TECHNICAL REPORT

TR-224
Technical Specification for MPLS in Carrier Ethernet Networks

Issue: 1
Issue Date: September 2014

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 SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER the Forum, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

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 Number	Approval Date	Publication Date	Issue Editor	Changes
1	8 September 2014	27 October 2014	Rao Cherukuri, Juniper Networks Scott Mansfield, Ericsson	Original

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

Editor	Rao Cherukuri	Juniper Networks
	Scott Mansfield	Ericsson
IP/MPLS&Core WG Co-Chairs	David Sinicrope	Ericsson
	Drew Rexrode	Verizon

Table of Contents

List of Figures

List of Tables

Executive Summary

Carrier Ethernet provides extensions to Ethernet enabling telecommunications network providers to provide Ethernet services to customers and to utilize Ethernet technology in their networks. Service providers are deploying Carrier Ethernet services around the globe, in large part, because Carrier Ethernet has compelling capabilities such as standardized service definitions as well as improved scalability, reliability, QoS, and manageability.

The MEF has defined Carrier Ethernet as a ubiquitous, standardized, carrier-class Service and Network defined by attributes that distinguish Carrier Ethernet from familiar LAN based Ethernet.

MEF 6.1 [67] specifies the Ethernet services types. It includes point to point (E-line), point to multipoint (E-Tree) and multipoint to multipoint (E-LAN). The service definition includes both port based and VLAN based service identification. MEF 10.2 [69] defines the service attributes.

TR-145 [2] and TR-178 [3] provide a set of architectures for broadband multi-service network, addressing typical infrastructures, topologies and deployment scenarios, and specify associated nodal requirements. This document provides technical architecture and equipment requirements implementing the specified Ethernet services with an MPLS network. By specifying a common technical architecture, common equipment requirements and common set of feature options, this document promotes multi-vendor interoperability.

1 Purpose and Scope

1.1 Purpose

Carrier Ethernet provides extensions to Ethernet enabling telecommunications network providers to provide Ethernet services to customers and to utilize Ethernet technology in their networks. Service providers are deploying Carrier Ethernet services around the globe, in large part, because Carrier Ethernet has compelling capabilities such as standardized service definitions as well as improved scalability, reliability, QoS, and manageability.

Carrier Ethernet services are being used in Broadband access networks, enterprise networks and backhaul networks. This document provides technical architecture and equipment requirements implementing the specified Ethernet services with an MPLS network. By specifying a common technical architecture, common equipment requirements and common set of feature options, this document promotes multi-vendor interoperability. This document may be used as a basis for conformance testing.

1.2 Scope

This document defines a reference architecture for Carrier Ethernet Services using Layer 2 VPN mechanisms:

- Ethernet point to point (E-Line) and multipoint to multipoint (E-LAN)
- A subset of point to multipoint (E-Tree*- defined in TR-221 [4])
- Control, OAM, QoS, reliability and scalability for the MPLS network

This document specifies how to implement the Ethernet services layer. It does not specify the service layer itself. Ethernet Control and OAM protocols will be transparently transported, except for cases where Layer 2 control protocol processing is required per service definition.

In order to support Carrier Ethernet services across multiple networks, the scope of this document includes the following:

- Attachment circuits providing user-to-network interface complying with Metro Ethernet Forum (MEF UNI) are supported.
- Supporting Ethernet attachment circuits for multi-service broadband access and aggregation (i.e., TR-101/TR-178) are supported.
- To support carrier Ethernet across multiple SP networks, the specification addresses multi autonomous systems which preserves end to end capabilities (e.g., OAM, QoS and protection etc).
- Cases where the UNI-N functions are or are not collocated with the PE are addressed.

External domain interfaces such as support of ENNI [71] and MPLS-ICI [5] are for further study.

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 [10].

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.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.
A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-101	*Migration to Ethernet-Based Broadband Aggregation*	BBF	2011
[2]	TR-145	*Multi-service Broadband Network Functional Modules and Architecture*	BBF	2012
[3]	TR-178	*Multi-service Broadband Network Architecture*	BBF	2014

		and Nodal Requirements		
[4]	TR-221	*Technical Specification for MPLS in Mobile Backhaul Networks*	BBF	2011
[5]	IP/MPLS Forum 19.0.0	*MPLS Inter-Carrier Interconnect (MPLS-ICI) Technical Specification*	BBF	2008
[6]	IP/MPLS Forum 22.0.0	*BGP Auto-Discovery and Signaling for VPWS-based VPN services*	BBF	2009
[7]	IEEE 802.1Q	*IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks*	IEEE	2011
[8]	IEEE 802.3	*IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*	IEEE	2008
[9]	RFC 1195	*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*	IETF	1990
[10]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[11]	RFC 2328	*OSPF Version 2*	IETF	1998
[12]	RFC 3107	*Carrying Label Information in BGP-4*	IETF	2001
[13]	RFC 3209	*RSVP-TE: Extensions to RSVP for LSP Tunnels*	IETF	2001
[14]	RFC 3270	*Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*	IETF	2002
[15]	RFC 3386	*Network Hierarchy and Multilayer Survivability*	IETF	2002
[16]	RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*	IETF	2003
[17]	RFC 3478	*Graceful Restart Mechanism for Label Distribution Protocol*	IETF	2003
[18]	RFC 3623	*Graceful OSPF Restart*	IETF	2003
[19]	RFC 3630	*Traffic Engineering (TE) Extensions to OSPF Version 2*	IETF	2003
[20]	RFC 3809	*Generic Requirements for Provider Provisioned Virtual Private Networks*	IETF	2004

		(PPVPN)		
[21]	RFC 3847	*Restart Signaling for Intermediate System to Intermediate System (IS-IS)*	IETF	2004
[22]	RFC 3916	*Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*	IETF	2004
[23]	RFC 3985	*Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*	IETF	2005
[24]	RFC 4090	*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*	IETF	2005
[25]	RFC 4111	*Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)*	IETF	2005
[26]	RFC 4206	*Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*	IETF	2005
[27]	RFC 4364	*BGP/MPLS IP Virtual Private Networks*	IETF	2006
[28]	RFC 4379	*Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*	IETF	2006
[29]	RFC 4385	*Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*	IETF	2006
[30]	RFC 4446	*IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*	IETF	2006
[31]	RFC 4447	*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*	IETF	2006
[32]	RFC 4448	*Encapsulation Methods for Transport of Ethernet over MPLS Networks*	IETF	2006
[33]	RFC 4664	*Framework for Layer 2 Virtual Private Networks (L2VPNs)*	IETF	2006
[34]	RFC 4761	*Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*	IETF	2007
[35]	RFC 4762	*Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*	IETF	2007
[36]	RFC 4928	*Avoiding Equal Cost Multipath Treatment in MPLS Networks*	IETF	2007
[37]	RFC 5036	*LDP Specification*	IETF	2007
[38]	RFC 5085	*Pseudowire Virtual Circuit Connectivity Verification (VCCV) A Control Channel for Pseudowires*	IETF	2007
[39]	RFC 5150	*Label Switched Path Stitching with*	IETF	2008

		Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)		
[40]	RFC 5151	*Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*	IETF	2008
[41]	RFC 5254	*Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)*	IETF	2008
[42]	RFC 5283	*LDP Extension for Inter-Area Label Switched Paths (LSPs)*	IETF	2008
[43]	RFC 5286	*Basic Specification for IP Fast Reroute: Loop-Free Alternates*	IETF	2008
[44]	RFC 5305	*IS-IS Extensions for Traffic Engineering*	IETF	2008
[45]	RFC 5586	*MPLS Generic Associated Channel*	IETF	2009
[46]	RFC 5603	*Ethernet Pseudowire (PW) Management Information Base (MIB)*	IETF	2009
[47]	RFC 5880	*Bidirectional Forwarding Detection (BFD)*	IETF	2010
[48]	RFC 5881	*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*	IETF	2010
[49]	RFC 5883	*Bidirectional Forwarding Detection (BFD) for Multihop Paths*	IETF	2010
[50]	RFC 5884	*Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs*	IETF	2010
[51]	RFC 5885	*Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*	IETF	2010
[52]	RFC 5994	*Application of Ethernet Pseudowires to MPLS Transport Networks*	IETF	2010
[53]	RFC 6072	*Certificate Management Service for the Session Initiation Protocol (SIP)*	IETF	2011
[54]	RFC 6073	*Segmented Pseudowire*	IETF	2011
[55]	RFC 6074	*Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*	IETF	2011
[56]	RFC 6310	*Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*	IETF	2011
[57]	RFC 6374	*Packet Loss and Delay Measurement for MPLS Networks*	IETF	2011
[58]	RFC 6391	*Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*	IETF	2011

[59]	RFC 6424	*Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*	IETF	2011
[60]	RFC 6478	*Pseudowire Status for Static Pseudowires*	IETF	2012
[61]	RFC 6790	*The Use of Entropy Labels in MPLS Forwarding*	IETF	2012
[62]	RFC 6870	*Pseudowire Preferential Forwarding Status Bit*	IETF	2013
[63]	RFC 7023	*Extension to LDP-VPLS for Ethernet Broadcast and Multicast*	IETF	2013
[64]	RFC 7117	*Multicast in Virtual Private LAN Service (VPLS)*	IETF	2014
[65]	ITU-T G.8032 / Y.1344	*Ethernet ring protection switching*	ITU-T	2012
[66]	ITU-T Y.1564	*Ethernet service activation test methodology*	ITU-T	2011
[67]	MEF 6.1	*Ethernet Services Definitions - Phase 2*	MEF	2008
[68]	MEF 6.1.1	*Layer 2 Control Protocol Handling Amendment to MEF 6.1*	MEF	2012
[69]	MEF 10.2	*Ethernet Services Attributes - Phase 2*	MEF	2009
[70]	MEF 22.1	*Mobile Backhaul Phase 2 Implementation Agreement*	MEF	2012
[71]	MEF 26	*External Network Network Interface (ENNI) – Phase 1*	MEF	2010
[72]	MEF 30	*Service OAM Fault Management Implementation Agreement*	MEF	2011
[73]	MEF 35	*Service OAM Performance Monitoring Implementation Agreement*	MEF	2012

2.3 Definitions

The following terminology is used throughout this Technical Report.

AGN	An aggregation node (AGN) is a node which aggregates several access nodes (ANs).
AN	An access node is a node which processes customers frames or packets at Layer 2 or above. This includes but is not limited to DSLAMs or OLTs (in case of (G)PON deployments).
E-Line	A service connecting two customer Ethernet ports over a WAN.

E-LAN	A multipoint service connecting a set of customer endpoints, giving the appearance to the customer of a bridged Ethernet network connecting the sites.
E-Tree*	Partially implementing MEF multipoint service connecting only one root and a set of leaves, but preventing inter-leaf communication. See details in TR-221 [4]. Note: Ethernet Tree (E-Tree) service type is specified in section 6.3/MEF 6.1 [67]. The Appendix in TR-221[4] modifies E-Tree service type which is used in different services. The modified E-Tree* service type is used in both Ethernet Private Tree service and Ethernet Virtual Private Tree Service specified in section 13.
SN	Service node is used to create services for customers and is connected to one or more transport nodes. Typical examples include Broadband Network Gateways (BNGs), video servers.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

AC	Attachment Circuit
AGN	Aggregation Node
AN	Access Node
ASBR	Autonomous System Border Router
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
CBS	Committed Burst Size
CE	Customer Edge
CES	Circuit Emulation Service
CIR	Committed Information Rate
CoS	Class of Service
CV	Connectivity Verification
EBS	Excess Burst Size
EIR	Excess Information Rate
EPL	Ethernet Private Line
EP-LAN	Ethernet Private-LAN
ERP	Ethernet Ring Protection
EVC	Ethernet Virtual Connection
EVPL	Ethernet Virtual Private Line
EVP-LAN	Ethernet Virtual Private - LAN
FD	Frame Delay

FRR	Fast ReRoute
FLR	Frame Loss Ratio
H-VPLS	Hierarchal Virtual Private LAN Service
IETF	Internet Engineering Task Force
IFDV	Inter-Frame Delay Variation
IP	Internet Protocol
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
L2VPN	Layer 2 Virtual Private Network
LAN	Local Area Network
LER	Label Edge Router
LFA	Loop Free Alternate
LSP	Label Switched Path
LSR	Label Switch Router
MAC	Medium Access Control
MEF	Metro Ethernet Forum
MPLS	Multi Protocol Label Switching
MS-PW	Multi-Segment Pseudowire
NSP	Native Service Processing
OAM	Operations, Administration and Management
OAMPDU	OAM Protocol Data Unit
P	Provider
PE	Provider Edge
PSN	Packet Switched Network
PW	Pseudowire
QoS	Quality of Service
RFC	Request for Comments
RSVP-TE	Resource ReSerVation Protocol
SLA	Service Level Agreement
SN	Service Node
S-PE	Switching Provider Edge Router
SS-PW	Single-Segment Pseudowire
TE	Traffic Engineering
T-LDP	Targeted Label Distribution Protocol
TLV	Type/Length/Value
T-PE	Terminating Provider Edge Router
TR	Technical Report
UNI	User to Network Interface

UDP	User Datagram Protocol
VCCV	Virtual Circuit Connectivity Verification
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WG	Working Group

3 Technical Report Impact

3.1 Energy Efficiency

TR-224 has no impact on energy efficiency.

3.2 IPv6

Carrier Ethernet services operate at layer 2 and therefore the network is agnostic to IPv6 user traffic. The IPv6 QoS or DSCP is assumed to be mapped to the Ethernet P bits by the service user.

IPv6 addressing may appear in its respective places in control, OAM, and management protocols. For example node ids, FECs, and loopback addresses, etc.

TR-224 has no impact on IPv6.

3.3 Security

Security requirements are specified for each service in respective sections.

3.4 Privacy

Any issues regarding privacy are not affected by TR-224.

4 Carrier Ethernet Services

Ethernet is now being used as both transport technology and service delivery architecture. MEF 6.1 [67] specifies the Ethernet services types. It includes point to point (E-line), point to multipoint (E-Tree) and multipoint to multipoint (E-LAN). The service definition includes both port based and VLAN based service identification. MEF 10.2 [69] defines the service attributes.

The MEF also defined Carrier Ethernet as a ubiquitous, standardized, carrier-class Service and Network defined by attributes that distinguish Carrier Ethernet from familiar LAN based Ethernet.

4.1 Carrier Ethernet Requirements

Service providers worldwide are migrating their existing networks to deliver Carrier Ethernet services to Enterprises, businesses & residential end-users. The attributes are as follows:

1. Standardized Services
   - Support E-Line, E-LAN and E-Tree service types as defined by MEF
   - no changes to customer LAN equipment or networks and accommodates existing network connectivity such as, time-sensitive, TDM traffic and signaling
   - Wide choice and granularity of bandwidth and quality of service options
2. Security
3. Scalability
   - The ability for millions of Ethernet Virtual Connection (EVC) services for enterprise and residential users
   - Scalability of bandwidth from 1Mbps to 10Gbps and beyond, in granular increments
4. Reliability
   - The ability for the network to detect & recover from faults quickly
   - Fast network convergence
5. Quality of Service
   - Service Level Agreements (SLAs) that deliver end-to-end performance
   - Traffic profile enforcement per EVC
   - Hierarchical queuing
6. Service Management
   - Minimize network touch points in provisioning
   - Standards based OAM to support SLA

5 MPLS L2VPN – VPWS and VPLS

MPLS has for a longtime been defined as a convergence technology, one that will allow service providers to bring together their disparate networks and leverage features like traffic engineering, hierarchal QoS and service interworking.

Provider Provisioned Virtual Private Networks (PPVPN) now dominates the IP-VPN services market and projected for significant growth. Many service providers have also introduced virtual private LAN services (VPLS) as a simpler alternative that allows enterprises to manage their own IP routing.

RFC 4664 [33] provides a framework for Layer 2 Provider Provisioned Virtual Private Networks (L2VPNs). It supports two different Layer 2 VPN service: Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS).

A VPWS is an MPLS based VPN service that provides Ethernet point to point (E-line) service between users. The network carries service traffic between two users using Pseudo Wire Emulation Edge to Edge (PWE3) over the underlying MPLS tunnels.

A VPLS service appears, in (almost) all respects, as an Ethernet LAN to customers of a Service Provider, however, the customers may be spread across a metro or wide area. This is accomplished by incorporating MAC address learning, flooding, and forwarding functions in Ethernet switching nodes connected by pseudowires across the packet switched network, to appear and function as a single LAN. VPLS supports functionality similar to bridging function defined in IEEE 802.1Q [7].

VPLS services are gaining momentum and require scalable solutions to extend the service reach beyond the metro network. The IETF specifies different approaches to improve scalability of VPLS (e.g., H-VPLS in RFC 4762 [35]).

RFC 4761 [34] and RFC 4762 [35] specify signaling mechanisms for VPLS. Although both use the same PWE3 forwarding plane, the scaling; provisioning and multicast replications are different. RFC 4761 [34] uses BGP for signaling and auto-discovery; RFC 4762 [35] uses Targeted LDP for signaling and may be coupled with the auto-discovery function.

RFC 6074 [55] specifies provisioning, auto-discovery and signaling in L2VPNs. The discovery is based on the Border Gateway Protocol (BGP). When the auto-discovery process is complete, the signaling protocol LDP is used to set up PWs. RFC 6074 [55] also enable support of Inter-AS operation with LDP signaling.

An E-Tree is a multipoint Ethernet service type. At the time of publication of this document, support of MEF E-Tree service types over an MPLS Network is work in progress in the IETF.

The only difference between E-LAN and E-Tree is:

- E-LAN has Root endpoints only, which implies there is no communication restriction between endpoints

- E-Tree has both Root and Leaf endpoints, which implies there is a need to enforce communication restriction between Leaf endpoints

In this release of the specification, a subset of multipoint E-Tree service type is supported. The description of the subset called E-Tree* is provided in TR-221 [4].

6 Reference Architecture

6.1 General Reference Architecture

Figure 1 provides a generic overview of how Carrier Ethernet Services can be deployed using an MPLS-based L2VPN infrastructure, including basic reference points and their functional roles. Depending on the application, non MEF defined Ethernet Attachment Circuits and Attachment Circuits providing User-to-Network interfaces complying with Metro Ethernet Forum definitions (MEF UNI) are supported. Multi-domain connectivity and external handoff are supported.

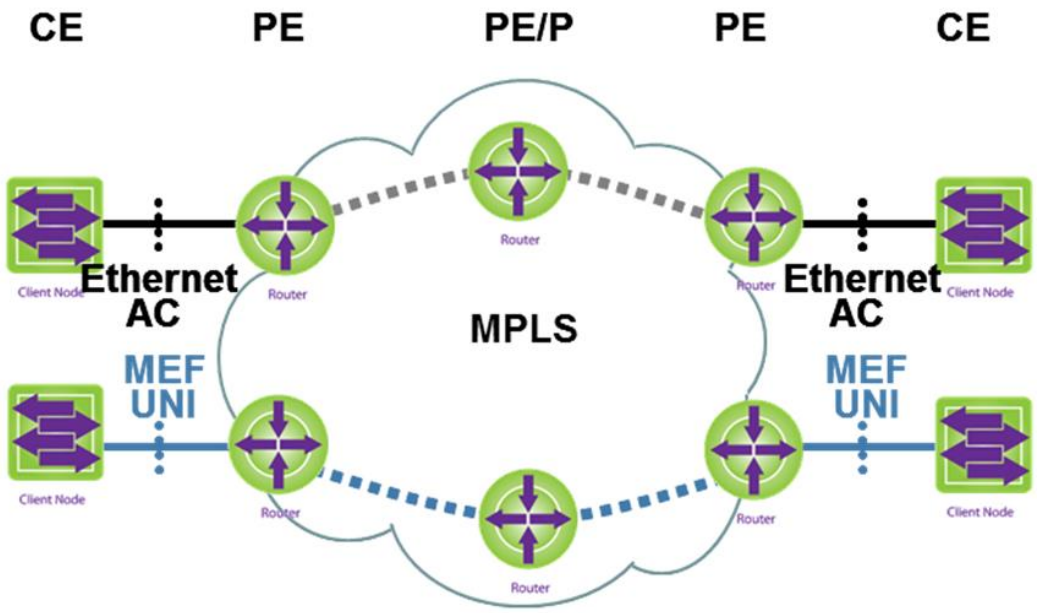

Figure 1 - Reference Architecture

Defined as business interfaces supporting the service handoff between different parties (between user and provider or between providers, respectively), UNI has two functions:

1. provide reference points for network demarcation
2. provide associated functionality

For deploying Metro Ethernet Forum compliant Ethernet Services over MPLS, PE nodes need to support the corresponding MEF UNI functionality at Attachment Circuit interfaces.

6.2 MPLS for Carrier Ethernet in Broadband Access & Aggregation

6.2.1 Multi-Service Broadband Access & Aggregation

The TR-145 [2] /TR-178 [3] Multi-Service Architecture requires support of an Ethernet service & aggregation layer between the U1 and A10 reference points. Additional functionality, in the areas

of business services, OAM, Quality of Service, Multicast and service discrimination, is required as well, in order to support different service types on a common network infrastructure.

MPLS supports multi-service adaptation and transport in broadband access, aggregation and core networks and has been adopted in the BBF Multi-Service Architecture. MPLS-based L2VPN can be used to accommodate and leverage common Ethernet/VLAN service access structures and mapping schemes for customer service identification, providing a versatile, scalable, carrier-grade aggregation and transport to the service edge.

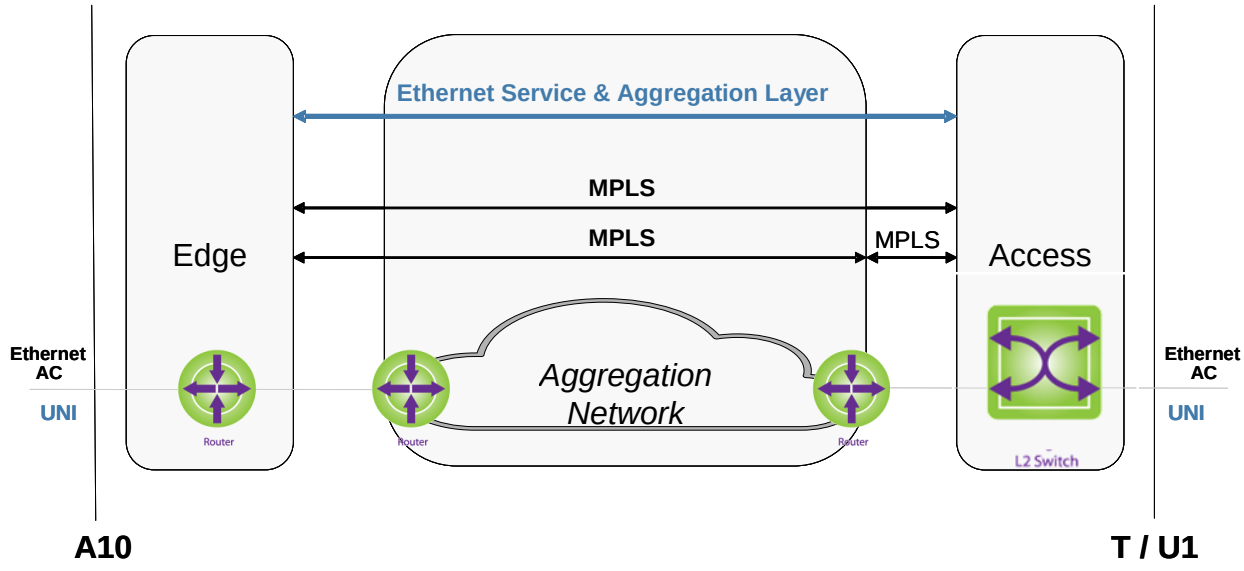

Figure 2 - Reference Architecture for Multi-Service Broadband Access & Aggregation

All requirements imposed by the service layer and its related user & business interfaces, clustered by reference points, are to be supported by the underlying MPLS adaptation and transport layer.

As defined by TR-145 [2], a UNI can be instantiated at either the U (access function set) or T (customer location function set) reference points, depending on the type of service (residential access or business VPN) and the type of hand-off (between Ethernet Service Provider and Regional Broadband Provider or between Ethernet Service Provider and end customer).
A10 is the reference point at which the Regional Access Network and Service Provider POPs interconnect.

6.2.2 TR-178 Architectures

There are two reference architectures that are being used to represent TR-178 networks: 1) MPLS enabled access and 2) TR-101. Within MPLS enabled access, there are two different types of access nodes.

Within the two reference architectures listed above, both MEF UNI and TR-101 UNI are supported. The attachment circuits for the two reference architectures above are Ethernet.

6.2.2.1 Architectures with MPLS Enabled Access Node

The approaches generally fall into two classes. The first is the use of MPLS for backhaul of customer traffic to service edges; the second is to push the service edge closer to the customer.

In both cases the MPLS edge is co-located with the access node, which leads to two classes of nodes not previously considered in BBF architectures. These are:

- The MPLS enabled access node (MAN) which is a class of access node that implements the minimum set of sufficient MPLS functionality needed for it to serve in a backhaul role
- The BNG enabled access node (BAN) which is an access node that implements the set of features normally associated with the combination of an Access node, a subset of MS-BNG features and an MPLS PE.

For additional details see TR-178 [3] section 4.3.

Both types of access nodes support Ethernet attachments circuits and MEF UNI. The MEF Ethernet services are specified between two or more MEF UNIs. This specification provides both connectivity and support service options for MEF services.

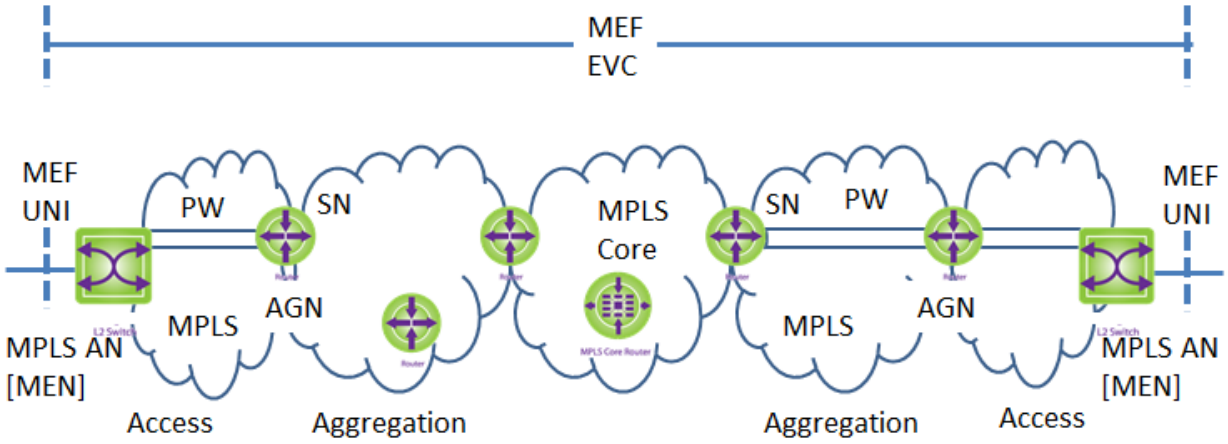

Figure 3 - Seamless MPLS using MPLS enabled Access Node [MAN]

The seamless MPLS architecture can be applied to L2 VPN services. For E-Line services, a point-to-point PW is provisioned end to end between access nodes. For E-LAN services, a PW is provisioned at the access node and is then transparently mapped to an Ethernet service at the Ethernet service node. In this case it looks similar to an H-VPLS (RFC 4762 [35]) spoke.

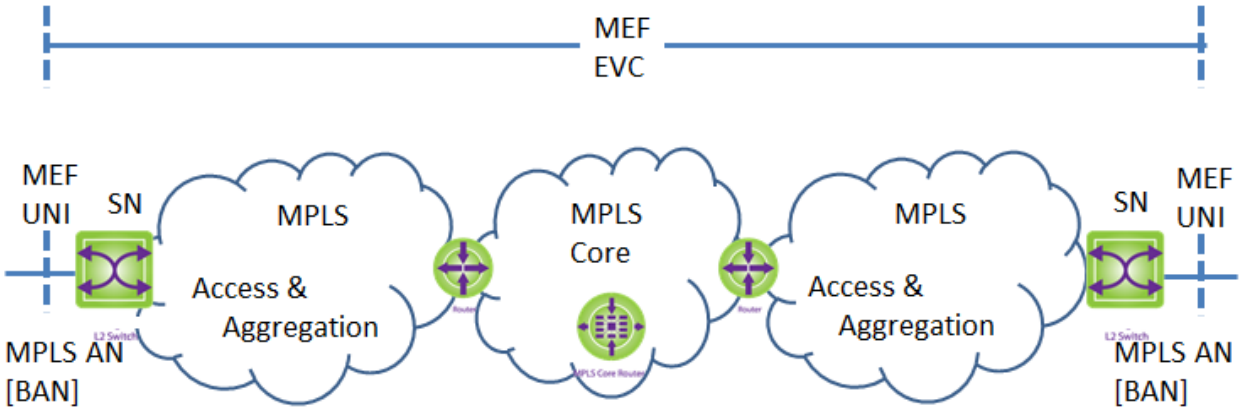

Figure 4 - Full MPLS in Access Node – BNG-enabled Access Node [BAN]

6.2.2.2 TR-101 Architectures

TR-178 [3] also supports TR-101 architecture which is shown in Figure 5 to support Ethernet services. In this case the MEF EVC consists of three segments. The two end segments are TR-101 [1] segments. TR-224 only supports the MPLS segment in the middle connecting the two TR-101 [1] Ethernet segments.
The Ethernet attachment circuit to PE is not a MEF UNI. The PE does not provide mapping of MEF service parameters, end-to-end QoS and OAM.

In this case, TR-224 describes connectivity of E-line and E-LAN service based on the provisioned MPLS segment parameters.

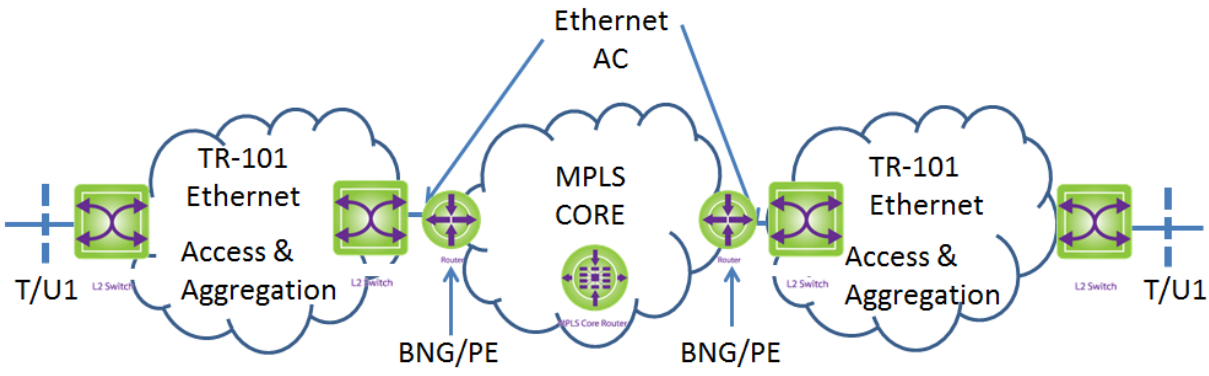

Figure 5 - TR-101 Ethernet Access and Aggregation with MPLS Core

7 LSP Signaling and Routing

This section specifies the signaling protocol used to establish the underlying MPLS tunnel that carry pseudowires.

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.

7.1 LSP Signaling

One of the following provisioning and signaling procedures are used for LSPs.

[R-1] PE and P routers supporting MPLS TE and non-TE LSPs MUST support one or both of the following methods:
- Static provisioning
- Dynamic signaling

[R-2] 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 [37].
- RSVP-TE is used to set up, maintain and release LSPs for traffic engineered tunnels per RFC 3209 [13] and RFC 5151 [40]. When traffic engineering is needed on the LSP, RSVP-TE MUST be used.

[R-3] When co-routed bidirectional LSPs are required, GMPLS-RSVP-TE as per RFC 3473 [16] MAY be supported by PE and P routers.

7.1.1 Multi-area LSP Signaling

Several operators have multi-area networks for scalability. Link state Interior Gateway Protocols (IGPs) such as OSPF (RFC 2328 [11]) and IS-IS (RFC 1195 [9]) allow dividing networks into areas or levels so as to increase routing scalability within a routing domain.

Further some operators L2VPN network span different geographical areas. To support these networks, it is necessary to support inter-area and inter-AS (Autonomous System) Multiprotocol Label Switching (MPLS) LSPs.

An “MPLS Domain” is considered to be any collection of network elements within a common realm of address space or path computation responsibility. Examples of such domains include Autonomous Systems, Interior Gateway Protocol (IGP) routing areas, and GMPLS overlay networks.

Inter-area LSPs (that is, LSPs that traverse at least two IGP areas) signaling extensions are required to ensure MPLS connectivity between PEs located in distinct IGP areas.

7.1.1.1 Multi-area RSVP-TE Signaling

Inter-domain TE LSPs can be supported by one of three options as specified in RFC 5151 [40] and given below:

- contiguous LSPs
- nested LSPs
- stitched LSPs.

Contiguous

A contiguous TE LSP is a single TE LSP that is set up across multiple domains using RSVP-TE signaling procedures described in Section 7.1.

Nested

One or more TE LSPs may be nested within another TE LSP as described in RFC 4206 [26]. This technique can be used to nest one or more inter-domain TE LSPs into an intra-domain hierarchical LSP (H-LSP). The label stacking construct is used to achieve nesting in packet networks.

To improve scalability, it may be useful to aggregate LSPs by creating hierarchy of such LSPs.

[R-4] PE routers SHOULD support establishment of RSVP-TE LSPs using LSP hierarchy as per RFC 4206 [26].

Stitched

LSP stitching signaling procedures are described in RFC5150 [39]. This technique can be used to stitch together shorter LSPs (LSP segments) to create a single, longer LSP. The LSP segments of an inter-domain LSP may be intra-domain LSPs or inter-domain LSPs.

The process of stitching LSP segments results in a single, end-to-end contiguous LSP in the data plane. But in the control plane, each segment is signaled as a separate LSP (with distinct RSVP sessions) and the end-to-end LSP is signaled as yet another LSP with its own RSVP session. Thus, the control plane operation for LSP stitching is very similar to that for nesting.

[R-5] PE routers SHOULD support establishment of RSVP-TE LSPs using LSP stitching as per RFC 5150 [39].

7.1.1.2 Multi-area LDP Signaling

RFC 5283 [42] facilitate the establishment of Label Switched Paths (LSPs) that would span multiple IGP areas in a given Autonomous System (AS).

[R-6] PE routers SHOULD support establishment of inter-area LSPs using LDP as per RFC 5283 [42].

7.2 Routing

[R-7] One or both of the following methods MUST be supported by PE and P routers:

- Static routing
- Dynamic routing

[R-8] 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 [11])
- IS-IS (RFC 1195 [9])

[R-9] 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 [19])
- IS-IS-TE (RFC 5305 [44])

8 OAM

OAM in Carrier Ethernet Networks was developed to provide fault management and performance monitoring tools for network links and end-to-end EVCs.

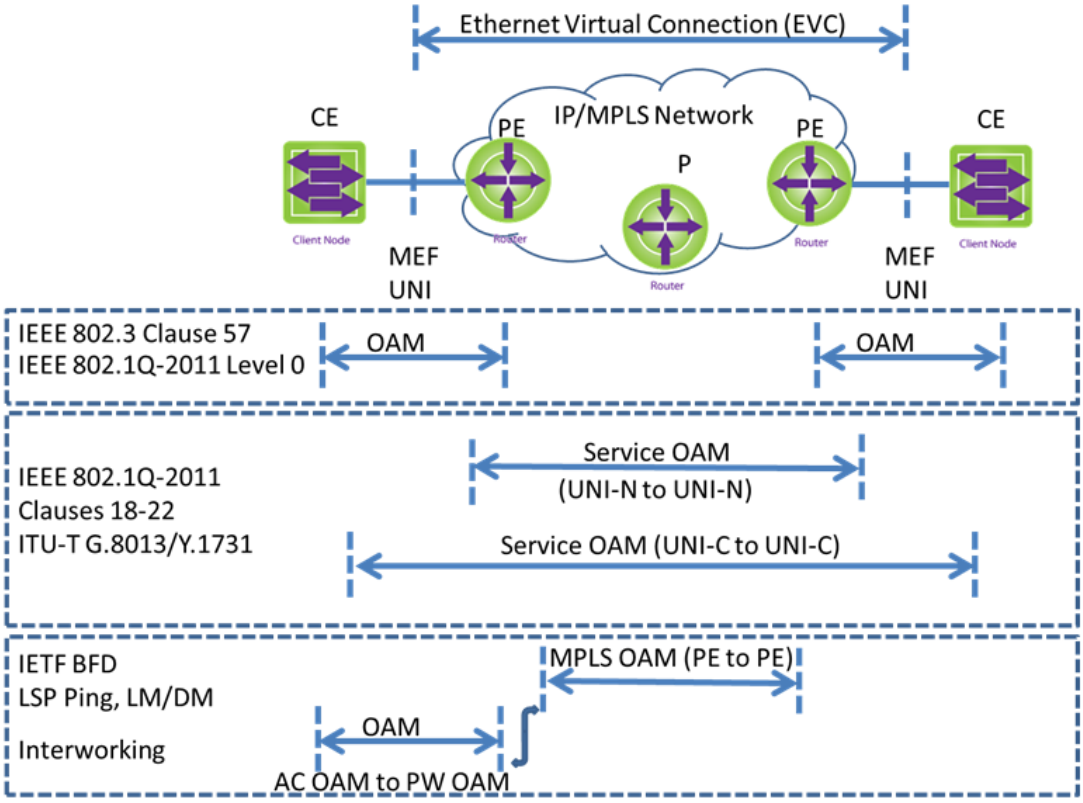

Figure 6 - Components of OAM

8.1 Ethernet OAM

8.1.1 Link OAM

The PE supports Ethernet Link OAM, when the user is directly connected to the network demarcation point. Link OAM provides OAM functions for network access segments (UNI-C to UNI-N). Link OAM provides for Ethernet Link Fault Detection, Monitoring and Loopback for access links.

[R-10] PE MUST support link OAM Active mode as per clause 57.2.9.1 of IEEE 802.3 [8].

[R-11] The PE MUST support initiating OAM Discovery process as per subclause 57.3.2.1 of IEEE 802.3 [8].

[R-12] The PE MUST support sending informational OAM Protocol Data Units (OAMPDU) as per subclause 57.2.10 of IEEE 802.3 [8].

[R-13] The PE MUST support sending Event Notification OAMPDUs as per subclause 57.2.10 of IEEE 802.3 [8].
[R-14] The PE MUST support sending loopback control OAMPDUs as per subclause 5.2.11 of IEEE 802.3 [8].
[R-15] The PE MAY support sending Organization specific OAMPDU per subclause 57 of IEEE 802.3 [8].
[R-16] The PE MAY support sending Variable Request OAMPDUs as per subclause 57.4.3.3 of IEEE 802.3 [8].

8.1.2 MEF Service OAM

The Carrier Ethernet Services are provided between one User Network Interface (UNI) to one or more UNI. A network operator must be able to manage the services using Service OAM (SOAM). The network operator's service OAM is originated at the PE UNI-N.

[R-17] The PE MUST support sending and receiving SOAM frames at the EVC SOAM level 4 as described in MEF 30 [72]. OAM frames are sent as user data and carried transparently.
[R-18] OAM frames, sent at SOAM levels 5, 6, or 7, as described in MEF 30 [72], are sent as user data and MUST be carried transparently.
[R-19] The PE MAY support sending and receiving SOAM frames across the UNI at the UNI SOAM level 1, as described in MEF 30 [72].

See section 11.4.8 for information on performance monitoring.

8.1.3 TR101/TR-178 OAM

The reference architecture in Figure 1 supports two modes of attachment circuits (AC). The AC is a physical connection between CE and PE.

In case of TR-145 [2]/TR-178 [3] Multi-Service networks, the AC can be either Ethernet UNI or non-UNI (coming from Ethernet network). In case of non-UNI attachment circuit, the network operator's OAM is originated at the native service processing (NSP) function of the PE.

Requirement [R-17] and [R-18] are applicable to the PE.

8.2 MPLS OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels and pseudowires used to support Ethernet services. OAM is an important and fundamental functionality in an MPLS network. 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, are used for fault-management, performance-monitoring, and by protection-switching applications.

8.2.1 LSP OAM

This section describes techniques to perform OAM for the underlying MPLS LSPs used in a L2VPN application for carrying PWs.

LSP-Ping RFC 4379 [28] and Bidirectional Forwarding Detection (BFD) RFC 5880 [47] are OAM mechanisms for MPLS LSPs. Further it is desirable that the OAM traffic is sent in-band in an LSP. The following OAM mechanisms are supported:

[R-20] The PE SHOULD support GAL and G-ACH per LSP, as per RFC 5586 [45].

Note: Both VPWS and VPLS protocols used for MEF services use PWs. When PWs are used, OAM is always sent in-band in an LSP.

8.2.1.1 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.

[R-21] PE and P routers MUST support BFD for MPLS LSPs as per RFC 5884 [50].

8.2.1.2 Detecting MPLS Data Plane Failures

LSP Ping is 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.

[R-22] PE and P routers MUST support “ping” mode as per RFC 4379 [28].

RFC 6424 [59] enhances the Mechanism for performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels and when LSP stitching [RFC5150] is in use.

[R-23] PE and P routers MUST support enhanced MPLS Ping and Traceroute as per RFC 6424 [59].

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.

[R-24] PE and P routers SHOULD support “traceroute” mode as per RFC 4379 [28].

The LSP Ping Reply modes as defined in Section 3/RFC 4379 [28] apply as shown in Table 1.

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 1 - LSP Ping Reply Modes

[R-25] The following subsections of Section 3.2/RFC 4379 [28] concerning Target FEC Stack apply as follows:

- When LDP is supported - LDP IPv4 prefix as defined in Section 3.2.1/RFC 4379 [28] MUST be supported.
- When RSVP is supported - RSVP IPv4 LSP as defined in Section 3.2.3/RFC 4379 [28] MUST be supported.
- When BGP is supported - BGP labeled IPv4 prefix as defined in Section 3.2.11/RFC 4379 [28] MUST be supported.
- When L3VPNv4 is supported - VPN IPv4 prefix as defined in Section 3.2.5/RFC 4379 [28] MUST be supported.
- When LDP is supported - LDP IPv6 prefix as defined in Section 3.2.2/RFC 4379 [28] SHOULD be supported.
- When RSVP is supported - RSVP IPv6 LSP as defined in Section 3.2.4/RFC 4379 [28] SHOULD be supported.
- When BGP is supported - BGP labeled IPv6 prefix as defined in Section 3.2.12/RFC 4379 [28] SHOULD be supported.
- When L3VPNv6 is supported - VPN IPv6 prefix as defined in Section 3.2.6/RFC 4379 [28] MUST be supported.

8.2.2 Native service OAM

[R-26] The PE MUST transparently transfer received native service OAM indications over the PW as defined in Section 1 and 4.1 RFC 7023 [63].

[R-27] Defects SHOULD be handled as follows:

- AC failure
  - AC receive defect state entry and exit criteria as per Section 5.1/ RFC 7023 [63].
  - AC transmit defect state Entry/exit criteria as per Section 5.2/ RFC 7023 [63].
  - AC receive defect Consequence action as per Section 6.5 and 6.6/ RFC 7023 [63].
  - AC transmit defect Consequence action as per Section 6.7 and 6.8/ RFC 7023 [63].
- PW failure
  - PW receive defect state entry and exit criteria as per Section 4.4.1/ RFC 7023 [63].
  - PW transmit defect state Entry/exit criteria as per Section 4.4.2/ RFC 7023 [63].
  - PW receive defect entry/exit procedure as per Section 6.1 and 6.2/ RFC 7023 [63].
  - PW transmit defect entry/exit procedure as per Section 6.3 and 6.4/ RFC 7023 [63].

8.2.3 PW OAM

8.2.3.1 Single Segment Pseudowire (SS-PW) OAM

[R-28] The VCCV Control Channel (CC) Type per RFC 5085 [38] 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.

[R-29] 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 [52] respectively. Please note that RFC 5994 [52] refers to RFC 5885 [51] for detailed description and usage of Connection Verification (CV) types.

[R-30] 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 RFC 6478 [60] MAY be used.

Note: As per RFC 6478 [60], VCCV status notification and Static PW status signaling cannot be used at the same time.

[R-31] When LDP is supported for PW establishment, fault notification MUST be supported per RFC 6310 [56] by PE routers.

[R-32] MPLS LSP Ping (CV type 0x02) SHOULD be supported per RFC 5085 [38].

8.2.3.2 Multi-Segment Pseudowire (MS-PW) OAM

8.2.3.2.1 VCCV Control Channel Types

[R-33] VCCV control channels types are supported per section 8.2.3.1 above. For additional tools addressing S-PEs, VCCV channels types MUST be supported per RFC 6073 [54].

8.2.3.2.2 VCCV-BFD

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

8.2.3.2.3 VCCV Connectivity Verification (Ping) and VCCV Path Verification & Path Trace (Traceroute)

If MS-PW is supported, the following requirements apply in addition to section 8.2.3.1:

[R-34] End-to-end MS-PW connectivity verification SHOULD be supported per Section 9.6/RFC 6073 [54].

[R-35] Partial MS-PW connectivity verification SHOULD be supported per Section 9.6/RFC 6073 [54].

[R-36] Pseudowire Switching Point PE sub-TLV Type SHOULD be supported as per RFC 6073 [54].

[R-37] The S-PE MUST support including the FEC 129 of the last PW segment in the Pseudowire Switching Point PE sub-TLV as per the FEC 129 encoding in Section 7.4.1/RFC6073 [54] when LDP FEC 129 is used to signal the PW.

[R-38] The S-PE MUST support including FEC 129 in the Target FEC stack TLV in the VCCV echo reply message as per the FEC 129 encoding in Section 3.2.10/RFC 4379 [28].

[R-39] MS-PW Path Verification MAY be supported as per Section 9.6/RFC 6073 [54], to verify the path of the MS-PW against the actual data path of the MS-PW.

[R-40] MS-PW Path Trace MAY be supported as per Section 9.6/RFC 6073 [54]. 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 defined in RFC 4379 [28] 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.

8.2.4 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.

[R-41] PE and P routers SHOULD support loss and delay measurement per RFC 6374 [57].

8.2.5 Service Activation Testing

Customer service-level agreements (SLAs) dictate certain performance criteria that must be met. ITU-T's Y.1564 [66] Recommendation outlines the out of service tests that can be used to measure and prove performance criteria for carrier Ethernet networks, and provides test methodologies to validate the service configuration and evaluate the service performance to an SLA.

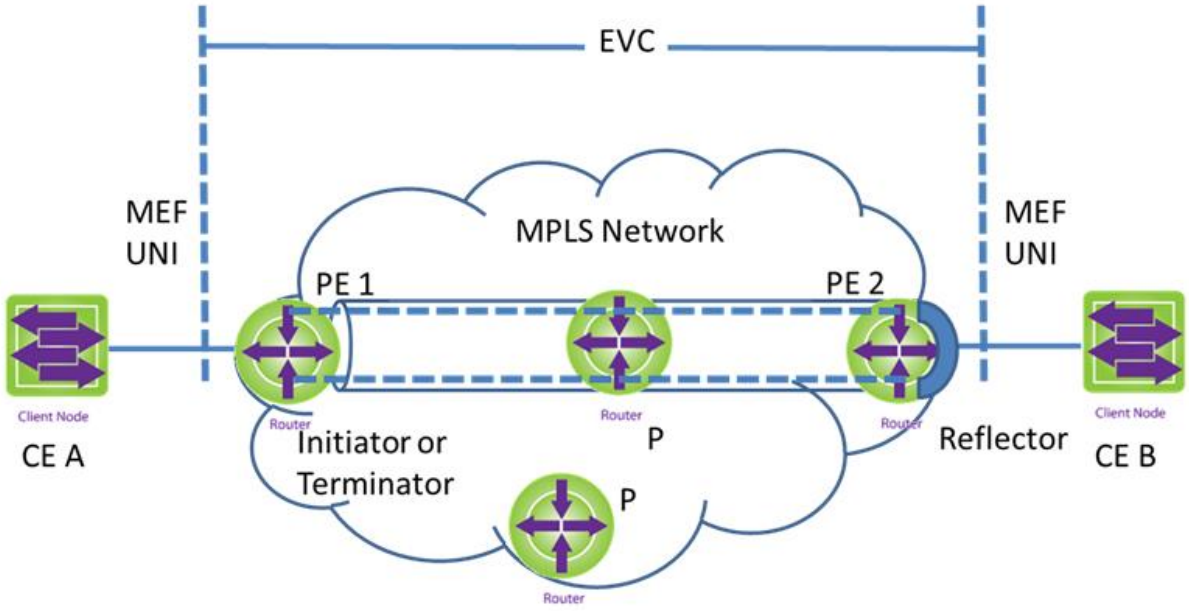

Figure 7 – Example of service activation testing for E-Line service

The PE routers at the ingress and egress will be configured either as an Initiator and Terminator or as a Reflector. The Initiator and Terminator function validates the service configuration (CIR, EIR, CBS, EBS) and measures the service performance (Information Rate (Throughput), FD, IFDV and FLR). The Reflector will receive the test traffic from the Initiator and send it back to the Terminator for analysis. The PE routers could both be configured as Initiator and Terminator to provide one-way measurement.

Unicast test packet (Destination MAC is unicast MAC) originates from initiator device (PE 1) simulating traffic from CE A, destined to CE B. The Reflector (PE 2) receives and reflects back the test packet on behalf of CE B. The reflector functionality (loopback, MAC address swapping) should be implemented in the data path.

The test packet would be simple UDP/IP packet and Source Mac address as MAC A and Destination Mac address as MAC B.

[R-42] The PE SHOULD support ITU-T's Y.1564 [66] configuration for testing 2 UNIs of EVC (EPL, and EVPL).

[R-43] The PE SHOULD support ITU-T's Y.1564 [66] test for testing UNIs of EVC (EP-LAN, and EVP-LAN), one test session between 2 UNIs at a time.

[R-44] The PE SHOULD support the testing packets of ITU-T's Y.1564 [66] be user-configurable with uni-cast untagged, or tagged with user-configurable VLAN ID and priority.

[R-45] The PE SHOULD support ITU-T's Y.1564 [66] generator traffics subject to same traffics classifier and policer/shaper as ingress customer traffics from UNI port.

[R-46] The PE SHOULD support ITU-T's Y.1564 [66] generator or reflector is configured to each individual EVC, even though the EVC shares UNI port with other services (such as EVPL).

9 QoS

The MPLS network supporting the carrier Ethernet services 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 MPLS network will support guaranteeing sufficient bandwidth is available to support new and existing carrier Ethernet connections conforming to all SLA metrics including protection mechanisms.

The following capabilities are to be supported by the PEs:

[R-47] 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" [70].

[R-48] The PE SHOULD support Connection Admission Control to guarantee sufficient bandwidth is available to support new connection conforming to all SLA metrics defined in MEF10.2 [69].

Section 4.7/ RFC 4448 [32] specifies the QoS considerations.

[R-49] The ingress PE MUST map the PCP (in the PRI field of the 802.1Q VLAN tag [7]) into TC field of the MPLS label stack.

9.1 Tunnel CoS mapping and marking

Two types of LSPs are defined in RFC 3270 [14]:

[R-50] The PE and P routers MUST support E-LSP as per Section 1.2/RFC 3270 [14]: 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).

[R-51] The PE and P routers MAY support L-LSP as per Section 1.3/RFC 3270 [14]: 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.

[R-52] The PE MUST support COS marking in the TC bits of the LSP labels.

[R-53] The PE MUST support the Pipe model as per RFC 3270 [14].

9.2 PW CoS mapping and marking

This section handles various PW types.

[R-54] The PE SHOULD support mapping of PRI field of the 802.1Q [7] VLAN tag to PW label TC bits.
[R-55] For multi-segment PW, the PE MUST support mapping of the 802.1Q [7] VLAN tag to PW label TC bits.
[R-56] The PE SHOULD support marking of the PW label TC bits.
[R-57] For multi-segment PW, the PE MUST support marking of the PW label TC bits.

10 Protection and Restoration

For MPLS networks supporting Ethernet services, 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.

The network must provide a deterministic end-to-end service restoration, and there are two categories of functions that help to achieve this. The first set of functions includes ways to enable detection and location of failure. The second set of functions is appropriate recovery actions needed to reroute and restore services.

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.

Depending on criteria such as provisioning complexity, topology and recovery time, LSP Path protection or local protection may be used to facilitate resiliency.

10.1 Failure Detection

There are various failure detection mechanisms available within the MPLS network. An OAM mechanism such as MPLS BFD (see section 8.2.1 LSP OAM) should be used for LSPs. For example this is particularly important to detect failure of the LSPs. For PWs a mechanism such as BFD-VCCV may be used.

10.2 Scope of resiliency

In this specification “resiliency” means protection switching (LSP or PW protection). 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 [15], 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 link protection is available in addition to IP/MPLS or PW protection, the PE must be able to delay its MPLS 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.

10.3 LSP resiliency

The choice of recovery mechanisms used to restore services often depends on the location and type of failure in the network. In order to achieve sub-second convergence subsequent to a network failure, it is preferred to use local repair techniques and pre-established paths to reroute around the failures. Pre-established paths can be accomplished by static configuration or by using an appropriate signaling protocol.

[R-58] For End to End Tunnel Resiliency the single hop MUST be supported as per RFC 5881 [48].
[R-59] For End to End Tunnel Resiliency the Multi-hop Option MUST be supported as per RFC 5883 [49].

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.

10.3.1 LSP resiliency requirements

[R-60] The PE and P routers MUST support Fast ReRoute (FRR) around link failure or router node failure as per RFC 4090 [24].
[R-61] The PE and P routers MUST support Facility backup function as defined in Section 3.2/RFC 4090 [24].
[R-62] The PE and P routers SHOULD support One to One backup as defined in Section 3.1/RFC 4090 [24].
[R-63] The PE and P routers MUST support loop-free alternate (LFA) for IS-IS, OSPF and LDP as per RFC 5286 [43].
[R-64] The PE and P routers MUST support RSVP-TE graceful restart in Section 9/RFC 3473 [16] as well as graceful restart for the routing protocols upon which RSVP-TE path computation depends.
[R-65] The PE and P routers MUST support LDP graceful restart RFC 3478 [17].
[R-66] To provide for continuous service when router control plane fails, the PE and P routers SHOULD support OSPF graceful restart RFC 3623 [18].

[R-67] To provide for continuous service when router control plane fails, the PE and P routers SHOULD support IS-IS graceful restart RFC 3847 [21].

11 Service Connectivity: E-Line

E-Line service is defined in MEF 6.1 [67] and is based on a Point-to-Point Ethernet Virtual Connection (EVC). An E-Line service type can be used to create broad range of point-to-point services. Both types of attachment circuits as defined in the general reference architecture (See Figure 1 - Reference Architecture), are supported.

Figure 8 below provides an example of a single-MEN implemented using multi-AS MPLS connectivity for point-to-point E-Line service. Service multiplexing may occur at one or both UNIs in the EVC.

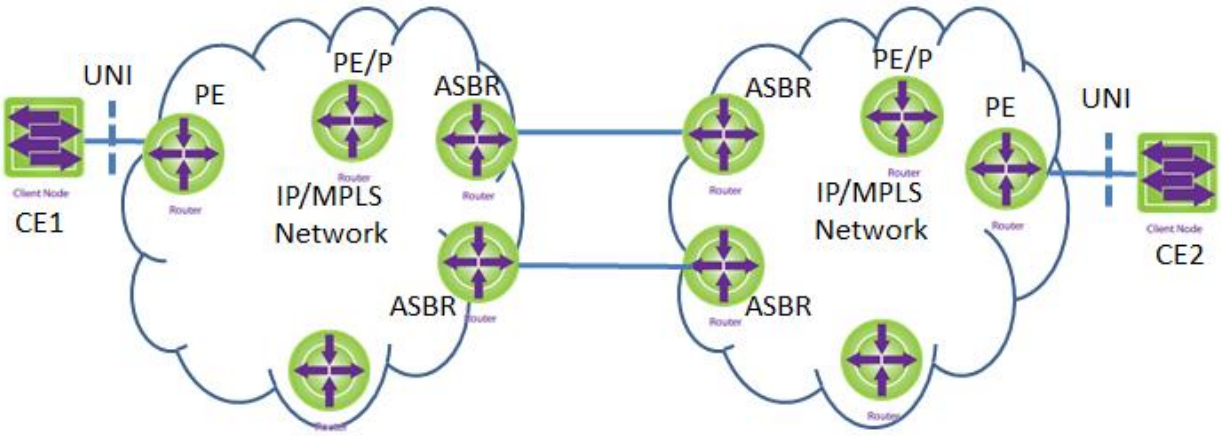

Figure 8 - Inter-AS L2VPNs

11.1 VPWS

The Ethernet Line service is a point to point service type. Virtual Private Wire Service (VPWS) is a layer 2 VPN service used to emulate the E-Line service type in an MPLS network. The pseudowire (PW) is a connection between provider Edge (PE) devices which are connected to the EVC UNIs. This section specifies the use of Ethernet PWs for VPWS to transport the E-Line service type over MPLS.

11.1.1 LSP Signaling and Routing

LSP signaling is supported per Section 7.1.

LSP routing is supported per Section 7.2.

11.1.2 VPWS Setup

[R-68] One or both of the following methods MUST be used for PWs:

- Static provisioning
- Dynamic signaling

Dynamic signaling is used for setup, maintenance and release of VPWS for point to point EVCs. One of the following provisioning and signaling procedures are used for VPWS.

- VPWS signaling with LDP
- BGP auto-discovery and signaling for VPWS-based VPN services

11.1.2.1 VPWS Signaling with LDP

[R-69] PE routers MUST support Single Segment Pseudowire (SS-PWs) as per RFC 3985 [23].

[R-70] PE and P routers SHOULD support static provisioned Multi-Segment Pseudowire (MS-PW) as per RFC 6073 [54].

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

[R-71] MUST support pseudowire setup, maintenance and release of PWs as per RFC 4447 [31] with FEC 128.

[R-72] SHOULD support pseudowire setup, maintenance and release of PWs as per RFC 4447 [31] with FEC 129.

11.1.2.1.1 Multi-AS with LDP and BGP Auto-Discovery

RFC 4364 [27], specifies a number of options for inter-AS operation using a BGP control plane. Section 4/RFC 6074 [55] also specifies Inter-AS operation using BGP for auto-discovery and then using an LDP control plane for PW signaling, using options similar to RFC 4364 [27].

[R-73] The PE implementing LDP signaling for VPWS as per section RFC 4447 [31] SHOULD also support inter- AS auto-discovery operation, per section 4.1/RFC 6074 [55].

NOTE: Section4.1/RFC6074 [55] is similar to RFC 4364 [27] "option (c)".

11.1.2.2 VPWS Signaling with BGP and Auto-Discovery

IP-MPLSF 20.0.0 [6] “BGP auto-discovery and signaling for VPWS-based VPN services”, provides specification for setup of VPWS pseudowires. The specification supports both auto-discovery and signaling.

[R-74] PE routers SHOULD support IP-MPLSF 20.0.0 [6] with encapsulation type values 4 and 5.

Section 10/IP-MPLSF 20.0.0 [6] supports multi-AS operation. If multi-AS operation is required:

[R-75] PE routers SHOULD support multi-AS per section 10.2/IP-MPLSF 20.0.0 [6].

11.1.3 Encapsulation

According to RFC 4448 [32], 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 [32] Sections 4.1 and 4.2.

RFC 4448 [32] also defines two modes of operations of using the 802.1Q [7] 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 [32] that tries to clarify the usage of "service delimiting tags" vs. "not service-delimiting tags". This section assumes the intent that is provided by the errata.

11.1.3.1 RFC 4448 Mapping Operation

Table 2 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 [32]. 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 2 - Raw and Tag Mode Operations for Service Delimiting and Non Service Delimiting Frames

11.1.3.2 Mapping between Ethernet and PWs

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

[R-76] The PE MUST support the Ethernet encapsulation over PW as specified in RFC 4448 [32].
[R-77] The Native Service Processing (NSP) function in a PE MUST support Service Delimiting and Non Service Delimiting functions specified in RFC 4448 [32].

11.1.3.3 Control Word and Frame ordering

Section 4.6/RFC 4448 [32] specifies the use of the control word for PWs.

[R-78] The PE SHOULD support control word.
[R-79] The PE SHOULD support Frame Ordering as per Section 4.6 of RFC 4448 [32].

11.1.4 OAM

This section describes techniques to perform OAM for the underlying MPLS tunnels and pseudowires used to support the Ethernet services.

11.1.4.1 AC OAM

AC OAM requirements as per section 8.2.2.

11.1.4.2 Label Switched Paths (LSPs)

LSP OAM is supported as per section 8.2.1.

11.1.4.3 Pseudowires

PW OAM is supported as per section 8.2.3.

11.1.4.4 Packet Loss and Delay Measurement

Packet loss and delay measurement is supported as per section 8.2.4.

11.1.4.5 MEF Service OAM

MEF service OAM is supported as per section 8.1.2.

11.1.5 QoS

11.1.5.1 Service Activation Testing

The MPLS network supporting carrier Ethernet services 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.

Service activation testing is supported as per section 8.2.5.

11.1.5.1.1 QoS mapping

The QoS mapping as per section 9.

11.1.5.1.2 QoS flexibility

The TC value of one Ethernet PW can be adapted according to the IEEE 802.1Q [7] clause 6.9.3 PCP 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).

11.1.6 Protection and Resiliency

Protection and resiliency is supported as per section 10.

11.1.7 LDP signaled PW redundancy

This section describes requirements to ensure resiliency for VPWS service signaled using LDP signaling. The PWs are set up from the PE nodes, using LDP signaling (RFC4447 [31]) or static methods with status signaling (RFC6478 [60]).

Note: Inter-domain related aspects of PW redundancy are out of scope.
Note: In the PW redundancy section, mechanisms that rely on more than one active path between the PE nodes, e.g., 1+1 protection switching, are also out of the scope.

PW redundancy scenarios in this chapter assume usage of SS-PW. Similar mechanisms apply for MS-PW scenarios, where a set of redundant PWs is configured between T-PE nodes. PE/T-PE nodes indicate the preferred PW to be used for forwarding via the Preferential Forwarding status bit as per RFC6870 [62].

Note: Protection for a PW segment can be provided by the PSN layer, e.g. LFA or FRR. Interaction between the PW redundancy mechanisms and these PSN restoration functions below and/or in the MPLS layer are out-of-scope. Such PSN restoration mechanisms are assumed to react rapidly enough to avoid the triggering of PW redundancy.

From PW redundancy related requirements cover specific network scenarios
The following network scenarios are addressed:

- PW redundancy PW redundancy between the same pair of PEs.
- Single sided Multi-homing with PW redundancy

11.1.7.1 PW redundancy between the same pair of PEs

In such scenarios two PWs are configured between two PE nodes (e.g. PW1: PE1-P1-PE2 and PW2: PE1-P2-PE2). As the PWs are terminated on the same pair of nodes, such a scenario can provide redundancy if the PWs are differently "routed" over the MPLS network. One of the PE nodes (e.g. PE1) acts as a Master Node for selecting the active PW. Figure below illustrates only the case of a SS-PW.

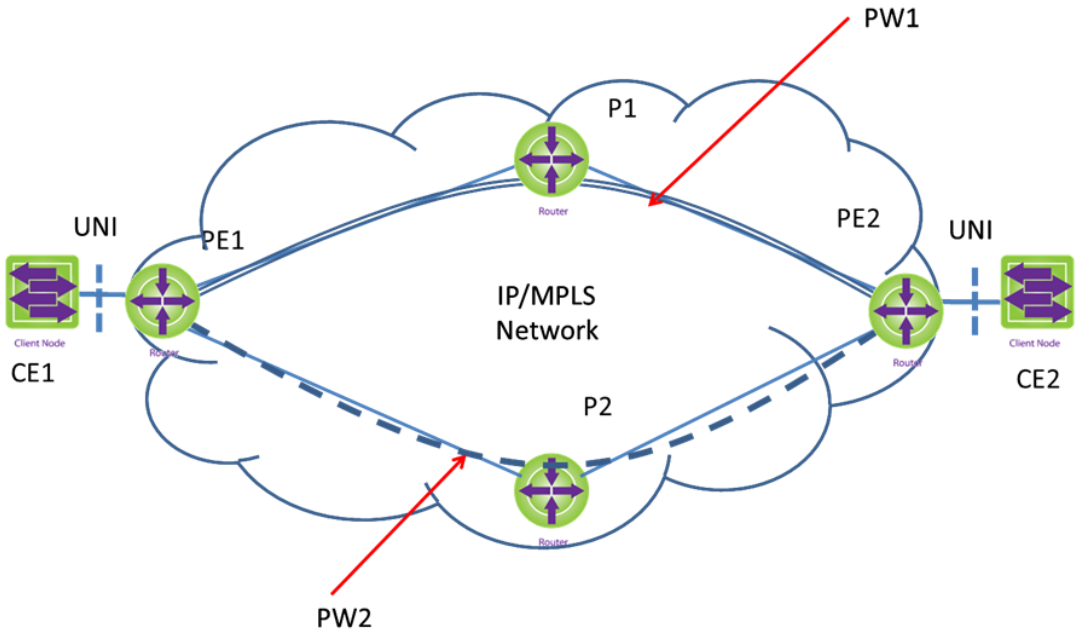

Figure 9 - PW redundancy between the same pair of PEs

[R-80] The PE SHOULD support PW redundancy and signaling procedures in Master/Slave Mode as per RFC 6870 [62].

11.1.7.2 Single sided Multi-homed with PW redundancy

The multi homing provides customer redundant connectivity to network. This scenario protects the emulated service against a failure of one of the PE2 or PE3 or ACs attached to the multi-homed user. The two PWs are configured between the PE nodes (e.g. PW1: PE1-PE2 and PW2: PE1-PE3). The single-homed PE node (PE1) acts as a Master Node for selecting the active PW.

PW redundancy determines which PW to make active based on the forwarding state of the ACs so that only one path is available from CE 1 to CE 2. The PE connected to active PW on multi-homing side will act as the forwarder to CE 2. Other PE on the multi-home side will block the AC for forwarding and receiving. Figure below illustrates only the case of a SS-PW.

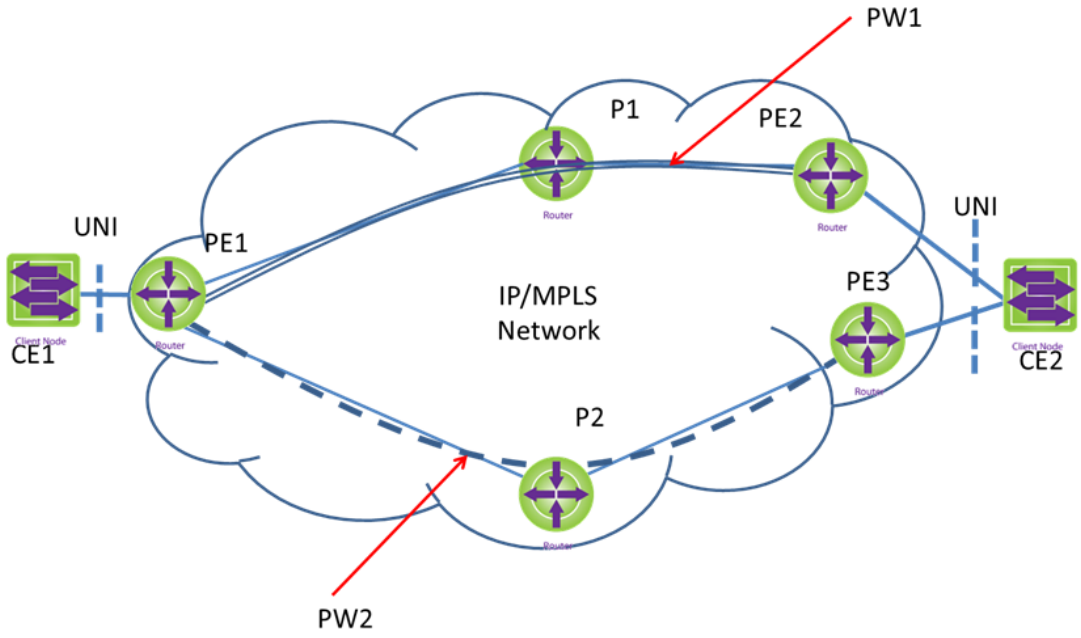

Figure 10 - PW redundancy with single sided Multi-homing

Considering AC status the Master node is able to select which PW to use for forwarding traffic. Depending on the technology used in the MPLS domain signaling of AC status methods differ. In case of LDP RFC4447 applies and in case of static PW RFC 6478.

[R-81] The PE SHOULD support PW redundancy and signaling procedures in Master/Slave Mode as per RFC 6870 [62].

11.1.7.3 Multi-homed on both ingress and egress

It is often required for a Service Provider (SP) to give the customer redundant connectivity to one or more sites, often called "multi-homing". There are several approaches for providing multi-homing such as Spanning Tree Protocol and Ethernet ring protection G.8032 [65].

11.1.8 BGP signaled PW redundancy

BGP signaled PW redundancy and multi homing is for further study.

11.1.9 Redundant ERP to MPLS (VPWS) Connection

See section 12.1.11.1.

11.1.10 Security

[R-82] The PE MUST support the following capabilities for MPLS network security.

- If SS-PW is supported, section 11 of RFC 3916 [22] applies.
- If MS-PW is supported, section 7.1 of RFC 5254 [41] applies.

11.2 Ethernet Private Line (EPL)

Ethernet Private line (EPL), uses a point-to-point EVC between two UNIs to provide a high degree of transparency for service frames between UNIs it interconnect. The service frames, headers, and most Layer 2 protocols are identical at both the source and destination UNI. It does not allow for service multiplexing; that is, a dedicated UNI (physical interface) is used for the EPL. The figure below shows EPL service.

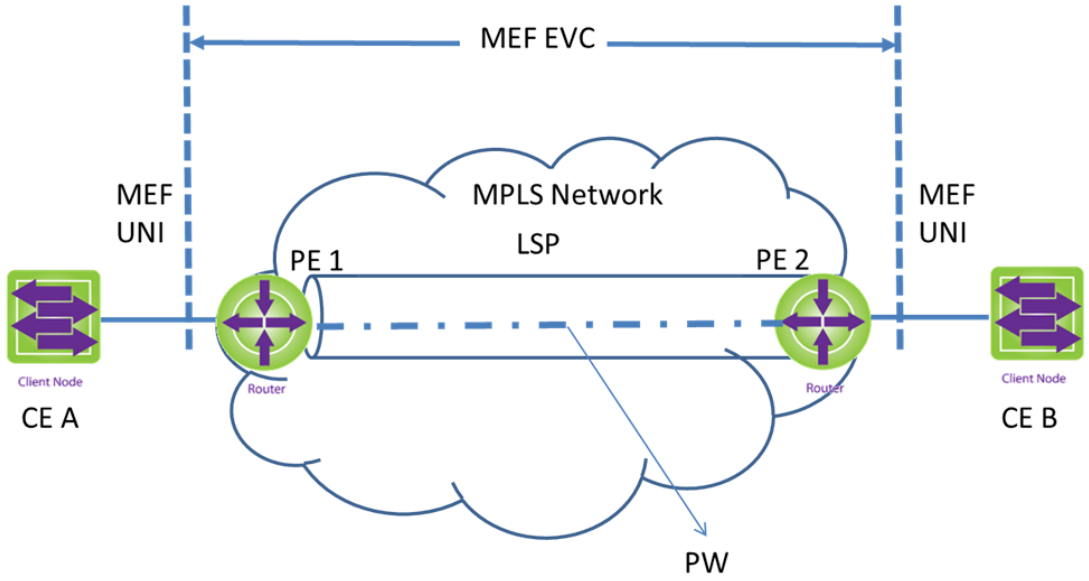

Figure 11 - Ethernet Private Line

Ethernet Private Line (EPL)

- It replaces a TDM Private line
- Dedicated UNIs for Point-to-Point connections
- Single Ethernet Virtual Connection (EVC) per UNI
- The most popular Ethernet service type due to its simplicity

11.2.1 EPL support in MPLS networks

The section 11.1 VPWS specifies support of E-line service type in MPLS networks. The E-line service is defined in section 7.1/MEF 6.1 [67]. Section 11.1.3.1 specifies RFC 4448 [32] mapping operations and section 11.1.3.2 provides the mapping between Ethernet and PWs.

RFC 5603 [46] MIB associates a port to a point-to-point PW. The service delimiting modes of operation are described in section 9/RFC 5603 [46]. One of the modes is port mode which is used for EPL service.

In addition to the mapping between Ethernet and PWs specified in section 11.1.3.2, the following functions are supported for EPL service.

[R-83] The NSP function in a PE MUST map all frames from a specific UNI port to point-to-point PW.
[R-84] The NSP function in a PE MUST support Raw Mode specified in RFC 4448 [32] including the operations specified in Table 2.
[R-85] The NSP function, when supporting non-service delimiting port mode, MUST support No operation by both the egress and ingress PEs.
[R-86] The NSP function MUST support the mode of operations as specified in section 9 (1) A. /RFC 5603 [46] for service delimiting port mode.

Note: Only single class of service per EVC is supported.

11.3 Ethernet Virtual Private Line (EVPL)

Ethernet virtual private line (EVPL), uses a point-to-point EVC between two UNIs, but does not provide full transparency as with the EPL. The EVPL also allows for service multiplexing, which means that more than one EVC can be supported at the UNI. Because service multiplexing is permitted, some service frames may be sent to one EVC, while other service frames may be sent to other EVCs. The service definition for EVPL is specified in section 7.2/MEF 6.1 [67].

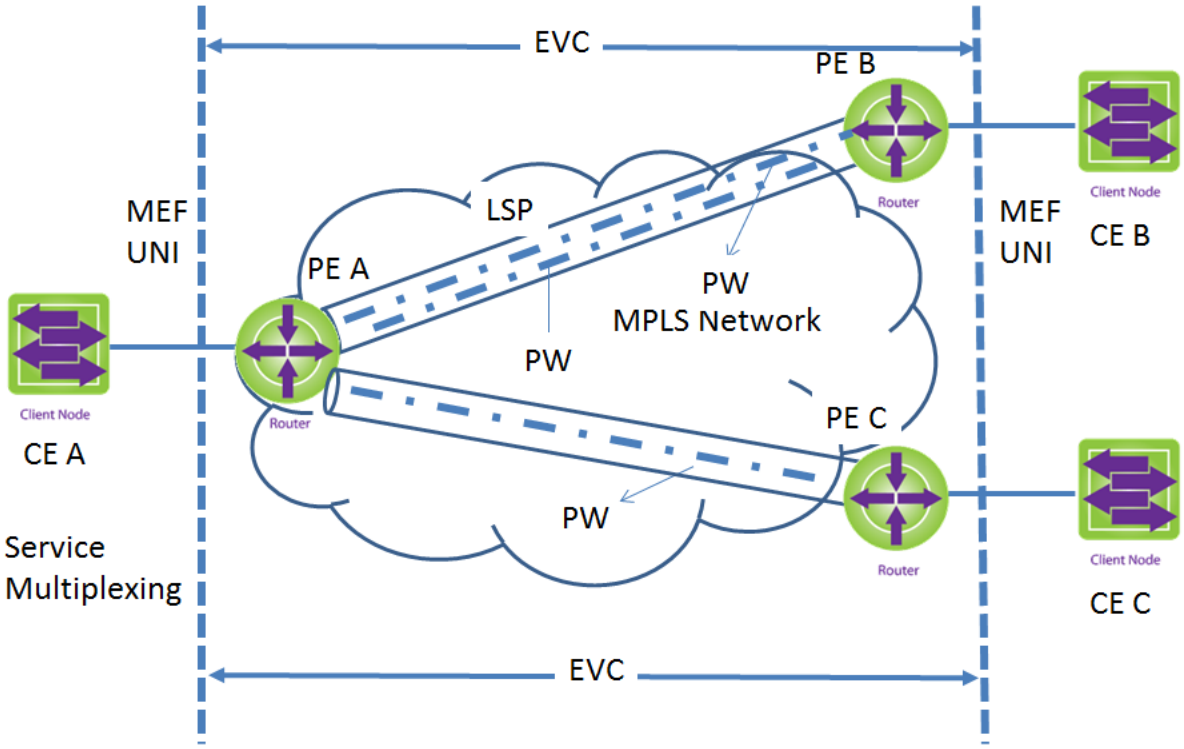

Figure 12 - Ethernet Virtual Private line (EVPL)

- Replaces Frame Relay or ATM services
- Supports Service Multiplexed UNI (i.e. multiple EVCs per UNI)
- Allows single physical connection (UNI) to customer premise equipment for multiple virtual connections

11.3.1 EVPL support in MPLS networks

Section 11.1 VPWS provides support for EVPL service type in MPLS networks. Section 11.1.3.1 specifies RFC 4448 [32] mapping operations and 11.1.3.2 provides the mapping between Ethernet and PWs.

The RFC 5603 [46] MIB supports various options for selecting Ethernet packets into the PW, as defined in RFC4448 [32]. These include VLAN-based PW, and VLAN-manipulated based (change, add, or remove) between the port to be emulated and the PW.

In addition to the mapping between Ethernet and PWs specified in section 11.1.3.2, the following functions are supported for EVPL service.

[R-87] The NSP function in a PE MUST map single VLAN from a specified UNI port to a point-to-point PW.

[R-88] The NSP function in a PE MUST support Tag Mode specified in RFC 4448 [32] including the operations specified in Table 2.

[R-89] The NSP function in a PE MAY support Raw Mode specified in RFC 4448 [32] including the operations specified in Table 2.

[R-90] The NSP function MUST support the mode of operations specified in section 9/RFC 5603 [46] in service delimiting single VLAN mode.

Section 9/RFC 5603 [46] describes the support of point-to-point applications with various VLAN service-delimiting options on the original Ethernet port and the corresponding PW mode and VLAN values. The mode of operations is described in section 9/RFC 5603 [46]. For single VLAN, look at the first VLAN and perform one-to-one bundling. The following options are supported with one-to-one mapping (see section 9/RFC 5603 [46] 2 (a) to 2 (f)):

- with tag preservation
- with VLAN swap
- VLAN removal and the PW label identify the EVC
- Untagged frames passed without modification
- Untagged frames mapped to PW and a VLAN field added
- With s-tag insertion

Note: RFC 5603 [46] supports only one-to-one bundling mode (each c-tag is mapped to a single EVC). Arbitrary bundling (general mapping of C-tags to EVC) mode is not supported.
These PWs can be used to support Label-Only-Inferred-PSC LSPs (L-LSPs) or EXP-Inferred-PSC LSPs (E-LSPs) that are from a single Class of Service (CoS), when mapping of the Ethernet user priority (PRI) bits to the PSN CoS is required. The QoS requirements are specified in section9.

11.4 Support of Service Attributes for EPL and EVPL

MEF 6.1 [67] specifies the UNI service attributes, parameters and values for Ethernet Line service. Section 7.1 and 7.2/MEF6.1 [67] provides service attributes and parameters for EPL and EVPL respectively. Some of the parameters are provided by Ethernet physical interface and service provisioning (e.g., Physical medium, Speed, Mode, MAC layer, EVC type, maximum number of EVCs, etc.). This section describes how other parameters are supported in a PE.

11.4.1 Bandwidth Profile

A bandwidth profile defines how rate enforcement of Ethernet frames is applied at an external interface UNI. Bandwidth profiles enable to offer "sub-rate" service bandwidth, which is bandwidth below the UNI speed and limit the amount of traffic entering their network per the terms of the SLA. It also enables multiple EVCs to be supported on a single UNI by dividing up the interfaces' bandwidth among the multiple EVCs.

For EPL service both ingress and egress bandwidth profiles per UNI are not specified, but per EVC and/or per CoS ingress bandwidth profiles can be specified and are optional.

For EVPL service bandwidth profiles can be specified per UNI (ingress and egress) or ingress EVC. They are optional.

[R-91] Bandwidth profiles, if present, MUST be supported by PEs as per MEF 10.2 [69].

When supporting guaranteed bandwidth, traffic engineered LSPs are used. In addition, PE supports the connection admission control requirement as specified in section9.

11.4.2 Bundling

As per MEF 6.1 [67] Bundling implies "A UNI attribute in which more than one CE-VLAN ID can be associated with an EVC". MEF 6.1 [67] also indicates that All to one bundling implies "A UNI attribute in which all CE-VLAN IDs are associated with a single EVC".

The RFC 5603 [46] MIB supports All to one bundling in case of EPL but do not support bundling in case of EVPL.

For additional details and requirements see sections 11.2.1 and 11.3.1.

11.4.3 CE-VLAN ID preservation for EVC

CE-VLAN ID preservation, defines whether the CE-VLAN ID is preserved (unmodified) across the EVC.

For EPL, the service frames are transported transparently between the UNIs hence the CE-VLAN ID is preserved as per MEF 6.1 [67] table 12.

For EVPL, it depends on VLAN service-delimiting options (see section 11.3.1).

11.4.4 CE-VLAN CoS preservation for EVC

CE-VLAN CoS preservation defines whether the CE-VLAN CoS bits are preserved (unmodified) across the EVC.

For EPL, the service frames are transported transparently between the UNIs hence the CE-VLAN CoS is preserved as per MEF 6.1 [67] table 12.

For EVPL, it depends on VLAN service-delimiting options (see section 11.3.1).

11.4.5 EVC MTU size

EVC MTU size must be lower or equal to the UNI MTU size. It must be at least 1522 bytes in order to support the maximum size of a standard IEEE 802.3 frame with a C-Tag. In some cases the subscriber would require a larger MTU in order to support the delivery of specific applications (for example, FCoE (Fiber Channel over Ethernet) and financial applications). The EVC MTU size is configurable with a default value of 1522 bytes.

When Ethernet frames are transported in MPLS networks, MPLS packet includes the labels, control word and EVC frame as payload. The path MTU is the largest packet size that can traverse

this path without suffering fragmentation. The ingress PE can use Path MTU Discovery to find the actual path MTU.

[R-92] PE MUST support configurable EVC MTU size with at least 1522 bytes.

11.4.6 Frame Delivery

The frame delivery rules enable the service provide to specify how different frame types are to be handled by NSP. They enable setting specific rules for forwarding, discarding or conditionally forwarding specific frame types. There are rules for:

- Unicast Service Delivery
- Multicast Service Delivery
- Broadcast Service Delivery

For an EPL, all three types must be set to Deliver Unconditionally.

[R-93] PE NSP function MUST support setting of specific rules for forwarding, discarding or conditionally forwarding frames (i.e., unicast, multicast and broadcast) per service.

11.4.7 Layer 2 Control Protocols

The layer 2 control protocol processing is independent of the EVC at the UNI. L2CP handling rules are set according to the definition of MEF 6.1.1 [68] section 8 and differ per service type. The PE NSP function supports setting of rules for handling L2CP per service type.

EVC L2CP handling per service type can be set to:

- Discard – Drop the frame.
- Peer can be applicable for the following L2CP LACP/LAMP, Link OAM, Port Authentication, and E-LMI.
- Tunnel – Pass to the egress UNI.

Since most of the L2CP protocols are carried using untagged frames, it is a challenge to tunnel these frames when virtual services are supported.

For Spanning Tree, tunneling xSTP may mean that these frames will not reach all the bridges and thus the service may be affected.

For EPL, the service frames are transported transparently between UNIs it connects.

[R-94] PE NSP function MUST support setting of rules for handing L2CP per service type as specified in section 8 MEF 6.1.1 [68].

11.4.8 EVC Performance

The performance parameters indicate the service quality experienced by the subscriber. They consist of the following:

- Availability
- Delay
- Jitter
- Loss

The requirements for support of CoS and mapping are specified in QoS section9.

[R-95] The PE MUST support MEF SOAM performance monitoring using MEF 35 [73].

OAM frames are sent as user data and carried transparently in the PW.

11.4.9 Multiple Class of Service

A multiple Class of Service (multi-CoS) Ethernet Service is specified in MEF 6.1 [67]. The multi-CoS capabilities of the Ethernet Service can be supported in a network using different approaches. They are:

- Multiple single class EVCs - All traffic in a given EVC be of a single class requiring multiple EVCs to be provisioned across the network to achieve multi-CoS
- Support multi class EVC (a single EVC carrying multiple classes of service) This is achieved by two mechanisms:
    - single EVC with multiple CoS
    - bundling multiple single-class VLANs

11.4.9.1 Ethernet PW

RFC 4448 [32] specifies an Ethernet pseudowire (PW) is used to carry Ethernet/802.3 Protocol Data Units (PDUs) over an MPLS network. There is a one-to-one correspondence between EVC and a PW. The multi class EVC can carry multiple client connections.

In an IP/MPLS network, a specific PW traffic will be treated as a single flow. When an EVC supports multiple CoS, it may contain several sub-flows. When mapping a multi-class EVC to a PW using RFC 4448 [32], the multiple sub-flows are contained inside of a single PW, they will be treated as a single flow, unless additional explicit mapping steps are taken to treat the sub-flows as independent flows.

11.4.9.2 Frame Ordering

In general, applications running over Ethernet do not require strict frame ordering. However, the network must use a mechanism to preserve packet order, if the application supported by Ethernet requires in-order packet delivery (e.g., SNA). There are two mechanisms to accomplish in-order packet delivery: for single class of service per EVC see section 11.4.9.4, for multi-CoS see section 11.4.9.5.

11.4.9.3 PW Control Word

The PW Control Word provides the ability to sequence individual frames on the PW for a single class of service EVC. For both single and multiple class of service EVCs, the PW Control Word is used to suppress ECMP (equal-cost multiple path) when encountered in the network (see RFC 4928 [36]).

[R-96] The PE SHOULD support control word per RFC 4448 Section 4.6.

11.4.9.4 One Class of Service per EVC

RFC 4448 section 4.8 specifies QoS considerations. One class of service per EVC is support as follows: One class of service (CoS) per PW End Service (PWES), mapped to a single CoS PW at the PSN.

[R-97] The PE MUST support one class of service per EVC mapped to a single CoS PW at the PSN per RFC 4448 [32].

[R-98] The PE SHOULD support Frame Ordering per Section 4.6 of RFC 4448 [32].

11.4.9.5 Multi CoS per EVC

Multi CoS per EVC is supported using the following method: Multiple CoS per EVC mapped to a single PW with multiple CoS at the PSN.

[R-99] The PE MUST support multiple CoS per EVC mapped to a single PW with multiple CoS at the PSN per RFC 4448 [32].

Note: In the Multi CoS EVC scenario, PW sequencing should not be used.

For PW CoS mapping see additional requirements in sections 9.1 and 9.2.

11.4.10 Load balancing in MPLS networks

In an IP/MPLS network, a specific PW traffic will be treated as a single flow. The EVC may contain several sub-flows.

As providers scale their networks, they use several techniques to achieve greater bandwidth between nodes. Two widely used techniques are: Link Aggregation Group (LAG) and Equal Cost Multi-Path (ECMP). When load balancing, a packets belonging to a given 'flow' must be mapped to the same port. When the MPLS payload is a PW, an intermediate node has no information on the type of PW being carried in the packet. This limits the forwarder at the intermediate node to only being able to make a choice based on the MPLS label stack.

11.4.10.1 NSP function

The Native Service Processing (NSP) function in a PE that has knowledge of the structure of the Ethernet service and is able to take action on the service.

IETF RFCs 6391 [58] and 6790 [61] provide methods of assigning labels to flows, or flow groups, within pseudowires such that Label Switching Routers can balance flows at a finer granularity than individual pseudowires.

The PE supporting the load balancing in MPLS network, should support one or both of following methods:

[R-100] The PE SHOULD support "Flow Aware transport of PW over MPLS" as per RFC 6391 [58].

[R-101] The PE SHOULD support "Entropy Labels in MPLS" as per RFC 6790 [61].

12 Service Connectivity: Ethernet LAN (E-LAN)

The E-LAN service is an Ethernet service type that is based on a multipoint-to-multipoint EVC. An E-LAN service type can be used to create a broad range of services. Ethernet LAN service is specified in MEF 6.1 [67]. Service multiplexing may occur at none, one, or more than one of the UNIs in an EVC.

12.1 VPLS

In MPLS network, Virtual Private LAN Service (VPLS) is used to support Ethernet LAN service. VPLS offers a Layer 2 Virtual Private Network (L2VPN) providing multipoint Ethernet LAN connectivity.

12.1.1 VPLS Provisioning and Signaling

The VPLS control plane has two primary functions: autodiscovery and signaling.

- Discovery refers to the process of finding all the PE routers that participate in a given VPLS instance. A PE router can be configured with the identities of all the other PE routers in a given VPLS instance, or the PE router can use a protocol to automatically discover the other PE routers. The latter method is called autodiscovery.
- After discovery occurs, each pair of PE routers in a VPLS must be able to establish and tear down pseudowires to each other. This process is known as signaling. Signaling is also used to transmit certain characteristics of the pseudowire that a PE router sets up for a given VPLS.

IETF specifies two specifications for VPLS: RFC 4761 [34] “Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling” and RFC 4762 [35] “Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling”.

12.1.2 BGP Auto-Discovery and Signaling

The BGP-VPLS control plane RFC 4761 [34], defines a means for a PE router to know which remote PE routers are members of a given VPLS (autodiscovery), and for a PE router to know the pseudowire label expected by a given remote PE router for a given VPLS (signaling). The BGP network layer reachability information (NLRI) contains enough information to provide the autodiscovery and signaling functions simultaneously.

Each PE router, a route target is configured for each VPLS. The route target is the same for a particular VPLS across all PE routers and is used to identify the VPLS to which an incoming BGP message pertains.

[R-102] The PE SHOULD support BGP signaling and Auto-Discovery for VPLS RFC 4761 [34].

12.1.2.1 BGP Multi AS VPLS

Section 3.4/RFC 4761 [34] provides specification for multi AS VPLS. Auto-discovery and signaling functions are typically provided via I-BGP. This assumes that all the sites in a VPLS are connected to PEs in a single Autonomous System (AS).

However, sites in a VPLS may connect to PEs in different ASes. In this case there is no I-BGP connection between those PEs, so some means of signaling across ASes is needed.
A similar problem is solved in section 10/RFC 4364 [27]. Three methods are suggested to address issue; all these methods have analogs in multi-AS VPLS. It is recommended to support method (c): Multi-hop EBGP redistribution of VPLS information.

[R-103] The PE implementing BGP signaling for VPLS SHOULD support multi AS, per section 3.4.3/RFC 4761 [34].

12.1.2.2 BGP Multi Homing VPLS

Multi homing is supported as per section 12.1.5.

12.1.3 LDP Signaling and Manual Provisioning

12.1.3.1 LDP VPLS Signaling

RFC 4762 [35] describes the control plane functions of signaling pseudowire labels using Label Distribution Protocol (LDP), extending RFC 4447 [31]. It is agnostic to discovery protocols. The data plane functions of forwarding are also described, focusing in particular on the learning of MAC addresses. The encapsulation of VPLS packets is described by RFC 4448 [32].

[R-104] The PE SHOULD support LDP signaling for VPLS as per RFC 4762 [35].

LDP VPLS defines the hierarchical VPLS (H-VPLS) scheme in which, instead of a PE router being fully meshed with LDP sessions, a two-level hierarchy is created involving hub PE routers and spoke PE routers. The hub PE routers are fully meshed with LDP sessions, whereas the spoke PE router has a pseudowire only to a single hub PE router or to multiple hub PE routers for redundancy.

[R-105] The PE SHOULD support H-VPLS per section 10 of RFC 4762 [35] .

This mode only supports single AS. If multi AS support is required use method described in section 12.1.4.

12.1.4 Auto-discovery for use with LDP VPLS Signaling

RFC 6074 [55] specifies L2VPNs "provisioning models", i.e., models for what information needs to be configured in what entities. It discusses the distribution of these identifiers by the discovery

process, especially when discovery is based on the Border Gateway Protocol (BGP). It then specifies how the endpoint identifiers are carried in the LDP signaling protocol.

[R-106] The PE implementing LDP signaling for VPLS as per section RFC 4762 [35] SHOULD also support BGP Provisioning, Autodiscovery and Signaling in Layer 2 VPN networks as per section 3.2.2/RFC 6074 [55].

12.1.4.1 LDP with Auto-discovery Multi AS VPLS

Section 4/RFC 6074 [55] specifies Inter-AS operation for LDP-VPLS control plane. As in RFC 4364 [27], there are a number of options for inter-AS operation. Option c in section 4.1/ RFC 4364 [27] is the most likely option. It is recommended.

[R-107] The PE implementing LDP signaling for VPLS as per section RFC 4762 [35] SHOULD also support inter AS, per section 4.1/RFC 6074 [55].

12.1.4.2 LDP with Auto-discovery Multi Homing VPLS

Multi homing is supported as per section 12.1.5.

12.1.5 Multi Homing VPLS

Virtual Private LAN Service (VPLS) is a Layer 2 Virtual Private Network (VPN) that gives its customers the appearance that their sites are connected via a Local Area Network (LAN). It is often required for the Service Provider (SP) to give the customer redundant connectivity to some sites, often called "multi-homing".

Extensions for VPLS multi-homing for both BGP and LDP control plane signaling are under development in the IETF.

12.1.6 LSP Signaling

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.

[R-108] PE and P routers supporting MPLS TE and non-TE LSPs MUST support dynamic signaling.

The requirements for dynamic signaling of LSPs per section 7.1 are applicable.

12.1.7 Routing

The requirements for routing per section 7.2 are applicable.

12.1.8 Encapsulation

For VPLS solutions, the encapsulation used is specified in the RFC 4762 [35] (for LDP based solution) and RFC 4761 [34] (for BGP based solution).

RFC 4762 [35] in Sections 7 and 8 specifies the encapsulation.

“While the encapsulation is similar to that described in RFC 4448 [32], the functions of stripping the service-delimiting tag and using a "normalized" Ethernet frame are described in sections 7/ RFC 4762 [35] and 8/ RFC 4762 [35]”.

Section 7/RFC 4762 [35] specifies for Ethernet PW and Section 8//RFC 4762 [35] specifies for Ethernet VLAN PW. RFC 4761 [34] 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.

12.1.8.1 Control Word and Frame Ordering

Section 4.6/RFC 4448 [32] specifies the use of the control word for PWs.

[R-109] The PE SHOULD support control word.

[R-110] The PE SHOULD support Frame Ordering per Section 4.6 of RFC 4448 [32].

12.1.9 OAM

12.1.9.1 AC Native Service OAM

AC native service OAM is supported as per section 8.2.2.

12.1.9.2 Label Switched Paths (LSP) OAM

LSP OAM is supported as per section 8.2.1.

12.1.9.3 Pseudowire (PWs) OAM

PW OAM is supported as per section 8.2.3.

12.1.9.4 Packet Loss and Delay Measurement

LSP packet loss and delay measurement is supported as per section 8.2.4.

12.1.9.5 MEF Service OAM

MEF service is supported as per section 8.1.2.

12.1.10 Service Activation Testing

Service activation testing is supported as per section 8.2.5.

12.1.11 Protection and Resiliency

12.1.11.1 Redundant ERP to MPLS (VPLS) Connection

For L2 services loop free transmission path must be ensured. This loop free characteristic must be ensured also if multiple domains are involved in the service provisioning.

The major challenge for interconnecting domains using different technologies is that they have non-congruent loop avoidance mechanisms:

- Non-MPLS domain: L2 control protocols (e.g. xSTP, ERP, etc.)
- MPLS domain: nothing (in case of VPWS) or split horizon technique (in case of VPLS)

As a consequence of the non-congruent loop avoidance mechanisms the following two concerns exists:

- Ensuring loop-free redundant domain interconnection
- Ensuring topology change propagation between domains

This section focuses on scenario where:

- Non-MPLS domain is ERP based and
- MPLS domain provides VPLS service

ITU-T G.8032 [65] specifies different ERP domain interconnection scenarios. For the redundant interconnection of ERP and MPLS (VPLS) domains the PE have to support ERP as per “Clause 9.7.2 Ring interconnection model without R-APS virtual channel” of G.8032 [65].

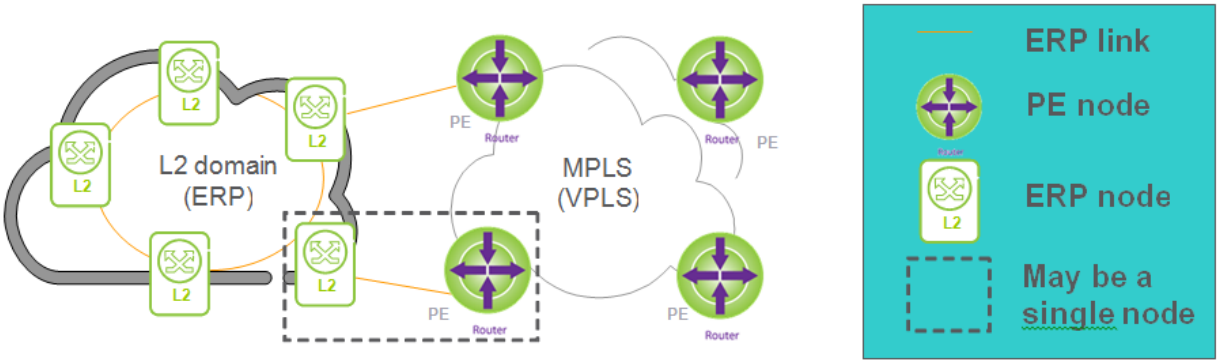

Figure 13 - Example of redundant ERP to MPLS (VPLS) Connection

If an implementation supports ACs in a ring topology, the following requirements apply:

[R-111] PE routers SHOULD support "Ring interconnection model without R-APS virtual channel" as per G.8032 [65] clause 9.7.2.
[R-112] PE routers SHOULD support triggering "MAC-withdraw" message in the MPLS domain for ERP switchover.

12.1.12 QoS and Service Level Agreement

QoS and service level agreement support is provided as per section9.

12.1.13 VPLS 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 [34] and RFC 4762 [35] provide VPLS multicast that relies on ingress replication. This solution has limitations for certain VPLS multicast traffic profiles. For example it may result in highly non-optimal bandwidth utilization in the MPLS network when large amount of multicast traffic is to be transported. The support of multicast tree is optional.

[R-113] Multicast in VPLS as per RFC 7117 [64] SHOULD be supported for Multicast trees in VPLS.

RFC 7117 [64] describes procedures for VPLS multicast that use multicast trees in the Service Provider (SP) network. The procedures described in this document are applicable to both RFC 4761 [34] and RFC 4762 [35].

12.1.14 Security

[R-114] PEs MUST support SS-PW per Section 11/RFC 3916 [22] for MPLS network security.
[R-115] PEs MUST support MS-PW per Section 7.1/RFC 5254 [41] for MPLS network security.
[R-116] PEs MUST support general VPN security per Section 4.5/RFC 3809 [20] and RFC 4111 [25] for VPN security.
[R-117] PEs MUST support L2VPN security per Section 6/RFC 4761 [34] and Section 14/RFC 4762 for VPN security.

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

12.2 Ethernet Private LAN

The Ethernet Private LAN (EP-LAN), uses a multipoint to multipoint EVC. In a multipoint EVC, two or more UNIs must be associated with one another. The EP-LAN service is defined to provide CE-VLAN tag preservation and tunneling of key layer 2 control protocols. A key advantage of

this service is that VLANs can be configured across the sites without any need to coordinate with the service provider.

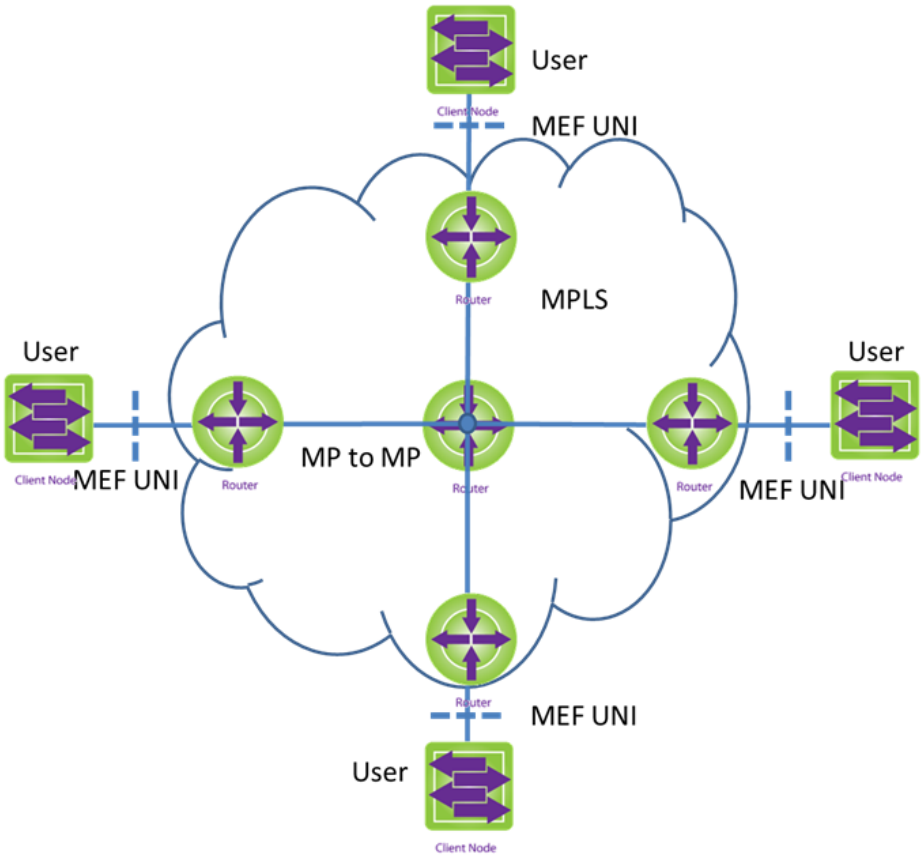

Figure 14 - Ethernet Private LAN (EP-LAN) service

12.2.1 EP-LAN support in MPLS networks

VPLS provides support for E-LAN service type in MPLS networks for requirements see Section 12.1.

12.3 Ethernet Virtual Private LAN

The Ethernet Virtual Private LAN (EVP-LAN) allows service multiplexing at the UNI. It allows users of an E-LAN service type to interconnect their UNIs and at the same time access other services (e.g. E-Line). The figure below shows an example of multiple services access from a single UNI. In this example, the user has an EVP-LAN service for multipoint data connectivity and an EVPL service (blue EVC) for accessing value-add service from one of the UNIs.

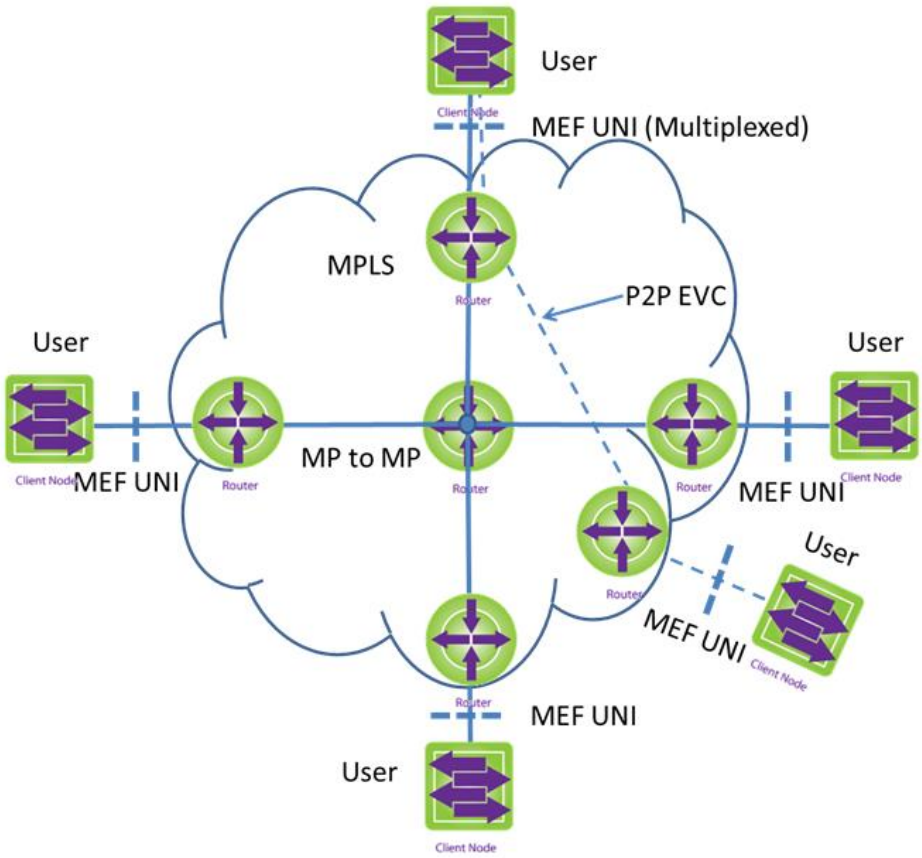

Figure 15 - Ethernet Virtual Private LAN (EVP-LAN) service

12.4 Support of Service Attributes for EP-LAN and EVP-LAN

Section 6.2/MEF 6.1 [67] specifies the E-LAN service type that can be used to create a range of services. Section 7.3 and 7.4/MEF6.1 [67] provides service attributes and parameters for EP-LAN and EVP-LAN respectively. Some of the service attributes and parameters are provided by Ethernet physical interface and service provisioning (e.g., Physical medium, Speed, Mode, MAC layer, EVC type, maximum number of EVCs, etc.). This section describes how other parameters are supported in a PE.

12.4.1 Bandwidth Profile

A bandwidth profile defines how rate enforcement of Ethernet frames is applied at an external interface UNI. Bandwidth profiles enable offering service bandwidth below the UNI access speed (aka Speed) and limit the amount of traffic entering the network per the terms of the SLA.

For LAN services, bandwidth profiles can be optionally specified per UNI (ingress and egress), per EVC (ingress and egress), and/or per CoS (ingress and egress).

[R-118] A PE SHOULD support the bandwidth profile algorithm as per MEF 10.2 [69].

When supporting guaranteed bandwidth, techniques such as traffic engineered LSPs or network engineering are used. In these cases some form of connection admission control must be implemented. In the case of traffic engineered LSPs, connection admission control requirements as specified in section 9 applies.

12.4.2 Bundling

Bundling for both EP-LAN and EVP-LAN services is for further study.

12.4.3 CE-VLAN ID preservation for EVC

CE-VLAN ID preservation, defines whether the CE-VLAN ID is preserved (unmodified) across the EVC.

[R-119] For both EP-LAN and EVP-LAN services the PE MUST support CE-VLAN ID preservation.

12.4.4 CE-VLAN CoS preservation for EVC

CE-VLAN CoS preservation defines whether the CE-VLAN CoS bits are preserved (unmodified) across the EVC.

[R-120] For both EP-LAN and EVP-LAN services the PE MUST support CE-VLAN CoS preservation.

12.4.5 EVC MTU size

EVC MTU size is supported per section 11.4.5.

12.4.6 Frame Delivery

The frame delivery rules enable the service provider to specify how different frame types are to be handled by NSP. They enable setting specific rules for forwarding, discarding or conditionally forwarding specific frame types. The frame types used by the rules are:

- Unicast
- Multicast
- Broadcast

[R-121] PE NSP function MUST support setting of frame delivery rules for forwarding, discarding or conditionally forwarding unicast, multicast and broadcast frames per E-LAN service.

12.4.7 Layer 2 Control Protocols

Layer 2 control protocols are supported per section 11.4.7.

12.4.8 EVC Performance

EVC performance is supported per section 11.4.8.

13 Service Connectivity: Ethernet Tree (E-Tree*)

The Ethernet Tree service type is a point to multipoint ethernet virtual connection. The Ethernet Tree(E-Tree) service type is specified in section 6.3/MEF 6.1 [67]. The service type is used to define Ethernet Private Tree service (EP-Tree) and Ethernet Virtual Private Tree service (EVP-Tree).

At the time of publication of this document, support of MEF E-Tree services over an MPLS network is work in progress in the IETF. In this release of the specification, a subset of point to multipoint E-Tree is supported. The description of the subset, called E-Tree*, is provided in TR-221 [4]. This service type is used for both Ethernet Tree services.

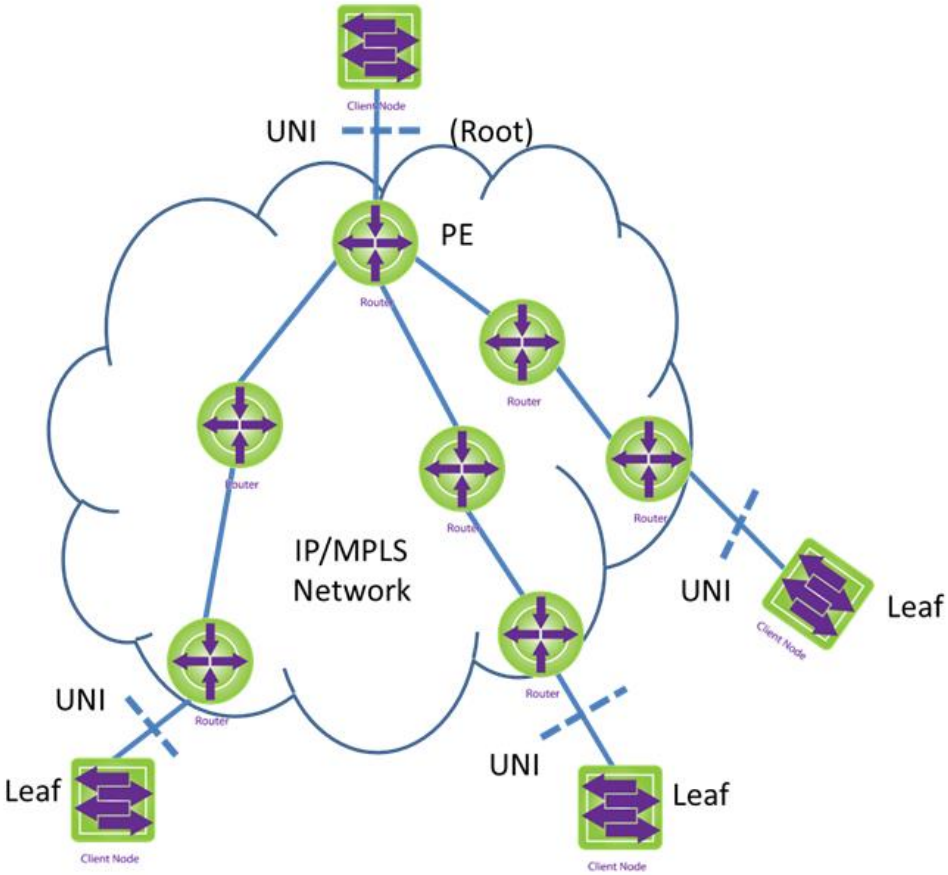

Figure 16 - E-Tree* Service type using point to multipoint EVC

- Provides traffic separation between users with traffic from one “leaf” being allowed to arrive at one “Root” but never being transmitted to other “leaves”.
- Targeted at single-host and where user traffic must be kept invisible to other users.
- Anticipated to be an enabler for mobile backhaul and triple-play infrastructure rather than end-user SLAs.

13.1 VPLS

VPLS (RFC4761 [34], RFC4762 [35]) is a L2VPN service that provides multipoint to multipoint connectivity for Ethernet across an IP or MPLS Network. VPLS emulates the Ethernet Virtual Local Area Network (VLAN) functionality of traditional Ethernet networks. Thus, in VPLS, the customer Ethernet frame is transported over the IP/MPLS from the ingress Provider Edge (PE) to the egress PE where the destination is connected based on the Ethernet frame destination MAC address.

A generic E-LAN/E-Tree service is always bidirectional in the sense that ingress frames can originate at any endpoint in the service.

The only difference between E-LAN and E-Tree is:

- E-LAN has Root endpoints only, which implies there is no communication restriction between endpoints.
- E-Tree has both Root and Leaf endpoints, which implies there is a need to enforce communication restriction between Leaf endpoints.

VPLS treats all attachment circuits (ACs) equal (i.e. not classified into Root or Leaf) and provides any-to-any connectivity among all ACs. VPLS does not include any mechanism of communication restriction between specific ACs, therefore it is insufficient for emulating generic E-Tree service over IP/MPLS.

There are some possible ways to get around this problem that do not require extension to existing VPLS solutions but they all come with significant constraints. One of the approaches specified in TR-224 is E-Tree* which does not require any extensions.

In its simplest form, an E-Tree* Service type can provide a single Root for multiple Leaf UNIs. Each Leaf UNI can exchange data with only the Root UNI.

See TR-221 [4] for details.

13.1.1 Provisioning and Signaling

See section 12.1.1 for provisioning and signaling.

13.1.2 BGP Auto-Discovery and Signaling

BGP auto discovery and signaling are supported as per section 12.1.2.

13.1.3 LDP Signaling and Manual Provisioning

LDP signaling and manual provisioning are supported as per section 12.1.3.

13.1.4 Auto-Discovery for use with LDP VPLS Signaling

Auto-discovery for use with LDP VPLS signaling and requirements are supported as per section 12.1.4.

13.1.5 Multi Homing VPLS

Multi homing VPLS and requirements are supported as per section 12.1.5.

13.1.6 LSP Signaling

LSP signaling and requirements are supported as per section 12.1.6.

13.1.7 Routing

Routing and requirements are supported as per section 12.1.7.

13.1.8 Encapsulation

Routing and requirements are supported as per section 12.1.8.

13.1.9 OAM

OAM and requirements are supported as per section 12.1.9.

13.1.10 Resiliency

Resiliency and requirements are supported as per section 12.1.11.

13.1.11 QoS and Service Level Agreement

QoS and service level agreement and requirements are supported as per section 12.1.12.

13.1.12 VPLS Multicast

VPLS multicast and requirements are supported as per section 12.1.13.

13.1.13 Redundant ERP to MPLS (E-Tree*) Connections

The redundant ERP to E-Tree connections are supported as per section 12.1.11.1.

13.1.14 Security

Security requirements are supported as per section 12.1.14.

13.2 Ethernet Private Tree (EP-Tree*)

The Ethernet private tree service (EP-Tree*) uses a subset of point to multipoint E-Tree service as defined by the MEF. This service type is called E-Tree* (see Figure 16). The PE receives ingress service frames on the attachment circuit connected to root, it replicates and a single copy would be delivered to each leaf UNIs in the EVC. The ingress service frame from a leaf UNI only delivers on the AC attached to route by the hub PE. In this case the hub PE knows which ACs are leaf and which one is root AC.

The EP-Tree* service provide CE-VLAN tag preservation and tunneling of key layer 2 control protocols. A key advantage of this service is that the user can configure VLANs across the sites without any need to coordinate with service provider.

13.2.1 EP-Tree* service support in MPLS networks

VPLS provides support for E-Tree* service type in MPLS networks. For procedures and requirements see section 13.1.

13.3 Ethernet Virtual Private Tree (EVP-Tree*)

The Ethernet Virtual Private Tree (EVP-Tree*) service uses the E-Tree* service type. It allows service multiplexing at the UNI. One or more of the UNIs may also support other services, e.g., EVPL or EVP-LAN.

Bundling may or may not be used on the UNIs in the rooted multipoint EVC. As such, CE-VLAN tag preservation and tunneling of certain layer 2 control protocols may or may not be provided. The Figure 17 below shows the EVP-Tree* service. In this example, an EVP-LAN service also provided among some UNIs.

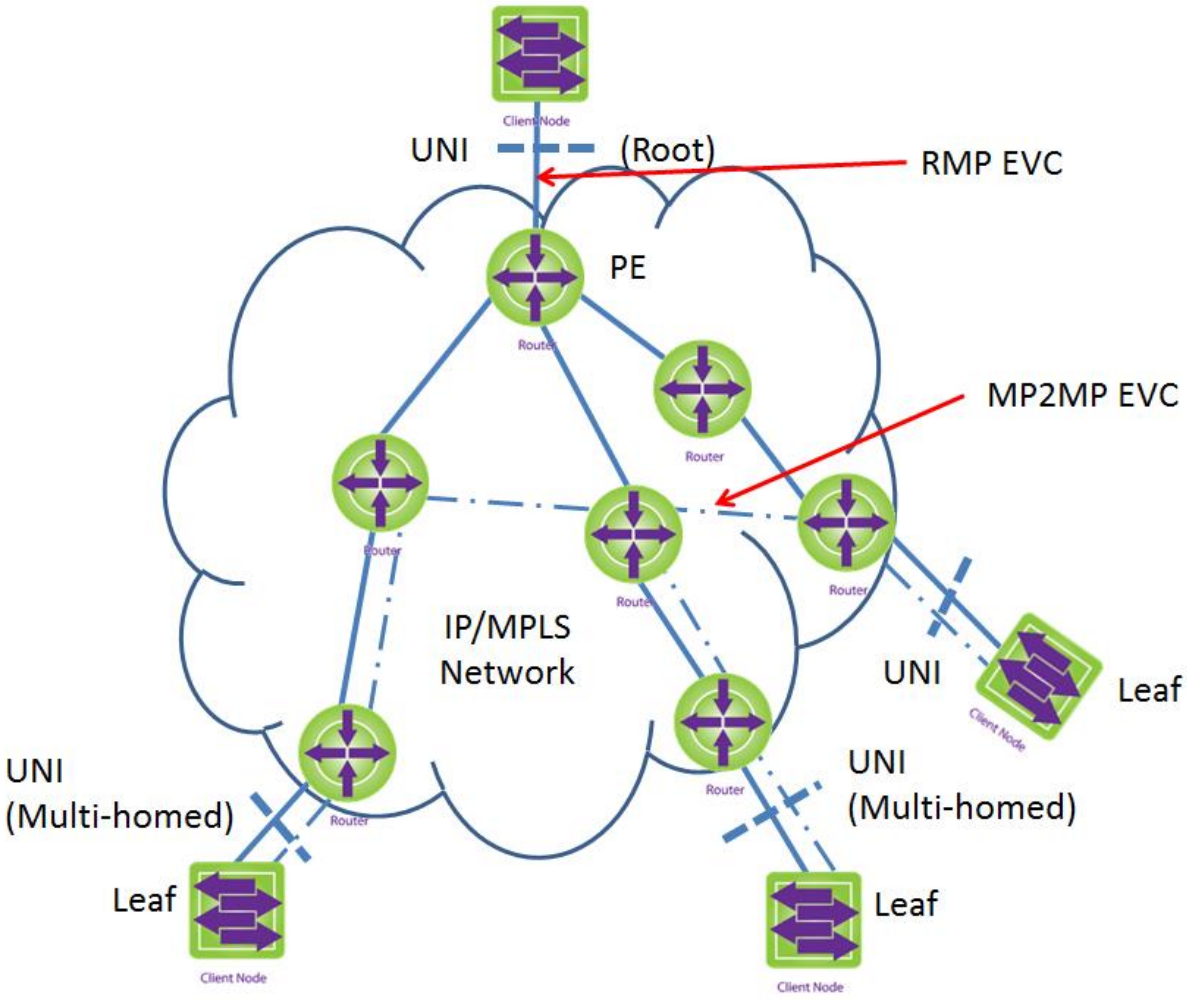

Figure 17 - Ethernet Virtual Private (EVP-Tree*) Service

13.3.1 EVP-Tree* service support in MPLS networks

VPLS provides support for E-Tree* service type in MPLS networks. For procedures and requirements see section 13.1.

Annex A: Seamless MPLS for L2VPN

[NORMATIVE]

Support of Seamless MPLS Architecture is optional. When supported, the requirements in this section are supported.

A.1 Multi Service Broadband Architecture

TR-145 [2] provides reference architectures for multi-service broadband networks, defines high level network requirements. Some of the major motivations for this architecture are:

- Simplification of network architecture: An end-to-end architecture that is a combination of an IP/MPLS and Ethernet.
- Seamless connectivity: Integration of access, aggregation and core networks within a given administrative domain.
- Service independence: support for separation of the client service and transport network.

Section 6.4 of TR-145 [2] provides the distribution of functions onto network nodes. Two sections that are relevant to seamless MPLS are:

- MPLS based aggregation in the access node
- MPLS and IP based aggregation in the access node.

In case of MPLS and IP based aggregation in the access node, the TR-101 [1] architecture is collapsed inside one node-type. The upstream nodes have to perform MPLS forwarding, while supporting extensions needed to scale the MPLS dataplane and control plane requirements on the Access Nodes downstream. In this mode of operation only interface supported is only "U" interface. Other interfaces of TR-145 [2] are not needed (see section I.3.2 of TR-145 [2]).

A.2 Seamless MPLS Architecture

Seamless MPLS architecture can be used to extend MPLS networks to integrate access and aggregation networks into a single MPLS domain ("Seamless MPLS"). The Seamless MPLS approach is based on existing and well known protocols. It enables the setup of LSPs and PW over multiple routing areas, building a single MPLS domain. From an organizational and operational point of view it may be desired to define the boundaries of such domains along the pre-existing boundaries between aggregation networks and the core network.

The key elements of this architecture are:

Separation of the service and transport

In traditional network deployments are built with implicit coupling between the network nodes, the underlying transport technology, and the service delivery over the network. Typically, services are provisioned in multiple segments.

With Seamless MPLS, the provisioning of services are end-to-end and minimize the number of provisioning points. It also uses single LSP across the access nodes. The services are running on the top of transport layer.

Scalable Networks

The Seamless MPLS network supports multi domain and hierarchy which enable scaling. By deploying multi-domain, the scaling is limited to smaller domains and is within the state of the art.

A.2.1 Intra-Domain Routing

The intra-domain routing within each of the MPLS domains (i.e. aggregation and core) must use standard IGP protocols like OSPF or ISIS. Each of these domains is small enough there are no scaling issues.

For intra-domain MPLS LSP setup and label distribution use standard protocols like LDP and RSVP.

A.2.2 Inter-Domain Routing

For scalability, the overall MPLS network is decomposed into multiple MPLS domains. The inter domain routing is used to establish routing and forwarding hierarchy.

For inter domain LSP setup and label distribution requirements see section 7.

RFC 3107 [12] defines procedures for having BGP allocate labels for routes between BGP peers. By implementing RFC 3107 [12] at the aggregation point, BGP label allocation eliminates the need for core devices to learn all the prefixes in the access domain as routes are summarized.

[R-122] PE routers supporting Seamless MPLS Architecture, MUST support using BGP-4 for label distribution as per RFC 3107 [12].

A.2.3 L2VPN

The reference architecture for L2VPNs is based on section 4.3.2 of TR-221 [4]. The architecture reference figures for E-Line and E-LAN given below. In TR-221 [4], the access network can support different options. In seamless MPLS Architecture, only MPLS is supported in the access network. There are two use cases for VPLS: one with IGP in the access and other without IGP in the access network.

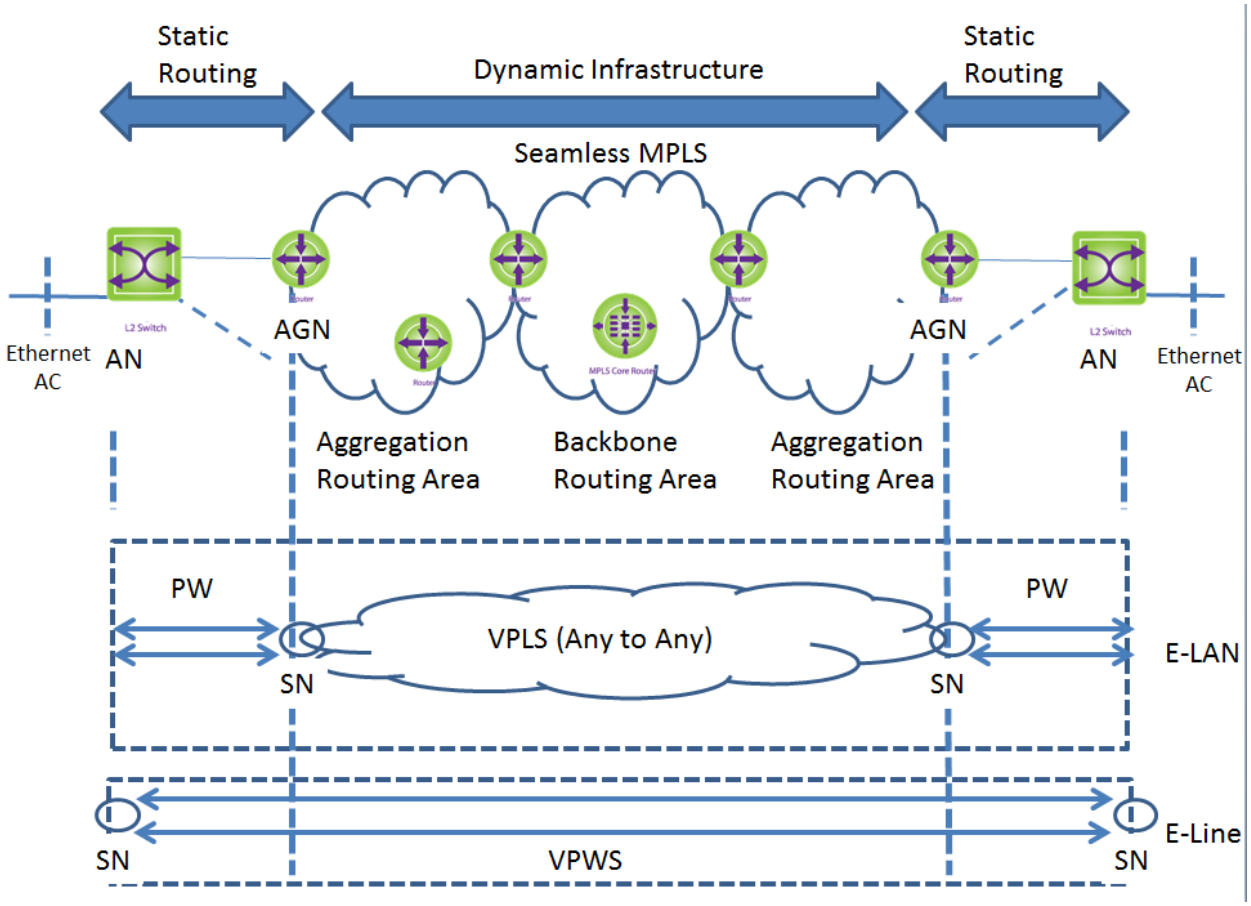

Figure 18 - Reference Architecture of VPLS connectivity with static routing (No IGP) in the access network

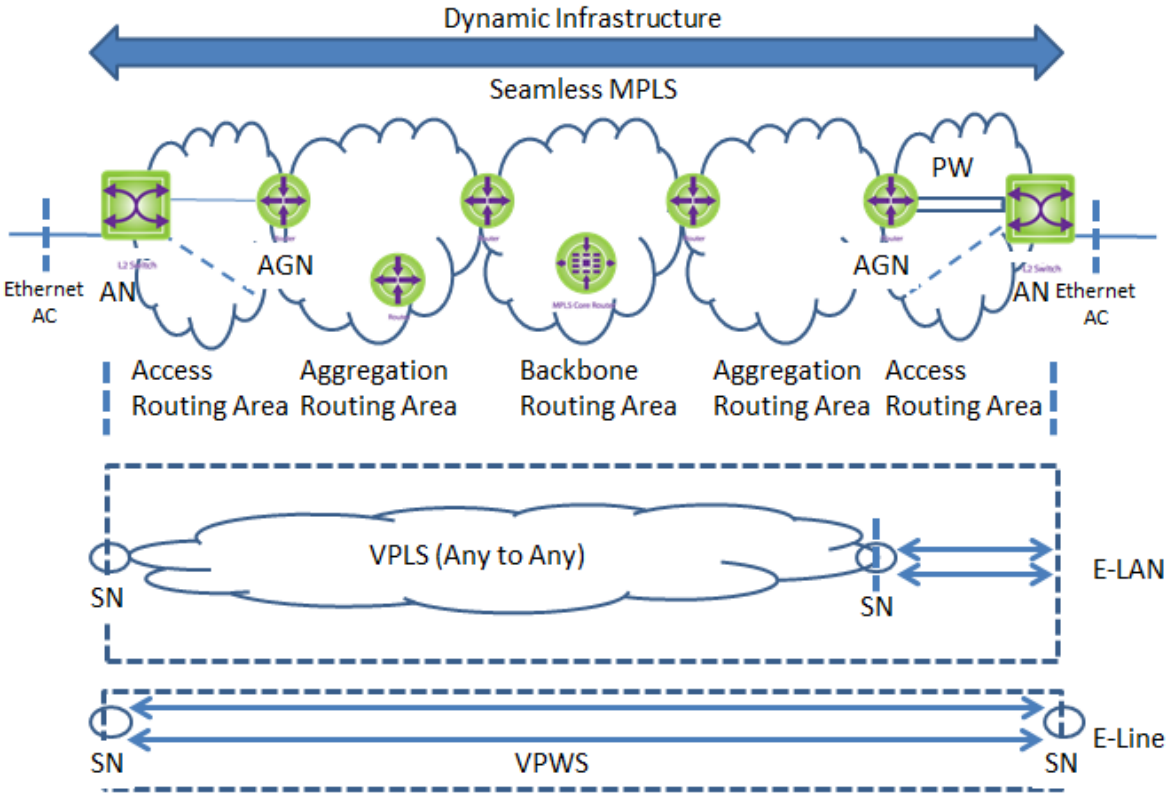

Figure 19 - Reference Architecture of VPLS connectivity with IGP in the access network

A.2.4 Access Node

The access node functionality depends upon mode of architecture supported for VPLS. MPLS functionality in the access node should be kept as simple as possible.

[R-123] PE routers supporting Seamless MPLS architecture, MUST support LDP Downstream on Demand label distribution as per RFC 5036 [37]. The default modes are:

- The default label retention mode is conservative.
- The default label distribution control mode is ordered.

End of Broadband Forum Technical Report TR-224

