Multicast

In order to support transport of multicast dependent applications like financial services, IPTV and video services a scalable and reliable VPLS multicast infrastructure is required.

RFC 4761 [39] and RFC 4762 [40] provide VPLS multicast that relies on ingress replication. This solution has certain limitations for certain VPLS multicast traffic profiles. For example it may result in highly non-optimal bandwidth utilization in the MPLS network when a large amount of multicast traffic is to be transported. The support of a multicast tree addresses this issue.

Multicast in VPLS should be supported for Multicast trees in VPLS as under development in the IETF.
Extensions for VPLS LDP to support multicast and broadcast should be supported as under development in the IETF.

These procedures for VPLS multicast that use multicast trees in the Service Provider (SP) network are applicable for both RFC 4761 and RFC 4762.

8.3.2.7 Security

Security is supported as per Section 5.6.

8.4 L3VPN MPLS solutions

8.4.1 Signaling and routing

This section specifies the signaling protocol used to setup the underlying MPLS tunnel carrying IP TNL.

[R145] The PE MUST support RFC 4364 [27].

This provides a method by which mobile equipment may use IP Virtual Private Networks (VPNs) for connecting any to any interfaces.

L3VPN traffic is carried on a PSN tunnel. Traffic Engineered PSN tunnels must be used when specific path, QoS, or bandwidth constraints are required.

PSN Tunnel LSP is supported per section 5.1.1.
Routing support is per section 5.1.2.

8.4.2 Encapsulation

Data is carried via IP packets encapsulated with VPN route label and tunneled in the LSPs per RFC 4364[27].

8.4.3 OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels used to transport IP TNL over L3VPN MPLS.

8.4.3.1 Label Switched Paths (LSPs)

LSP OAM is supported as per section 5.2.1 (LSP OAM section).

8.4.3.2 Packet Loss and Delay Measurement

LSP Packet Loss and Delay Measurement is supported as per Section 5.2.4 (LSP loss and delay measurement section).

8.4.4 Resiliency

This section describes solutions to ensure resiliency of the underlying MPLS tunnels which carry the backhaul traffic.

LSP resiliency specified in Section 5.3 will apply.

8.4.5 QoS

The packet based backhaul network has to provide QoS and service level agreements. The QoS capabilities must be end to end, which includes both Ethernet domain and MPLS domain.

Traffic engineering could even be used to establish label switched paths with particular QoS characteristics between particular pairs of sites. RFC 4365 [28] (Applicability Statement for BGP/MPLS IP Virtual Private Networks) section 14 provides QoS and SLA requirements. BGP/MPLS IP VPNs can support both the “hose model” and the “pipe model” methods of how service providers offer QoS in their networks. Providing the pipe model would require the use of traffic engineering to explicitly create the necessary tunnels.

QoS mappings are supported for the tunnel LSPs as per Section 5.4.

8.4.6 Multicast

In order to support transport of IP multicast dependent applications as IPTV relying on e-MBMS architecture (defined from 3GPP R10), a scalable and reliable multicast VPN (MVPN) infrastructure is required. RFC 4364 [27] provides protocols and procedures for building BGP-MPLS for forwarding VPN unicast traffic only.

[R146] An implementation MAY support the multicast procedures specified in this section:

Multicast VPNs are based on the following IETF specifications:

[R147] The MPLS PE and P MUST support Multicast in MPLS/BGP IP VPNs (draft-ietf-l3vpn-2547bis-mcast-10.txt [69]).

[R148] The MPLS PE and P MUST support BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs (draft-ietf-l3vpn-2547bis-mcast-bgp-08.txt [70]).

[R149] The MPLS PE and P MUST support Mandatory Features in a Layer 3 Multicast BGP/MPLS VPN Solution draft-ietf-l3vpn-mvpn-considerations-06 [71]).

[R150] The MPLS PE and P MUST support RFC 4875 [43] Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths (LSPs).

[R151] The MPLS PE and P MUST support LDP Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths (draft-ietf-mpls-ldp-p2mp-15) [72].

8.4.7 Security

See the following for control plane security:

[R152] The MPLS PE and P MUST implement section 13.2/ RFC 4364 [27].

[R153] The MPLS PE and P MUST implement section 6.2/RFC 4365 [28] for SP Security Measures.

8.5 IP Over LSPs

This section specifies the requirements used to support routing IP traffic over MPLS LSPs for the IP TNL.

[R154] The PE SHOULD support routing IP over MPLS LSPs.

8.5.1 Signaling and routing

This section specifies the signaling protocol used to setup the underlying MPLS PSN tunnels carrying IP TNL. PSN tunnels may be traffic Engineered or topology driven, Traffic Engineered PSN tunnels are used to take into account specific path, QoS, or bandwidth constraints, while topology driven tunnels follow the IGP protocol determined path.

For Traffic Engineering, RSVP-TE and GMPLS are used. The RSVP-TE and GMPLS signaling requirements defined in section 5.1.1.

For topology driven tunnels, LDP is used. LDP signaling requirements are defined in section 5.1.1.

Routing support is per section 5.1.2.

8.5.2 Encapsulation

Data is carried via IP packets encapsulated within the LSPs per RFC 3032 [13].

8.5.3 OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels used to transport IP TNL.

OAM is supported per section 5.2.1.

8.5.4 Resiliency

This section describes solutions to ensure resiliency of the underlying MPLS tunnels which carry the backhaul traffic.

Resiliency is supported per Section 5.3.

8.5.5 QoS

Qos mappings are supported for the tunnel LSPs as per Section 5.4.1.

8.5.6 Security

Security is supported as per Section 5.6.

9 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 [75], 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 last-mile 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 [78].

(4) The fundamentals and specifics of the physical-layer or packet-based frequency distribution are outside the scope of this document.

9.1 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.

9.2 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. 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, 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).

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.

9.2.1 Frequency distribution requirement

[R155] 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.

[R156] 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.

9.2.1.1 TDM PW Frequency Distribution Methods

These methods are used to support a TDM PWE (TDM-TNL) service 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 [82], Clause 8.3. DCR is addressed in ITU-T G.8261 [82] Clause 8.2. The frame format as described in section 6.2 in this specification.

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.

9.2.1.2 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 [82]. Being a higher-layer frequency distribution protocol, PTP is sensitive to the network introduced PDV. PTP is defined in IEEE 1588-2008 [5]. The architecture and requirements for packet-based frequency distribution in telecom networks is described in ITU-T G.8265 [84].

A telecom profile has been specified by the ITU in Recommendations G.8265.1 [85] 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.

[R157] The synchronization distribution network architecture MUST be per G.8265 [84].

[R158] 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 [85].

9.2.1.3 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 [82]. Being a higher-layer frequency distribution protocol, NTP is sensitive to the network introduced PDV. NTP is defined in RFC 1305 (v3) [7] and RFC 5905 (v4) [62].

[R159] The synchronization distribution network architecture MUST be per G.8265 [84].

[R160] 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) [62].

9.3 Encapsulation

The timing protocol mapping might depend on the specific protocol. (e.g. in case of PTP this is specified in G.8265.1 [85] i.e. IEEE 1588 Annex D).

[R161] A PE SHOULD support transport of timing packets as specified in section 8 of this document.

The encapsulation for the TDM PW is described in section 6.2 (TDM TNL Encapsulation).

Note: Non-MPLS encapsulations are out of scope of this document.

Appendix A provides some examples of encapsulations for timing packets in the Mobile Backhaul Environment.

Appendix A: Timing Packets Encapsulations [INFORMATIVE]

A.1 Timing packets over IP TNL

There are three protocols and related packet formats of timing packets that can be used:

- Clock PW (TDM PW), (See section 6 for details)
- NTP as described in RFC 5905 [62], or
- PTPV2 as described in G.8265.1 [85]

These packet formats are intended as guidance for the implementer. If there is a discrepancy between the packet formats in this document and G.8265.1 or its references, G.8265.1 and its references take precedence.

A.1.1 IP Encapsulations

These IP encapsulations are further encapsulated depending on the type of MPLS based transport network used for mobile backhaul.

PTPV2 over IP

IP header
UDP header
1588 data

PTPV2 TP over UPD/IP
The PTPv2 mapping is as per G.8265.1 (i.e. IEEE 1588 Annex D).

NTP over IP

IP header
UDP header
NTP data

NTP TP over UPD/IP
As per RFC 5905

A.1.2 Timing Packets over L2VPN

PSN Tunnel Label
PWE3 header [RFC 4448]

MAC
IP header
UDP header
TP (Timing packet)

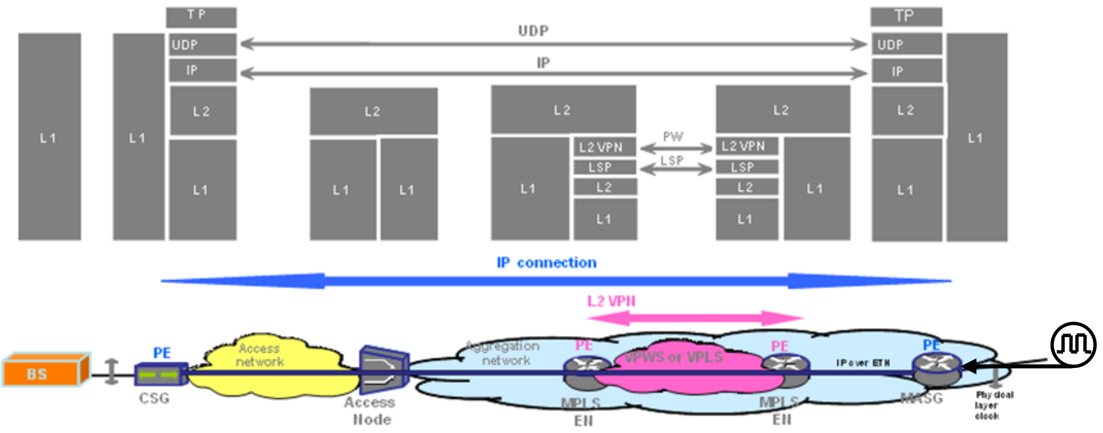


Figure 21: Timing Packets – TP: NTP or PTPV2

The figure above represents deployment case (c) in figure 10.
For other cases such as (a) or (b) the timing packets are terminated in the aggregation network and the clock signal may be sent to the base station at the physical layer.

A.1.3 Timing packets over L3VPN

PSN tunnel label
L3VPN label
IP header
UDP header
TP (Timing packet)

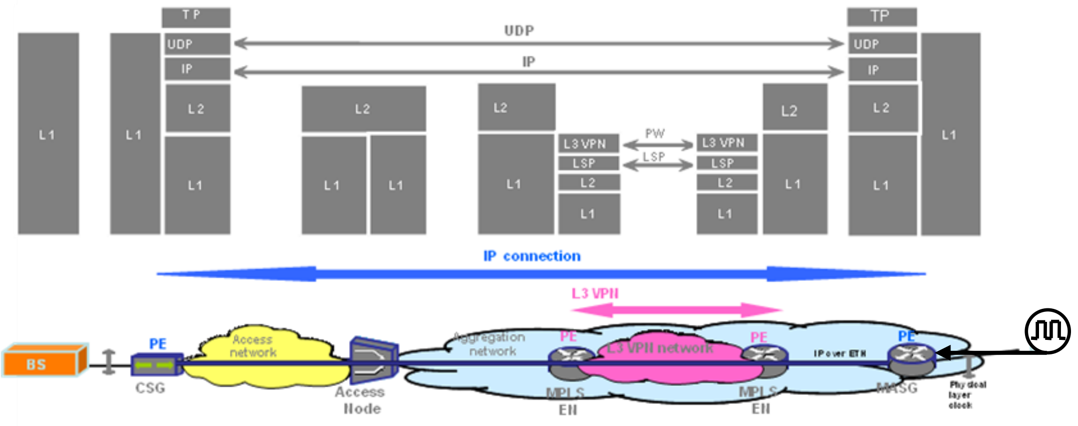


Figure 22: Timing Packets – TP: NTP or PTPV2

APPENDIX B: Frequency Distribution Scenarios

[INFORMATIVE]

With frequency distribution, the elements that participate in the frequency distribution and recovery are the RAN equipment (e.g. RNC, Node-Bs, or BSC), the MASGs, and the CSGs.

The following deployment cases are considered:

- "Deployment case (ax): Frequency is distributed over physical-layer only. Both the RC and the BS may use a common or separate reference PRC clocks.
- Deployment case (b): The packet-based frequency distribution starts at the aggregation network (MASG). Packet-based frequency distribution includes both the aggregation and access network segments. The packet based frequency distribution could be terminated directly in the base station or the short-distance link between the CSG and the BS is based on physical-layer distribution.
- Deployment case (c): The packet-based frequency distribution starts at the aggregation network (MASG). Packet-based frequency distribution includes only the aggregation segment while over the access network segment physical-layer methods are used. The packet based frequency distribution could be terminated directly in the base station or the short-distance link between the CSG and the BS is based on physical-layer distribution.
- Deployment case (d): The packet-based frequency distribution starts at the edge node of the aggregation network that is fed with a physical-layer based frequency reference. The packet based frequency distribution could be terminated directly in the base station or the short-distance link between the CSG and the BS is based on physical-layer distribution.
- Deployment case (e): The packet-based frequency distribution starts at the edge node of the aggregation network but is terminated at the access node. Over the access network segment physical-layer methods are used. The packet based frequency distribution could be terminated directly in the base station or the short-distance link between the CSG and the BS is based on physical-layer distribution.

Note: Frequency distribution using packet-based methods can be markedly improved using network on-path support mechanisms. Such mechanisms that might include intermediate terminations of the synchronization flow (e.g. PTP BCs) or the use of various manipulations to compensate for the PDV introduced by the network-element (e.g. PTP TCs) are outside the scope of this document.

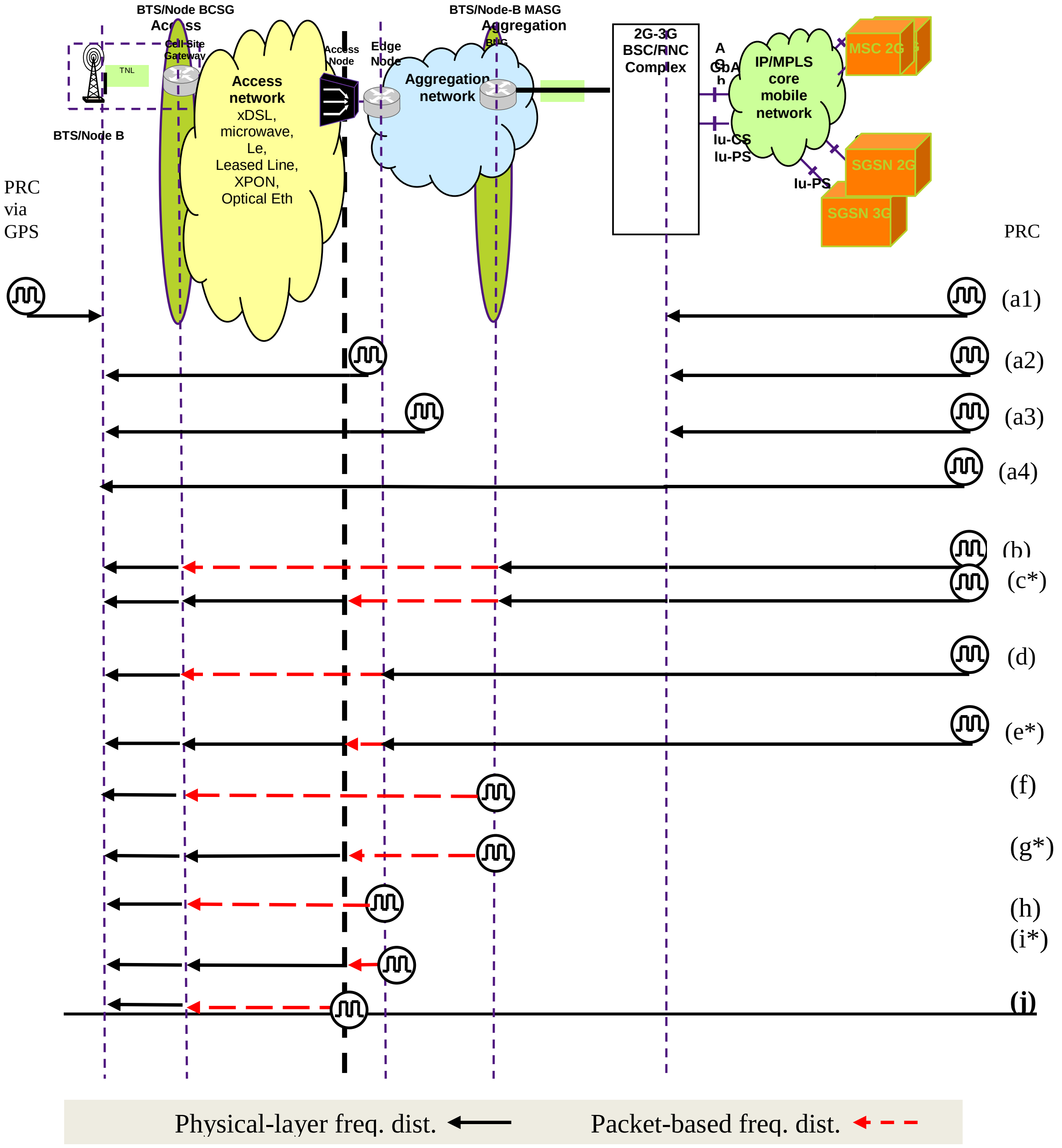


Figure 23: Frequency distribution deployment scenarios

*=Note: These cases where the recovery is not directly connected to the base station are for further study in the ITU-T. The performance of the timing delivered to the base station needs further investigation.

Note: In cases b, d, f ,h and j the packet timing can be terminated in the base station directly.

Frequency distribution using packet based methods from device within the MPLS network

There are some cases where the frequency distribution device is located somewhere in the network to distribute the frequency information over the MPLS transport infrastructure

The frequency information is always distributed towards the cellular base-stations (downstream). The following deployment cases are considered:

- Deployment case (f): The frequency information is distributed, using packet-based techniques, from the frequency distribution function, located within the aggregation network or in the MASG, towards the CSG. The short-distance link between the CSG and the BS is either based on physical-layer or packet based frequency distribution. In the former, the frequency recovery function is performed in the CSG, whereas in the latter it is performed in the base-station itself. As in the end-to-end packet based distribution case.
- Deployment case (g): The frequency information is distributed using packet-based techniques, from the frequency distribution function, located within the aggregation network or in the MASG , across the aggregation network, but is being terminated in the access node. Physical-layer frequency distribution is used to distribute the frequency across the access segment towards the CSG. The short-distance link between the CSG and the BS is based on physical-layer . As in cases a to e.
- Deployment case (h): The frequency information is distributed using packet-based techniques, from the frequency distribution function, located within the aggregation network or in the EN, across the AN towards the CSG, The short-distance link between the CSG and the BS is based on physical-layer . As in cases a to e.
- Deployment case (i): The frequency information is distributed using packet-based techniques, from the frequency distribution function, located within the aggregation network or in the EN, across the aggregation network, but is being terminated in the access node. Physical-layer frequency distribution is used to distribute the frequency across the access segment towards the CSG. The short-distance link between the CSG and the BS is based on physical-layer . As in cases a to e.
- Deployment case (j): The frequency information is distributed using packet-based techniques, from the frequency distribution function, located within the aggregation network or in the Access Node, towards the CSG. The short-distance link between the CSG and the BS is based on physical-layer . As in cases a to e.

Frequency synchronization distributed at physical layer

Transport of frequency information over the physical-layer provides a robust method of frequency distribution that will meet the frequency based requirements. Furthermore, such a technique is not subject to any packet-based stress, which will affect a packet-based frequency distribution method.

The physical-layer frequency distribution for the transport network and physical-layer frequency distribution for the end-application (e.g. cellular base-station) are differentiated. All together four different major technologies of physical-layer frequency distributions can be identified:

1. TDM frequency distribution is a physical-layer distribution method that is aimed at supporting the TDM network, being a synchronous data transport scheme. TDM frequency distribution can take the form of PDH (T1/E1) timing distribution conforming to G.823 [79]/G.824 [80]Sync, or Traffic Interfaces masks, or SDH/SONET STM-N/STS-N interfaces conforming to G.825.

   Note: TDM frequency distribution, although originally aimed at providing frequency reference to the transport network, can be sometimes also used to deliver accurate frequency reference to the end-application.

2. Synchronous Ethernet (defined in ITU-T G.8261 [82], Clauses 7.1.1 and ITU-T G.8262 [83]) is physical-layer frequency distribution method that is used to deliver synchronization to cellular base-stations over native Ethernet networks. With Synchronous Ethernet the frequency information is being propagated, node-by-node, using the internal clocks of the Ethernet switches called EECs. The entire frequency distribution chain is timed by a PRC clock (very similar concept to TDM). Options a1 to a4 in Figure 23: Frequency distribution deployment scenarios present such approach.

3. Using various synchronous last-mile technologies such as the Network Timing Reference (NTR) in DSL and the synchronous downstream 8kHz clock distribution of xPON systems.

4. Using GPS.

APPENDIX C: Use cases of the different LTE mobile nodes location in the transport network

[INFORMATIVE]

Location flexibility of the LTE mobile nodes in the transport network

The purpose of this section is to give visibility on the different locations of the mobile nodes over the transport network. Different sites in the transport network can be chosen by the operator to locate the MME, S-GW and P-GW while eNB will be located into NB site. The different sites to locate the MME and S-GW/P-GW are described in this section.

Regional PoP site is the site where IP routers called BEN (Backbone Edge Node) are positioned to aggregate the user traffic at regional level and delimit the border between Aggregation and transport Core networks. National PoP site is the site where IP routers called BEN (Backbone Edge Node) are positioned to aggregate the user traffic at national level.

SGSN site is the site where the SGSN is located and the GGSN site is the site where the GGSN is located.

The different use cases of location of LTE mobile nodes in the transport network are described in this Appendix.

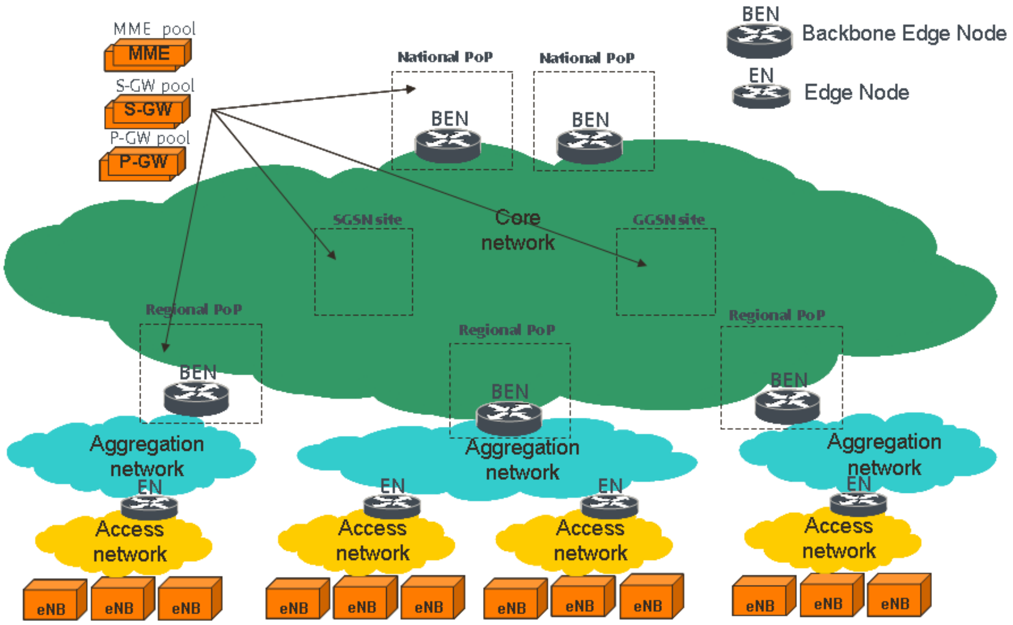


Figure 24: location flexibility of LTE mobile nodes in the transport network

MME location

The MME can be located into these different sites of the transport network:

- the SGSN site especially when SGSN migrates to MME
- the Regional PoP site (MME distribution)
- the National PoP site (MME centralization)

S-GW and P-GW location

The S-GW and P-GW can be integrated into the same node or they can be split into 2 separated nodes so they can be positioned at different sites.
The S-GW and the P-GW can be located into:

- the GGSN site when GGSN migrates to S-GW/P-GW
- the Regional PoP site (e.g. distribution case)
- the National PoP site (e.g. centralization case)

Centralized scenarios - 3G migration scenario

This scenario relies on the migration from 3G SGSN to MME and from 3G GGSN to S-GW/P-GW. The MME is located in the SGSN site and the S-GW/P-GW in the GGSN site.

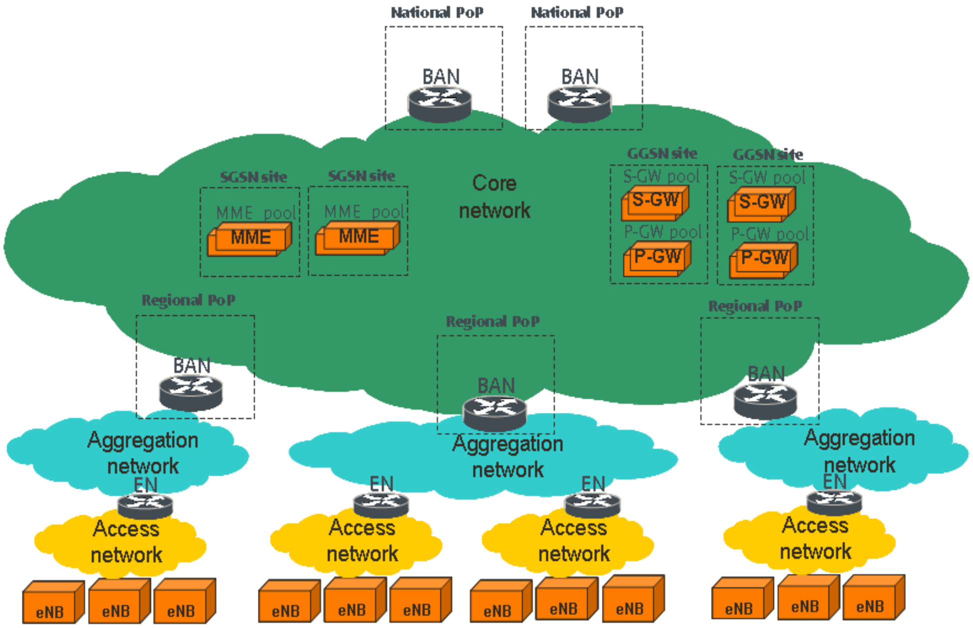


Figure 25: Centralized scenarios - 3G migration scenario

Centralized scenarios - No 3G migration scenario

The MME and S-GW/P-GW are both centralized into the National PoP site.

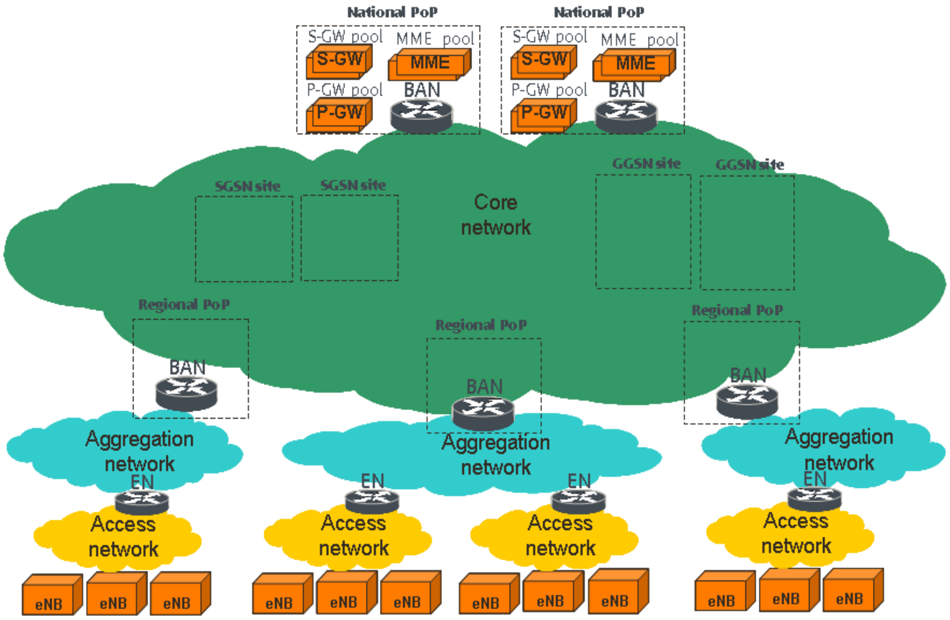


Figure 26: Centralized scenario (no 3G migration)

Distributed scenario

The MME and S-GW/P-GW are both distributed into the Regional PoP site.

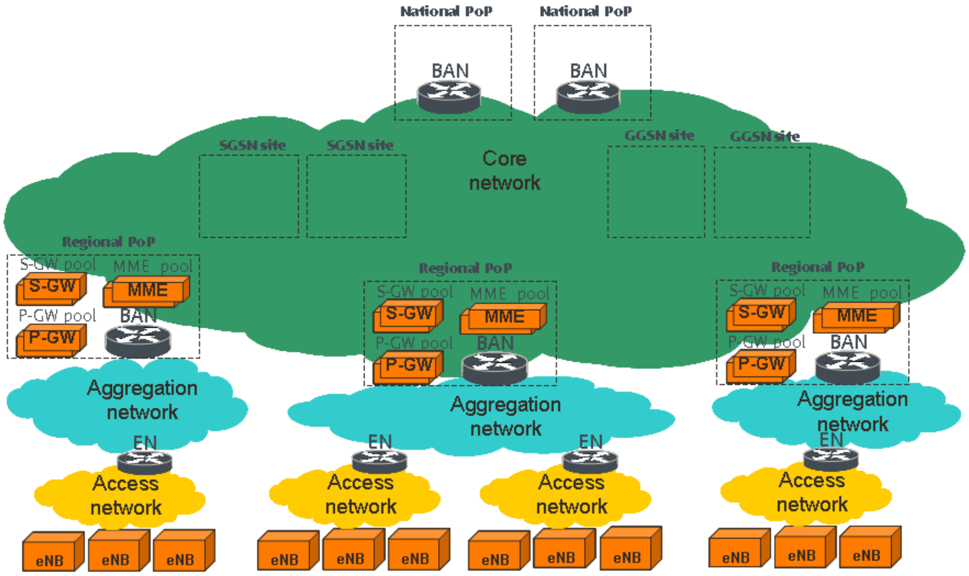


Figure 27: Distributed scenario

Hybrid scenarios - MME centralized and S-GW/P-GW distributed scenario

The MME is centralized into SGSN site (or into National PoP) site while the S-GW/P-GW are distributed into Regional PoP site.

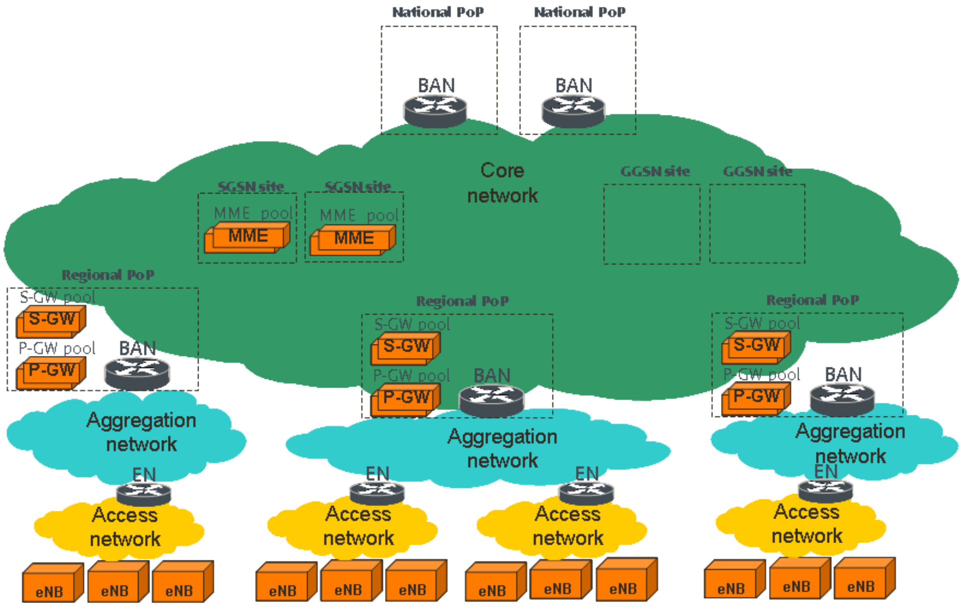


Figure 28: Hybrid scenario 1 (MME centralized, S-GW/P-GW distributed)

Hybrid scenarios - MME and P-GW centralized, S-GW distributed scenario

The MME is centralized into SGSN site (or into National PoP site) while the S-GW is distributed into Regional PoP site and the P-GW centralized into GGSN site (or into National PoP site).

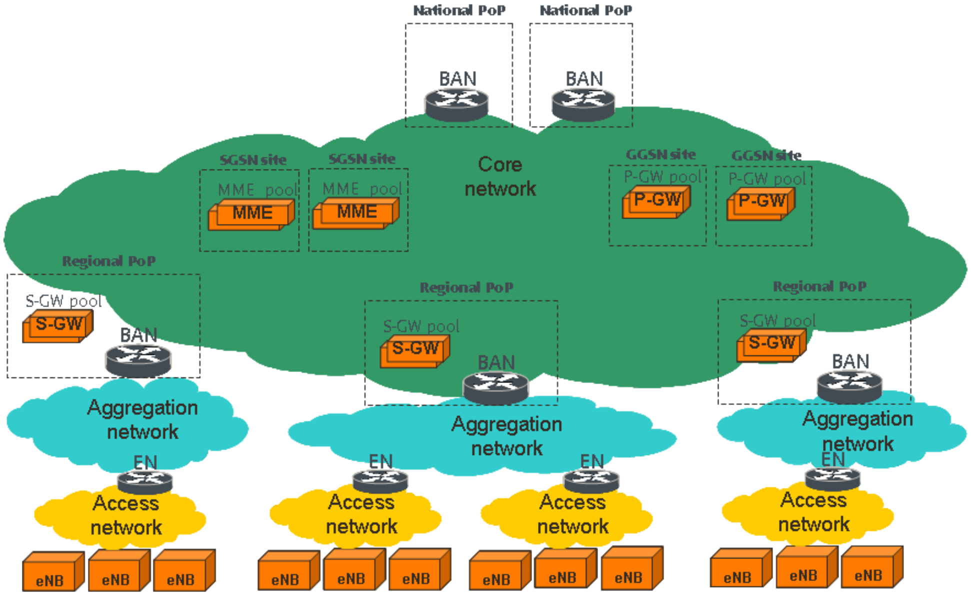


Figure 29: Hybrid scenario 2 (MME and P-GW centralized, S-GW distributed)

Hybrid scenarios - MME and S-GW distributed, P-GW centralized scenario

The MME and S-GW are distributed into Regional PoP site while the P-GW is centralized into GGSN site (or into National PoP site).

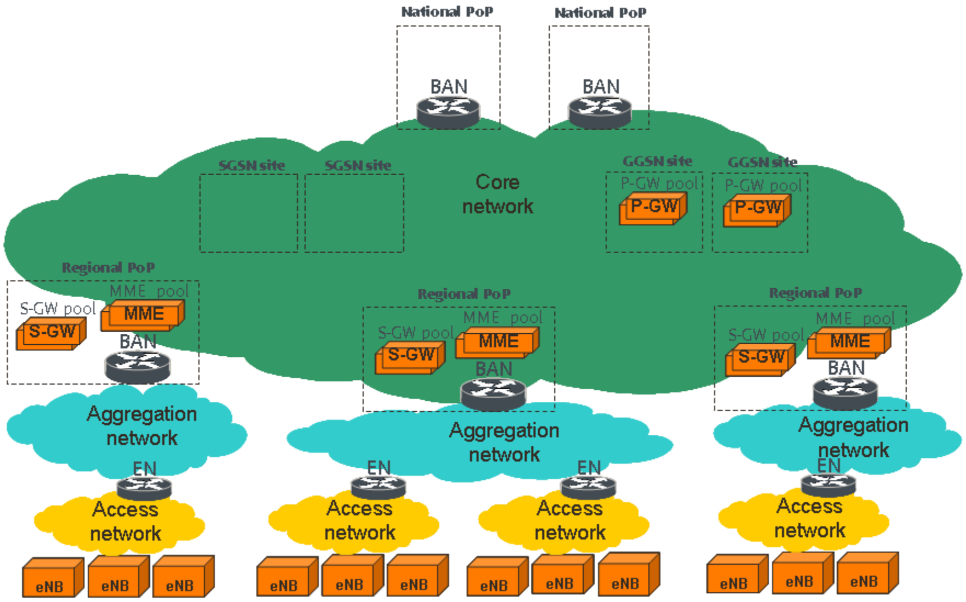


Figure 30: Hybrid scenario 3 (MME and S-GW distributed, P-GW centralized)

Hybrid scenarios - MME distributed, S-GW/P-GW centralized scenario

The MME is distributed into Regional PoP site while the S-GW and P-GW are centralized into GGSN site (or into National PoP site).

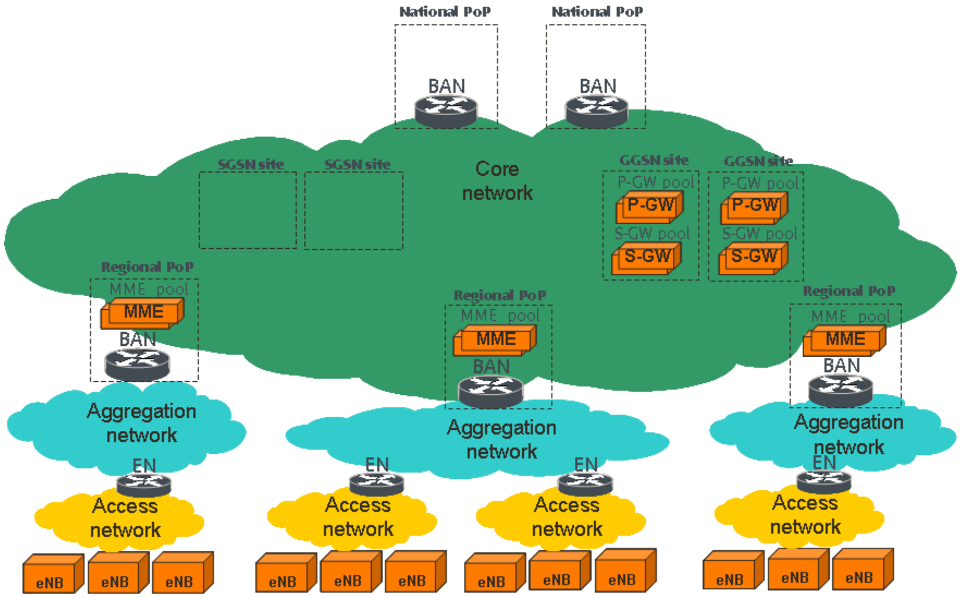


Figure 31: Hybrid scenario 4 (MME distributed, S-GW and P-GW centralized)

APPENDIX D: IP connectivity requirements for LTE networks [INFORMATIVE]

The following sections and figures briefly describe the interfaces noted. If there is a discrepancy between this document and the corresponding 3GPPP document, the 3GPP document takes precedence.

S1 interface

S1 interface is split into S1-MME interface used for Control Plane and S1-U interface for User Plane.

S1-MME interface relies on one SCTP association set up between one eNB and one MME. This SCTP association is carried over IP connectivity that is established between these two mobile nodes.
S1-U interface relies on GTP tunnels set up between one eNB and one S-GW. Multiple GTP tunnels are carried over IP connectivity that is established between these two mobile nodes.

S1-MME Flex enables to connect one eNB to multiple MMEs in order to protect MME failure, to load-balance the CP traffic between MMEs and to avoid MME relocation in case of UE mobility. IP connectivity between one eNB and each MME is required to support S1-MME Flex.

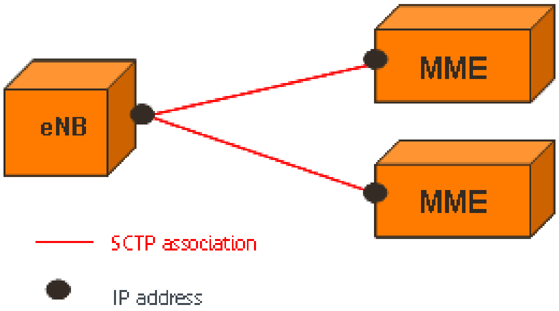


Figure 32: -MME Flex requiring IP connectivity between one eNB and each MME

S1-U Flex enables to connect one eNB to multiple S-GWs in order to protect S-GW failure, to load-balance the UP traffic between S-GWs and to avoid S-GW relocation in case of UE mobility. IP connectivity between one eNB and each S-GW is required to support S1-U Flex.

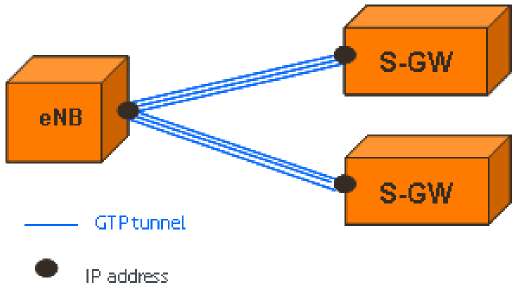


Figure 33: S1-U Flex requiring IP connectivity between one eNB and each S-GW

X2 interface

X2 interface is split into X2-C interface for Control Plane and X2-U interface for User Plane.

X2-C relies on one SCTP set up between two neighboring eNBs. This SCTP association is carried over IP connectivity that established between these two mobile nodes.
X2-U interface relies on GTP tunnels set up between neighboring eNBs. Multiple GTP tunnels are carried over IP connectivity that is established between these two mobile nodes.

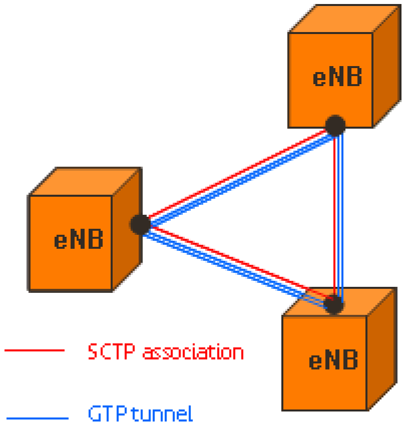


Figure 34: X2 interface requiring IP connectivity between neighboring eNBs

APPENDIX E: Mapping IP TNL Ethernet Frames At The UNI

[INFORMATIVE]

9.4 F.1 Introduction

The use cases discussed in this Appendix are examples that show how IP TNL Ethernet frame formats might be supported by the MBH.

The use cases addressed in this Appendix, describe mapping IP TNL Ethernet frames at the UNI External Interface of the mobile backhaul network to MPLS/PWs transport, based on MEF22.1 [96] (see Appendix C – Mobile Backhaul Services, Section 16.1, Use Case 1). The MEF UNI definition corresponds to the AC attached to the PEs at the edge of the MBH network. The mapping is based on IETF RFC 4448 [34].

Each deployment scenario listed in section F.2 below reflects the capabilities of the RAN BSs in supporting one of the following Ethernet frame formats and processing at the NSP between RAN BSs and MBH network. In the deployment scenarios listed in section F.3 (with exceptions listed explicitly), the RAN NC node always support IEEE 802.1Q C-VLAN frame format so the network must perform the required processing to align between the RAN BS and RAN NC frame formats.

Note that some deployment scenarios and use cases address older Base Stations that only support untagged or priority tagged Ethernet frames.

9.5 F.2 Deployment Scenarios

Deployment Scenarios presented in the Appendix are not exhaustive. They are provided to encourage interoperability, but others scenarios may be used. The scenarios noted in this Appendix attempt to highlight the most common cases that could be encountered. The assumed default NSP mode is Tag mode. Where there are alternatives using either Raw Mode or Tag mode, Tag mode is used.

Deployment Scenario A (corresponds to Scenario A in MEF 22.1) [96]:

- Each RAN BS is represented by a unique C-VLAN
- The RAN NC supports unique C-VLANs
- The NSPs connected to the RAN BS and RAN NC respectively are configured to support Tag Mode and Service-Delimiting. NSP at both sides of the PW forwards the Ethernet frames, transparently (Egress - No operation configured).

Deployment Scenario B (corresponds to Scenario B in MEF 22.1):

- Each RAN BS supports untagged frames
- The RAN NC supports unique C-VLANs
- The NSPs connected to the RAN BS and RAN NC respectively are configured to support Tag Mode and Service-Delimiting. NSP at the RAN BS side must append

ingress VLAN that uniquely identify each RAN BS. NSP at the RAN NC side must remove ingress VLAN.

Deployment Scenario C (corresponds to Scenario C in MEF 22.1):

- Each RAN BS supports priority tagged frames
- The RAN NC supports unique C-VLANs
- The NSPs connected to the RAN BS and RAN NC respectively are configured to support Tag Mode and Service-Delimiting. NSP at the RAN BS side must remove egress. NSP at the RAN NC side must swap ingress VLAN.

Deployment Scenario D (corresponds to Scenario D in MEF 22.1):

- Each RAN BS supports non unique tagged frames (identical for all RAN BSs)
- Each RAN BS is represented by a unique source MAC address
- The RAN NC supports unique tagged frames and source MAC addresses. RAN BSs are differentiated by a unique tagged.
- The NSPs connected to the RAN BS and RAN NC respectively are configured to support Tag Mode and Service-Delimiting. NSP at both RAN BS and RAN NC sides must swap VLANs to/from VLANs that uniquely identify each RAN BS.

Deployment Scenario E:

- Each RAN BS supports non unique tagged frames (identical for all RAN BSs)
- Each RAN BS is represented by a unique source MAC address
- The RAN NC supports non unique tagged frames. RAN BSs are differentiated by their source MAC address.
- The RAN BS filters the frames according to the destination MAC address.
- The NSPs connected to the RAN BS and RAN NC respectively are configured to support Tag Mode and Service-Delimiting. NSP at both sides of the PW forwards the Ethernet frames, transparently.

9.6 F.3. MBH Mapping Use Cases

Deployment Scenario A: C-VLANs on the AC are unique

- Direction from RAN BS to RAN NC
  - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress and Egress - No operation.
  - Ingress processing at the NSP connected to the RAN BS
    - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged.
  - Egress processing at the NSP connected to the RAN NC
    - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged
- Direction from RAN NC to RAN BS
  - The PE connected to the RAN NC must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress and Egress - No operation.

    - Ingress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged.
    - Egress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the RAN NC since the frames are tagged.

Deployment Scenario B: Untagged frames on the RAN BS AC

- **Direction from RAN BS to RAN NC**
    - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress append tag; Egress No operation.
    - Ingress processing at the NSP connected to the RAN BS
        - Unique C-VLAN tag must be appended to the Ethernet frames before they are delivered to the PW forwarder function (frames sent tagged).
    - Egress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the RAN NC, since the frames are tagged.

- **Direction from RAN NC to RAN BS**
    - The PE connected to the RAN NC must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress No operation; Egress Tag remove.
    - Ingress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged.
    - Egress processing at the NSP connected to the RAN BS
        - Ethernet frames with C-VLAN tags must be removed before they are delivered to the RAN BS (frames sent untagged).

Deployment Scenario C: Priority tagged frames on the RAN BS AC

- **Direction from RAN BS to RAN NC**
    - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress No operation; Egress Tag swap.
    - Ingress processing at the NSP connected to the RAN BS
        - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are priority tagged.
    - Egress processing at the NSP connected to the RAN NC
        - Priority tagged Ethernet frames must be swapped to a unique C-VLAN tag Ethernet frames before they are delivered to the RAN NC (frames sent tagged).
- **Direction from RAN NC to RAN BS**
    - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress No operation; Egress Tag remove.

    - Ingress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the PW forwarder function, since the frames are tagged.
    - Egress processing at the NSP connected to the RAN BS
        - Ethernet frames with C-VLAN tags must be removed before they are delivered to the RAN BS (frames sent untagged).

Deployment Scenario D: Non unique tagged frames on the AC

- **Direction from RAN BS to RAN NC**
    - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress No operation; Egress Tag swap.
    - Ingress processing at the NSP connected to the RAN BS
        - Ethernet frames must be delivered transparently to the PW forwarder function, since the frames are tagged.
    - Egress processing at the NSP connected to the RAN NC
        - C-VLAN tagged Ethernet frames must be swapped to a unique C-VLAN tag Ethernet frames before they are delivered to the RAN NC (frames sent tagged)
- **Direction from RAN NC to RAN BS**
    - The PE connected to the RAN NC must be configured to support Tag Mode and Service-Delimiting. Required Operation: Ingress No operation; Egress Tag swap.
    - Ingress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the PW forwarder function, since the frames are tagged.
    - Egress processing at the NSP connected to the RAN BS
        - Unique C-VLAN tagged Ethernet frames must be swapped to a non unique C-VLAN tag Ethernet frames before they are delivered to the RAN BS (frames sent tagged)

Deployment Scenario E: Non Unique Tagged frames on the AC

- **Direction from RAN BS to RAN NC**
    - The PE connected to the RAN BS must be configured to support Tag Mode and Service-Delimiting. Note that the RAN BS and RAN NC both filter Ethernet frames according to their DA MAC addresses. The Tag on each frame is only used for carrying the priority of the frame (via priority bits). Required Operation: Ingress and Egress - No operation.
    - Ingress processing at the NSP connected to the RAN BS
        - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged.
    - Egress processing at the NSP connected to the RAN NC
        - Ethernet frames must be delivered transparently to the RAN NC since the frames are tagged (non unique tag). The RAN NC identifies the RAN BSs according to their source MAC address.
- **Direction from RAN NC to RAN BS**

- The PE connected to the RAN NC must be configured to support Tag Mode and Service-Delimiting.
- Ingress processing at the NSP connected to the RAN NC
    - Ethernet frames must be delivered transparently to the PW forwarder function since the frames are tagged (non unique tag). The correct PW is selected by lookup on the destination MAC address.
- Egress processing at the NSP connected to the RAN BS
    - Ethernet frames must be delivered transparently to the RAN BS since the frames are tagged. The RAN BS filters the frames according to the destination MAC address.

APPENDIX F: E-Tree* - Partially Implementing MEF Rooted-Multipoint Service using VPLS with Partial Mesh of PWs

[INFORMATIVE]

MEF has defined a rooted-multipoint EVC based on E-Tree service type. In a Rooted-Multipoint EVC, one or more of the UNIs must be designated as a Root and each of the other UNIs must be designated as a Leaf. An ingress Service Frame mapped to the EVC at a Root UNI may be delivered to one or more of the other UNIs in the EVC. An ingress Ethernet frame mapped to the EVC at a Leaf UNI must not result in an egress Ethernet frame at another Leaf UNI but may result in an egress Ethernet frame at some or all of the Root UNIs.

To date, IETF has not specified a solution based on MPLS that fully satisfies MEF rooted-multipoint service requirements.
However, partial solutions based on VPLS could be implemented. A VFI in the current VPLS solutions cannot distinguish between packets and hence cannot filter at a leaf AC packets that are generated by another leaf AC.

This Appendix discusses an MPLS based implementation solution using partial mesh of PWs to create the required service model. This is called the E-Tree* service.

This Appendix discusses an MPLS based implementation solution using a partial solution that provide the VPLS supports for the MEF defined rooted-multipoint service requirements. The following exceptions are assumed:

- Root and leaf ACs do not use the same VFI.
- Each PW can only be used to convey packets from either root or leaf AC but not both
- Only a single root AC can be supported by the rooted-multipoint service
- No VLAN manipulation is allowed on PWs, only on the NSF function.

The following network model depicts the proposed solution for rooted-multi-point service with VPLS partial mesh deployment.

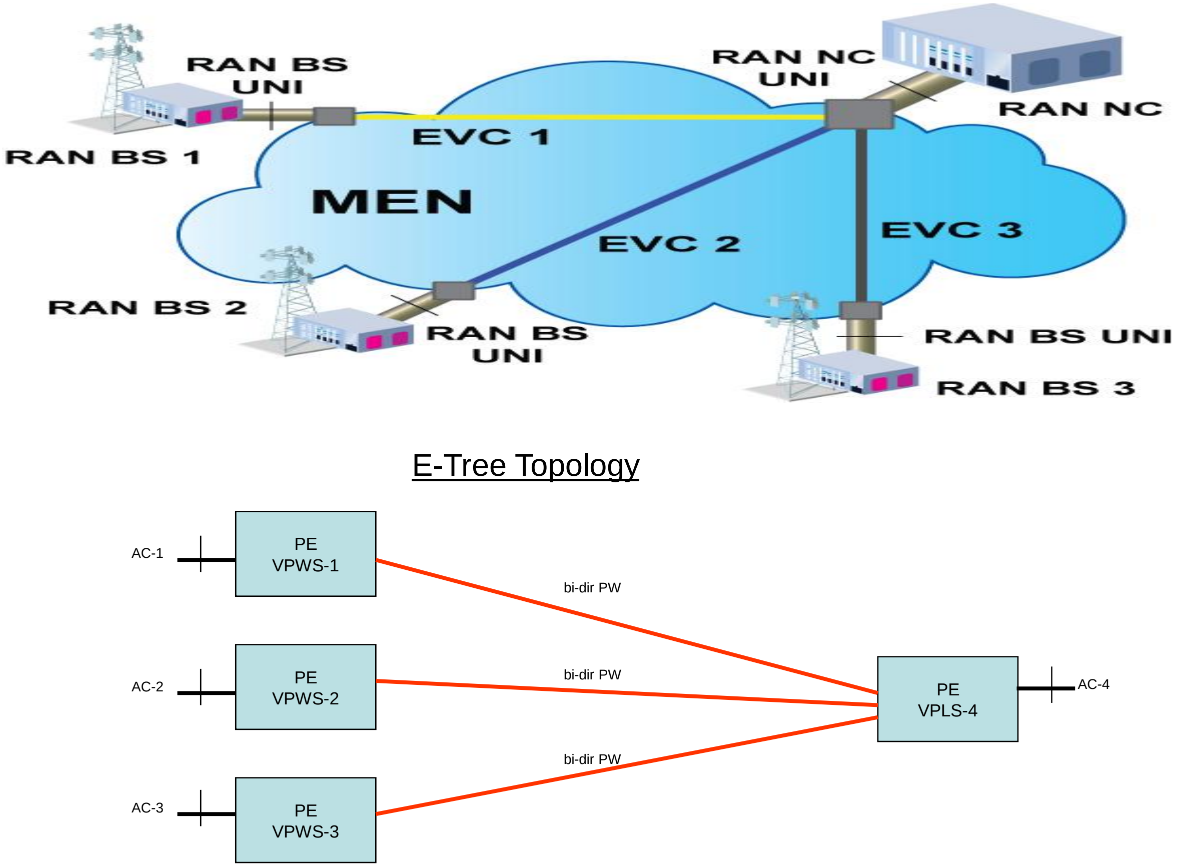


Figure 35: partial mesh topology implementing MEF rooted-multipoint services

End of Broadband Forum Technical Report TR-221