Internet-Draft
L2VPN Working Group
Category: Informational

A. Sajassi (Editor)
Cisco

D. Mohan (Editor)

Expires: April 24, 2011
October 24, 2010

L2VPN OAM Requirements and Framework
draft-ietf-l2vpn-oam-req-frmk-11.txt

Status of this Memo

Copyright and License Notice

Contributions published or made publicly available before November

Abstract

This draft provides framework and requirements for Layer 2 Virtual Private Networks (L2VPN) Operation, Administration and Maintenance (OAM). The OAM framework is intended to provide OAM layering across L2VPN services, Pseudo Wires (PWs) and Packet Switched Network (PSN) tunnels. The requirements are intended to identify OAM requirement for L2VPN services (i.e. VPLS, VPWS, and IPLS). Furthermore, if L2VPN services OAM requirements impose specific requirements on PW OAM and/or PSN OAM, those specific PW and/or PSN OAM requirements are also identified.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

When these key words are used in consideration of RFC 2119, these key words are used in capitalized form as indicated above.

Table of Contents

1. Introduction

This draft provides framework and requirements for Layer 2 Virtual Private Networks (L2VPN) Operation, Administration and Maintenance (OAM).

The scope of OAM for any service and/or transport/network infrastructure technologies can be very broad in nature. OSI has defined the following five generic functional areas commonly abbreviated as "FCAPS" [NM-Standards]: a) Fault Management, b) Performance Management, c) Configuration Management, d) Accounting Management, and e) Security Management.

This draft focuses on the Fault and Performance Management aspects. Other functional aspects of FCAPS are for further study.

Fault Management can typically be viewed in terms of the following categories:

- Fault Detection
- Fault Verification
- Fault Isolation
- Fault Notification & Alarm Suppression
- Fault Recovery

Fault Detection deals with mechanism(s) that can detect both hard failures, such as link and device failures, and soft failures, such as software failure, memory corruption, mis-configuration, etc. Typically a lightweight protocol is desirable to detect the fault and thus it would be prudent to verify the fault via Fault

Verification mechanism before taking additional steps in isolating the fault. After verifying that a fault has occurred along the data path, it is important to be able to isolate the fault to the level of a given device or link. Therefore, a Fault Isolation mechanism is needed in Fault Management. Fault Notification mechanism can be used in conjunction with Fault Detection mechanism to notify the devices upstream and downstream to the fault detection point. For example, when there is a client/server relationship between two layered networks, Fault Detection at the server layer may result in the following Fault Notifications:

- sending a forward Fault Notification from server layer to the client layer network(s) using the Fault Notification format appropriate to the client layer
- sending a backward Fault Notification at server layer, if applicable, in the reverse direction
- sending a backward Fault Notification at client layer, if applicable, in the reverse direction

Finally, Fault Recovery deals with recovering from the detected failure by switching to an alternate available data path using alternate devices or links (e.g., device redundancy or link redundancy).

Performance Management deals with mechanism(s) that allow determining and measuring the performance of network/services under consideration. Performance Management can be used to verify the compliance to both the service and network level metric objectives/specifications. Performance Management typically consists of measurement of performance metrics e.g. Frame Loss, Frame Delay, Frame Delay Variation (aka Jitter) etc. across managed entities when the managed entities are in available state. Performance Management is suspended across unavailable managed entities.

[L2VPN-FRWK] specifies three different types of Layer 2 VPN services. These are VPWS, VPLS and IPLS.

This document provides a reference model for OAM as it relates to L2VPN services and their associated Pseudo Wires (PWs) and Public Switched Network (PSN) tunnels. OAM requirement for L2VPN services (e.g. VPLS and VPWS) are also identified. Furthermore, if L2VPN services OAM requirements impose requirements for PW and/or PSN OAM, those specific PW and/or PSN OAM requirements are also identified.

1.1 Relationship with Other OAM Work

This document leverages protocols, mechanisms and concepts defined as part of other OAM work. More specifically:

IEEE Std. 802.1ag-2007 [IEEE 802.1ag] specifies the Ethernet Connectivity Fault Management protocol, which defines the concepts of Maintenance Domains, Maintenance End-Points and Maintenance Intermediate Points. This standard also defines mechanisms and procedures for proactive fault detection (Continuity Check), fault notification (Remote Defect Indication - RDI), fault verification (Loopback) and fault isolation (LinkTrace) in Ethernet networks.

ITU-T Std. Y.1731 [Y.1731] builds upon and extends IEEE 802.1ag in the following areas: it defines fault notification and alarm suppression functions for Ethernet (via Alarm Indication Signal - AIS). It also specifies messages and procedures for Ethernet performance management, including loss, delay, jitter and throughput measurement.

1.2 Terminology

This document introduces and uses the following terms. Further, this document also uses the terms defined in [L2VPN-FRWK] and [L2VPN-TERM].

AIS	Alarm Indication Signal
FM	Fault Management
IPLS	IP-only LAN Service
ME	Maintenance Entity which is defined in a given OAM domain and represents an entity requiring monitoring
MEG	Maintenance Entity Group which represents MEs belonging to the same service instance. MEG is also called as Maintenance Association (MA).
MEP	Maintenance End Point is responsible for origination and termination of OAM frames for a given MEG
MIP	Maintenance Intermediate Point is located between peer MEPs and can process OAM frames but does not initiate or terminate them
OAM Domain	OAM Domain represents a region over which OAM frames can operate unobstructed
PM	Performance Management
RDI	Remote Defect Indication
SLA	Service Level Agreement
STP	Spanning Tree Protocols
VPLS	Virtual Private LAN Service
VPWS	Virtual Private Wire Service

2. L2VPN Services & Networks

As described in [L2VPN-REQ], following Figure 1 shows a L2VPN reference model. L2VPN A represents a point-to-point service while L2VPN B represents a bridged service.

```
 +-----+                                   +-----+
 + CE1 +--+                             +--| CE2 |
 +-----+  |    .....................    |  +-----+
 L2VPN A  |  +-----+            +-----+ |  L2VPN A
          +--| PE |-- Service --| PE |--+
             +-----+  Provider  +-----+
            /  .      Backbone     .  \    --------_
 +-----+   /   .         |         .   \  /        \   +-----+
 + CE4 +--+    .         |         .    +-\ Access  \--| CE5 |
 +-----+       .       +-----+     .      | Network |  +-----+
 L2VPN B       ........| PE |.......       \       /   L2VPN B
                       +-----+  ^           -------
                         |      | logical
                         |      | switching
                      +-----+   | instance
                      | CE3 |
                      +-----+
                      L2VPN B
```

Figure 1: L2VPN Reference Model

[L2VPN-FRWK] specifies VPWS, VPLS and IPLS services. VPWS is a point-to-point service where CEs are presented with point-to-point virtual circuits. VPLS is a bridged LAN service provided to a set of CEs that are members of a VPN. CEs that are members of the same service instance communicate with each other as if they are connected via a bridged LAN. IPLS is a special VPLS which is used to carry only IP service packets.

[L2VPN-REQ] assumes the availability of runtime monitoring protocols while defining requirements for management interfaces. This draft specifies the requirements and framework for operations, administration and maintenance (OAM) protocols between network devices.

3. L2VPN OAM Framework

3.1. OAM Layering

The point-to-point or bridged LAN functionality is emulated by a network of PEs to which the CEs are connected. This network of PEs can belong to a single network operator or can span across multiple network operators. Furthermore, it can belong to a single service provider or can span across multiple service providers. A service provider is responsible for providing L2VPN services to its customers; whereas, a network operator (aka facility provider) provides the necessary facilities to the service provider(s) in support of their services. A network operator and a service provider can be part of same administrative organization or they can be different administrative organizations.

Different layers involved in realizing L2VPNs include service layer and network layers. Network layers can be iterative. In context of L2VPNs, the service layers consists of VPLS, VPWS (e.g. Ethernet, ATM, FR, HDLC, SONET, etc. point-to-point emulation), and IPLS. Similarly in context of L2VPNs, network layers consist of MPLS/IP networks. The MPLS/IP networks can consist of networks links realized by different technologies e.g. SONET, Ethernet, ATM etc.

Each layer is responsible for its own OAM. This document provides the OAM framework and requirements for L2VPN services and networks.

3.2. OAM Domains

When discussing OAM tools for L2VPNs it is important to provide OAM capabilities and functionality over each domain that a service provider or a network operator is responsible for. For these reasons, it is also important that OAM frames are not allowed to enter/exit other domains. We define an OAM domain as a network region over which OAM frames operate unobstructed as explained below.

At the edge of an OAM domain, filtering constructs should prevent OAM frames from exiting and entering that domain. OAM domains can be nested but not overlapped. In other words, if there is a hierarchy of the OAM domains, the OAM frames of a higher-level domain pass transparently through the lower-level domains but the OAM frames of a lower-level domain get blocked/filtered at the edge of that domain.

In order to facilitate the processing of OAM frames, each OAM domain can be associated with a level at which it operates. Higher level OAM domains can contain lower level OAM domains but the converse is not true. It may be noted that the higher level domain does not necessarily mean a higher numerical value of the level encoding in the OAM frame.

A PE can be part of several OAM domains with each interface belonging to the same or a different OAM domain. A PE shall block outgoing OAM frames and filter out incoming OAM frames whose domain level is lower or same to the one configured on that interface and pass through the OAM frames whose domain level is higher than the one configured on that interface.

Generically, L2VPNs can be viewed as consisting of customer OAM domain, service provider OAM domain, and network operator OAM domain as depicted in Figure 2.

```
    ---                                                  ---
   /   \         ------     -------     -----           /   \
   |   CE--     /      \   /       \   /     \      --CE    |
   \   /   \   /        \ /         \ /       \    /    \   /
    ---     --PE         P           P         PE--      ---
               \        / \         / \       /
                \      /   \       /   \     /
                 ------     -------     -----

                    Customer OAM Domain
       |<--------------------------------------------->|

                 Service Provider OAM Domain
              |<------------------------------>|

                Operator   Operator   Operator
              |<-------->|<--------->|<------->|
                OAM Domain OAM Domain OAM Domain
```

Figure 2: OAM Domains

The OAM Domains can be categorized as:

8 Hierarchical OAM Domains: Hierarchical OAM Domains result from OAM Layering and imply a contractual agreement among the OAM Domain ownerships. In the above example, Customer OAM Domain, Service Provider OAM Domain and Operator OAM Domains are hierarchical.

8 Adjacent OAM Domains: Adjacent OAM Domains are typically independent of each other and do not have any relationship among them. In the above example, the different Operator OAM Domains are independent of each other.

3.3. MEPs and MIPs

Maintenance End Points (MEPs) are responsible for origination and termination of OAM frames. MEPs are located at the edge of their corresponding OAM domains. Maintenance Intermediate Points (MIPs) are located within their corresponding OAM domains and they normally pass OAM frames but never initiate them. Since MEPs are located at the edge of their OAM domains, they are responsible for filtering outbound OAM frames from leaving the OAM domain or inbound OAM frames from entering the OAM domain.

An OAM frame is generally associated with a Maintenance Entity (ME) or a Maintenance Entity Group (MEG), where a MEG consists of a set of MEs associated with the same service instance. A ME is a point-to-point association between a pair of MEPs and represents a monitored entity. For example, in a VPLS service which involves n CEs, all the MEs associated with the VPLS service in the customer

OAM domain (i.e. from CE to CE) can be considered to be part of a VPLS MEG, where the n-point MEG consists of a maximum of n(n-1)/2 MEs. MEPs and MIPs correspond to a PE or more specifically to an interface of a PE. For example, an OAM frame can be said to originate from an ingress PE or more specifically an ingress interface of that PE. A MEP on a PE receives messages from n-1 other MEPs (some of them may reside on the same PE) for a given MEG.

In Hierarchical OAM Domains, a MEP of lower-level OAM domain can correspond to a MIP or a MEP of a higher-level OAM domain. Furthermore, the MIPs of a lower-level OAM domain are always transparent to the higher-level OAM domain (e.g., OAM frames of a higher-level OAM domain are not seen by MIPs of a lower-level OAM domain and get passed through them transparently). Further, the MEs (or MEGs) are hierarchically organized in hierarchical OAM domains. For example, in a VPWS service, the VPWS ME in Customer OAM domain can coincide with the Attachment Circuit (AC) ME, PW ME and another AC ME in Service Provider OAM Domain. Similarly, the PW ME can coincide with different ME in Operator OAM Domains.

3.4. MEP and MIP Identifiers

As mentioned previously, OAM at each layer should be independent of other layers e.g. service layer OAM should be independent of underlying transport layer. MEPs and MIPs at each layer should be identified with layer specific identifiers.

4. OAM Framework for VPLS

Virtual Private LAN Service (VPLS) is used in different contexts. In general, VPLS is used in the following contexts: a) as a bridged LAN service over networks, some of which are MPLS/IP, b) as an MPLS/IP network supporting these bridged LAN services, and c) as (V)LAN emulation.

4.1. VPLS as Service/Network

4.1.1. VPLS as Bridged LAN Service

The most common definition for VPLS is for bridged LAN service over an MPLS/IP network. The service coverage is considered end-to-end from UNI to UNI (or AC to AC) among the CE devices and it provides a virtual LAN service to the attached CEs belonging to that service instance. The reason it is called bridged LAN service is because the VPLS-capable PE providing this end-to-end virtual LAN service is performing bridging functions (either full or a subset) as described in the [L2VPN-FRWK]. This VPLS definition, as specified in [L2VPN-

REQ], includes both bridge module and LAN emulation module (as specified in [L2VPN-FRWK]).

A VPLS service instance is also analogous to a VLAN provided by IEEE 802.1Q networks since each VLAN provides a Virtual LAN service to its MAC users. Therefore, when a part of the service provider network is Ethernet based (such as H-VPLS with QinQ access network), there is a one-to-one correspondence between a VPLS service instance and its corresponding provider VLAN in the service provider Ethernet network. To check the end-to-end service integrity, the OAM mechanism needs to cover the end-to-end VPLS service as defined in [L2VPN-REQ] which is from AC to AC including bridge module, VPLS forwarder, and the associated PWs for this service. This draft specifies the framework and requirements for such OAM mechanism.

4.1.2. VPLS as a Network

Sometimes VPLS is also used to refer to the underlying network that supports bridged LAN services. This network can be an end-to-end MPLS/IP network as H-VPLS with MPLS/IP access or can be a hybrid network consisting of MPLS/IP core and Ethernet access network as in H-VPLS with QinQ access. In either case, the network consists of a set of VPLS-capable PE devices capable of performing bridging functions (either full or a subset). These VPLS-capable PE devices can be arranged in a certain topology such as hierarchical topology (H-VPLS) or distributed topology (D-VPLS) or some other topologies such as multi-tier or star topologies. To check the network integrity regardless of the network topology, network-level OAM mechanisms (such as OAM for MPLS/IP networks) are needed. The discussion of network-level OAM is outside of the scope of this draft.

4.1.3. VPLS as (V)LAN Emulation

Sometimes VPLS also refers to (V)LAN emulation. In such context, VPLS only refers to the full mesh of PWs with split horizon that emulates a LAN segment over MPLS/IP network for a given service instance and its associated VPLS forwarder. Since the emulated LAN segment is presented as a Virtual LAN (VLAN) to the bridge module of a VPLS-capable PE, the emulated segment is also referred to as an emulated VLAN. The OAM mechanisms in this context refer primarily to integrity check of VPLS forwarders and its associated full-mesh of PWs and the ability to detect and notify a partial mesh failure. This draft also covers the OAM framework and requirements for such OAM mechanism.

4.2. VPLS OAM

When discussing the OAM mechanisms for VPLS, it is important to consider that the end-to-end service can span across different types of L2VPN networks. As an example, in case of [VPLS-LDP], the access network on one side can be bridged network e.g. [IEEE 802.1ad], as described in section 11 of [VPLS-LDP]. The access network can also be a [IEEE 802.1ah] based bridged network. The access network on other side can be MPLS based as described in section 10 of [VPLS-LDP]; and the core network connecting them can be IP, MPLS, ATM, or SONET. Similarly, the VPLS service instance can span across [VPLS-BGP], and distributed VPLS as described in [L2VPN-SIG].

Therefore, it is important that the OAM mechanisms can be applied to all these network types. Each such network may be associated with a separate administrative domain and also multiple such networks may be associated with a single administrative domain. It is important to ensure that the OAM mechanisms are independent of the underlying transport mechanisms and solely rely on VPLS service, i.e. the transparency of OAM mechanisms must be ensured over underlying transport technologies such as MPLS, IP, etc.

This proposal is aligned with the discussions in other standard bodies and groups such as ITU-T Q.5/13, IEEE 802.1, and MEF which address Ethernet network and service OAM.

4.2.1. VPLS OAM Layering

Figure 3 shows an example of a VPLS service (with two CE belonging to customer A) across a service provider network marked by UPE and NPE devices. More CE devices belonging to the same Customer A can be connected across different customer sites. Service provider network is segmented into core network and two types of access network. Figure 3(A) shows the bridged access network represented by its bridge components marked B, and the MPLS access and core network represented by MPLS components marked P. Figure 3(B) shows the service/network view at the Ethernet MAC layer marked by E.

```
        ---                                                   ---
       /   \         ------      -------      ----           /   \
       | A CE--     /      \    /       \    /    \       --CE A |
       \   /   \   /        \  /         \  /      \     /   \   /
        ---     --UPE       NPE          NPE        UPE--     ---
                   \        /  \         /  \      /
                    \      /    \       /    \    /
                     ------      -------      ----

    (A)    CE----UPE--B--B--NPE---P--P---NPE---P----UPE----CE

    (B)    E------E---E--E---E------------E----------E-----E
```

Figure 3: VPLS specific device view

As shown in Figure 3(B), only the devices with Ethernet functionality are visible to OAM mechanisms operating at Ethernet

MAC layer and the P devices are invisible. Therefore, the OAM along the path of P devices (e.g., between two PEs) is covered by transport layer and it is outside the scope of this document.

However, VPLS services may impose some specific requirements on PSN OAM. This document aims to identify such requirements.

4.2.2. VPLS OAM Domains

As described in the previous section, a VPLS service for a given customer can span across one or more service providers and network operators. Figure 4 depicts three OAM domains: (A) customer domain which is among the CEs of a given customer, (B) service provider domain which is among the edge PEs of the given service provider, and (C) network operator domain which is among the PEs of a given operator.

```
     ---                                                    ---
    /   \         ------      -------      ----          /   \
    |   CE--     /      \    /       \    /    \       --CE   |
    \   /   \   /        \  /         \  /      \     /   \   /
     ---     --UPE       NPE          NPE        UPE--     ---
                \        /  \         /  \      /
                 \      /    \       /    \    /
                  ------      -------      ----

                       Customer OAM Domain
(A)     |<----------------------------------------------->|

                       Provider OAM Domain
(B)            |<---------------------------------->|

                 Operator     Operator     Operator
(C)            |<--------->|<----------->|<-------->|
                 OAM Domain  OAM Domain   OAM Domain
```

Figure 4: VPLS OAM Domains

4.2.3. VPLS MEPs & MIPs

As shown in Figure 5, (C) represents those MEPs and MIPs that are visible within the customer domain. The MIP associated with (C) are expected to be implemented in the bridge module/VPLS forwarder of a PE device, as per the [L2VPN-FRWK]. (D) represents the MEPs and MIPs visible within the service provider domain. These MEPs and MIPs are expected to be implemented in the bridge module/VPLS forwarder of a PE device, as per the [L2VPN-FRWK]. (E) represents the MEPs and MIPs visible within each operator domain where MIPs only exist in an Ethernet access network (e.g., an MPLS access network doesn't have MIPs at the operator level). Further, (F) represents the MEPs and MIPs corresponding to the MPLS layer and may apply MPLS based mechanisms. The MPLS layer shown in Figure 5 is just an example and specific OAM mechanisms are outside the scope of this document.

```
     ---                                                    ---
    /   \         ------      -------      ----           /   \
    | A CE--     /      \    /       \    /    \       --CE A |
    \   /   \   /        \  /         \  /      \     /   \   /
     ---     --UPE       NPE          NPE        UPE--     ---
                \        /  \         /  \      /
                 \      /    \       /    \    /
                  ------      -------      ----

 (A)    CE----UPE--B-----NPE---P------NPE---P----UPE----CE
 (B)    E------E---E------E------------E----------E------E

                         Customer OAM domain
 (C)    MEP---MIP--------------------------------MIP---MEP

                         Provider OAM domain
 (D)          MEP--------MIP-----------MIP-------MEP

                 Operator    Operator     Operator
 (E)          MEP-MIP--MEP|MEP-------MEP|MEP-----MEP
                OAM domain   OAM domain   OAM domain

                              MPLS OAM   MPLS OAM
 (F)                       MEP--MIP--MEP|MEP-MIP-MEP
                               domain     domain
```

Figure 5: VPLS OAM Domains, MEPs & MIPs

4.2.4. VPLS MEP and MIP Identifiers

In VPLS, for Ethernet MAC layer, the MEPs and MIPs should be identified with their Ethernet MAC addresses. As described in [VPLS-LDP], VPLS instance can be identified in an Ethernet domain (e.g., 802.1ad domain) using VLAN tag (service tag) while in an MPLS/IP network, PW-ids are used. Both PW-ids and VLAN tags for a given VPLS instance are associated with a Service Identifier (e.g., VPN identifier). MEPs and MIPs Identifiers, i.e. MEP Ids and MIP Ids, must be unique within their corresponding Service Identifiers within the OAM domains.

For Ethernet services, e.g. VPLS, Ethernet frames are used for OAM frames and the source MAC address of the OAM frames represent the source MEP in that domain. For unicast Ethernet OAM frames, the destination MAC address represents the destination MEP in that domain. For multicast Ethernet OAM frames, the destination MAC addresses corresponds to all MEPs in that domain.

5. OAM Framework for VPWS

Figure 6 shows the VPWS reference model. VPWS is a point-to-point service where CEs are presented with point-to-point virtual circuits. VPWS is realized by combining a pair of Attachment Circuits between the CEs and PEs and a PW between PEs.

```
     |<------------- VPWS1 <AC11,PW1,AC12> ------------>|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC11---|    |.......PW1........|    |--AC12----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
|    |---AC21---|    |.......PW2........|    |--AC22----|    |
+----+          |    |==================|    |          +----+
     |          +----+     PSN Tunnel   +----+          |
     |                                                  |
     |<------------- VPWS2 <AC21,PW2,AC22> ------------>|
```

Figure 6: VPWS Reference Model

5.1. VPWS as Service

VPWS service can be categorized as:
  8 VPWS with homogeneous ACs (where both ACs are same type)
  8 VPWS with heterogeneous ACs (where the ACs are of different
     Layer-2 encapsulation)

Further, the VPWS can itself be classified as:
  8 Homogeneous VPWS (when two ACs and PW are of the same type)
  8 Heterogeneous VPWS (when at least one AC or PW is different
     type than the others)

Based on the above classifications, the heterogeneous VPWS may have either homogeneous or heterogeneous ACs. On the other hand, homogeneous VPWS can have only homogeneous ACs.

5.2. VPWS OAM

When discussing the OAM mechanisms for VPWS, it is important to consider that the end-to-end service can span across different types of networks. As an example, the access network between CE and PE on one side can be Ethernet bridged network, ATM network, etc. In common scenarios, it could simply be a point-to-point interface such as Ethernet PHY. The core network connecting PEs can be IP, MPLS, etc.

Therefore, it is important that the OAM mechanisms can be applied to different network types some of which are mentioned above. Each such network may be associated with a separate administrative domain and also multiple such networks may be associated with a single administrative domain.

5.2.1. VPWS OAM Layering

Figure 7 shows an example of a VPWS service (with two CE devices belonging to customer A) across a service provider network marked by PE devices. Service provider network can be considered to be segmented into a core network and two types of access network.

In the most general case, a PE can be client service aware when it processes client service PDUs and is responsible for encapsulating and de-encapsulating client service PDUs onto PWs and ACs. This is particularly relevant for homogeneous VPWS. The service specific device view for such a deployment is highlighted by Figure 7(A) for these are the devices that are expected to be involved in end-to-end VPWS OAM.

In other instances, a PE can be client service unaware when it does not process native service PDUs but instead encapsulates access technology PDUs over PWs. This may be relevant for VPWS with heterogeneous ACs. For example, if the service is Ethernet VPWS which is offered across an ATM AC, ATM PW and Ethernet AC. In this case, the PE which is attached to ATM AC and ATM PW may be transparent to the client Ethernet service PDUs. On the other hand, the PE which is attached to ATM PW and Ethernet AC is expected to be client Ethernet service aware. The service specific device view for such a deployment is highlighted by Figure 7(B) for these are the devices that are expected to be involved in end-to-end VPWS OAM, where PE1 is expected to be client service unaware.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+

        access             core                 access
     |<---------->|<---------------------->|<------------>|

 (A).CE----------PE----------------------PE-------------CE

 (B).CE-----------------------------------PE-------------CE
```

Figure 7: VPWS specific device view

5.2.2. VPWS OAM Domains

As described in the previous section, a VPWS service for a given customer can span across one or more network operators.

Figure 8a and 8b depicts three OAM domains: (A) customer domain which is among the CEs of a given customer, (B) service provider domain which depends on the management model, and (C) network operator domain which is among the PEs of a given operator and could also be present in the access network if the ACs are provided by a different network operator. The core network operator may be responsible for managing the PSN Tunnel in these examples.

For the first management model, as shown in Figure 8a, the CEs are expected to be managed by the customer and the customer is responsible for running end-to-end service OAM, if needed. The service provider is responsible for monitoring the PW ME and the monitoring of the AC is the shared responsibility of the customer and the service provider. In most simple cases, when the AC is realized across a physical interface that connects the CE to PE, the monitoring requirements across the AC ME are minimal.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+

                     Customer OAM Domain
 (A).|<------------------------------------------------->|

                 Service Provider OAM Domain
 (B)            |<---------------------------->|

                     Operator OAM Domain
 (C)                 |<---------------->|
```

Figure 8a: VPWS OAM Domains - Management Model 1

Figure 8b highlights another management model, where the CEs are managed by the Service Provider and where CEs and PEs are connected via an access network. The access network between the CEs and PEs may or may not be provided by a distinct network operator. In this model, the VPWS service ME spans between the CEs in the Service Provider OAM Domain, as shown by Figure 8b(B). The Service Provider OAM Domain may additionally monitor the AC MEs and PW MEs individually, as shown by Figure 8b(C). The network operators may be responsible for managing the access service MEs (e.g. access tunnels) and core PSN Tunnel MEs, as shown by Figure 8b(D). The distinction between Figure 8b-(C) and 8(b)-D) is that in (C), MEs have MEPs at CEs and at PEs, and have no MIPs. While in (D) MEs have MEPs at CEs and at PEs and furthermore, MIPs may be present in between the MEPs; thereby, providing visibility of the network to the operator.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+

                     Customer OAM Domain
(A) |<-------------------------------------------------->|

                Service Provider (SP) OAM Domain
(B)  |<------------------------------------------------>|

        SP OAM             SP OAM             SP OAM
(C)  |<--------->|<----------------------->|<---------->|
        Domain              Domain             Domain

       Operator            Operator          Operator
(D)  |<--------->|<----------------------->|<---------->|
      OAM Domain          OAM Domain         OAM Domain
```

Figure 8b: VPWS OAM Domains - Management Model 2

Note: It may be noted that unlike VPLS OAM Domain in Figure 4, where multiple operator domains may occur between the U-PE devices, VPWS OAM domain in Figure 8a and 8b highlight a single Operator domain between PE devices. This is since unlike the distributed VPLS PE case (H-VPLS) where VPLS service aware U-PEs and N-PEs may be used to realize a distributed PE, the VPWS has no such distributed PE model. If the PSN involves multiple Operator domains, resulting in a Multi-segment PW [Ms-PW Arch], VPWS OAM Domains remain unchanged since S-PEs are typically not aware of native service.

5.2.3. VPWS MEPs & MIPs

The location of MEPs and MIPs can be based upon the management model used in the VPWS scenarios. The interest remains in being able to monitor end-to-end service and also support segment monitoring in the network to allow isolation of faults to specific areas within the network.

The end-to-end service monitoring is provided by end-to-end ME and additional segment OAM monitoring is provided by segment MEs, all in the Service Provider OAM Domain. The end-to-end MEs and segment MEs are hierarchically organized as mentioned earlier for hierarchical OAM domains. This is shown in Figure 8b (B) and (C).

The CE interfaces support MEPs at the end-to-end Service Provider OAM level for VPWS as an end-to-end service as shown in Figure 9 (B1) and (B2). In addition, PE interfaces may support MIPs at end-to-end Service Provider OAM level when PEs are client service aware, as shown in Figure 9 (B2). As an example, if one considers an end-to-end Ethernet line service offered to a subscriber between CE1 and CE2 which is realized via ATM type AC1 and AC2 and PW which encapsulates ATM over MPLS, the PEs can be considered as Ethernet service unaware, and therefore cannot support any Ethernet MIPs. Figure 9 (B1) represents this particular situation. Of course, another view of the end-to-end service can be ATM, in which case PE1 and PE2 can be considered to be service aware, and therefore support ATM MIPs. Figure 9 (B2) represents this particular situation.

In addition, CEs and PE interfaces support MEPs at a segment (lower level) Service Provider OAM level for AC and PW MEs and no MIPs are involved at this segment Service Provider OAM Level, as shown in Figure 9 (C). Operators may also run segment OAM by having MEPs at Network Operator OAM level, as shown in Figure 9 (D).

The advantage of having layered OAM is that end-to-end and segment OAM can be carried out in an independent manner. It is also possible to carry out some optimizations, e.g. when proactive segment OAM monitoring is performed, proactive end-to-end monitoring may not be needed since client layer end-to-end ME could simply use fault notifications from the server layer segment MEs.

Although many different OAM layers are possible, as shown in Figure 9, not all may be realized. For example, Figure (B2) and (D) may be adequate in some cases.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+


(B1) MEP-----------------------------------------------MEP
```

```
(B2) MEP----------MIP---------------------MIP----------MEP
(C)  MEP-------MEP|MEP------------------MEP|MEP--------MEP
(D)  MEP-------MEP|MEP------------------MEP|MEP--------MEP
```

Figure 9: VPWS MEPs & MIPs

5.2.4. VPWS MEP and MIP Identifiers

In VPWS, the MEPs and MIPs should be identified with their native addressing schemes. MEPs and MIPs Identifiers, i.e. MEP Ids and MIP Ids, must be unique within their corresponding OAM domains and must also be unique to the VPWS service instance.

6. VPLS Service OAM Requirements

These requirements are applicable to VPLS PE offering VPLS as an Ethernet Bridged LAN service, as described in Section 4.1.1. Further, the performance metrics used in requirements are based on [MEF10.1] and [RFC2544].

It is noted that OAM solutions that meet the following requirements may make use of existing OAM mechanisms e.g. Ethernet OAM, VCCV, etc. however must not break these existing OAM mechanisms. If extensions are required to existing OAM mechanisms, these should be coordinated with relevant groups responsible for these OAM mechanisms.

6.1. Discovery

Discovery allows a VPLS service aware device to learn about other devices that support the same VPLS service instance within a given domain.

Discovery also allows a VPLS service aware device to learn sufficient information (e.g. IP addresses, MAC addressed etc.) from other VPLS service aware devices such that VPLS OAM frames can be exchanged among the service aware devices.

(R1) VPLS OAM MUST allow a VPLS service aware device to discover other devices that share the same VPLS service instance(s) within a given OAM domain.

6.2. Connectivity Fault Management

VPLS service is realized by exchanging service frames/packets between devices that support the same VPLS service instance. To allow the exchange of service frames, connectivity between these service aware devices is required.

6.2.1. Connectivity Fault Detection

To ensure service, pro-active connectivity monitoring is required. Connectivity monitoring facilitates connectivity fault detection.

(R2a) VPLS OAM MUST allow pro-active connectivity monitoring between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.2.2. Connectivity Fault Verification

Once a connectivity fault is detected, connectivity fault verification may be performed.

(R2b) VPLS OAM MUST allow connectivity fault verification between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.2.3. Connectivity Fault Localization

Further, localization of connectivity fault may be carried out.

(R2c) VPLS OAM MUST allow connectivity fault localization between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.2.4. Connectivity Fault Notification and Alarm Suppression

Typically, when connectivity fault is detected and optionally verified, VPLS service device may notify the NMS (Network Management System) via alarms.

However, a single transport/network fault may cause multiple services to fail simultaneously causing multiple service alarms. Therefore, VPLS OAM must allow service level fault notification to be triggered at the client layer as a result of transport/network faults in the service layer. This fault notification should be used for the suppression of service level alarms at the client layer.

(R2d) VPLS OAM MUST support fault notification to be triggered as a result of transport/network faults. This fault notification SHOULD be used for the suppression of redundant service level alarms.

6.3. Frame Loss

A VPLS service may be considered degraded if service-layer frames/packets are lost during transit between the VPLS service aware devices. To determine if a VPLS service is degraded due to frame/packet loss, measurement of frame/packet loss is required.

(R3) VPLS OAM MUST support measurement of per-service frame/packet loss between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.4. Frame Delay

A VPLS service may be sensitive to delay experienced by the VPLS frames/packets during transit between the VPLS service aware devices. To determine if a VPLS service is degraded due to frame/packet delay, measurement of frame/packet delay is required.

VPLS frame/packet delay measurement can be of two types:

One-way delay
One-way delay is used to characterize certain applications like multicast and broadcast applications. The measurement for one-way delay usually requires clock synchronization between two devices in question.

Two-way delay
Two-way delay or round-trip delay does not require clock synchronization between two devices involved in measurement and is usually sufficient to determine the frame/packet delay being experienced.

(R4a) VPLS OAM MUST support measurement of per-service two-way frame/packet delay between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

(R4b) VPLS OAM SHOULD support measurement of per-service one-way frame/packet delay between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.5. Frame Delay Variation

A VPLS service may be sensitive to delay variation experienced by the VPLS frames/packets during transit between the VPLS service aware devices. To determine if a VPLS service is degraded due to frame/packet delay variation, measurement of frame/packet delay variation is required. For frame/packet delay variation measurements, one-way mechanisms are considered to be sufficient.

(R5) VPLS OAM MUST support measurement of per-service frame/packet delay variation between two VPLS service aware devices that support the same VPLS service instance within a given OAM domain.

6.6. Availability

A service may be considered unavailable if the service frames/packets do not reach their intended destination (e.g. connectivity is down or frame/packet loss is occurring) or the service is degraded (e.g. frame/packet delay and/or delay variation threshold is exceeded).

Entry and exit conditions may be defined for unavailable state. Availability itself may be defined in context of service type.

Since availability measurement may be associated with connectivity, frame/packet loss, frame/packet delay and frame/packet delay variation measurements, no additional requirements are specified currently.

6.7. Data Path Forwarding

If the VPLS OAM frames flow across a different path than the one used by VPLS service frames/packets, accurate measurement and/or determination of service state may not be made. Therefore data path, i.e. the one being taken by VPLS service frames/packets, must be used for the VPLS OAM.

(R6) VPLS OAM frames MUST be forwarded along the same path (i.e. links and nodes) as the VPLS service/data frames.

6.8. Scalability

Mechanisms developed for VPLS OAM need to be such that per-service OAM can be supported even though the OAM may only be used for limited VPLS service instances, e.g. premium VPLS service instances, and may not be used for best-effort VPLS services.

(R7) VPLS OAM MUST be scalable such that a service aware device can support OAM for each VPLS service that is supported by the device.

6.9. Extensibility

Extensibility is intended to allow introduction of additional OAM functionality in future such that backward compatibility can be maintained when interoperating with older version devices. In such a case, VPLS OAM with reduced functionality should still be possible. Further, VPLS Service OAM should be defined such that OAM incapable devices in the middle of the OAM domain should be able to forward the VPLS OAM frames similar to the regular VPLS service/data frames/packets.

(R8a) VPLS OAM MUST be extensible such that new functionality and information elements related to this functionality can be introduced in future.

(R8b) VPLS OAM MUST be defined such that devices not supporting the OAM are able to forward the OAM frames in a similar fashion as the regular VPLS service/data frames/packets.

6.10. Security

VPLS OAM frames belonging to an OAM domain originate and terminate within that OAM domain. Security implies that an OAM domain must be capable of filtering OAM frames. The filtering is such that the OAM frames are prevented from leaking outside their domain. Also, OAM frames from outside the OAM domains should be either discarded (when such OAM frames belong to same or lower-level OAM domain) or transparently passed (when such OAM frames belong to a higher-level OAM domain).

(R9a) VPLS OAM frames MUST be prevented from leaking outside their OAM domain.

(R9b) VPLS OAM frames from outside an OAM domain MUST be prevented from entering the OAM domain when such OAM frames belong to the same level or lower-level OAM domain.

(R9c) VPLS OAM frames from outside an OAM domain MUST be transported transparently inside the OAM domain when such OAM frames belong to the higher-level OAM domain.

6.11. Transport Independence

VPLS service frame/packets delivery is carried out across transport infrastructure, also called network infrastructure. Though specific transport/network technologies may provide their own OAM capabilities, VPLS OAM must be independently supported as many different transport/network technologies can be used to carry service frame/packets.

(R10a) VPLS OAM MUST be independent of the underlying transport/network technologies and specific transport/network OAM capabilities.

(R10b) VPLS OAM MAY allow adaptation/interworking with specific transport/network OAM functions. For example, this would be useful to allow Fault Notifications from transport/network layer(s) to be sent to the VPLS service layer.

6.12. Application Independence

VPLS service itself may be used to carry application frame/packets.

The application may use its own OAM; service OAM must not be dependent on application OAM. As an example, a VPLS service may be used to carry IP traffic; however, VPLS OAM should not assume IP or rely on the use of IP level OAM functions.

(R11a) VPLS OAM MUST be independent of the application technologies and specific application OAM capabilities.

7. VPWS OAM Requirements

These requirements are applicable to VPWS PE. The performance metrics used in requirements are based on [MEF10.1] and [RFC2544], which are applicable to Ethernet Services.

It is noted that OAM solutions that meet the following requirements may make use of existing OAM mechanisms e.g. Ethernet OAM, VCCV, etc. however must not break these existing OAM mechanisms. If extensions are required to existing OAM mechanisms, these should be coordinated with relevant groups responsible for these OAM mechanisms.

7.1. Discovery

Discovery allows a VPWS service aware device to learn about other devices that support the same VPWS service instance within a given domain. Discovery also allows a VPWS service aware device to learn sufficient information (e.g. IP addresses, MAC addresses etc.) from other VPWS service aware devices such that OAM frames can be exchanged among the VPWS service aware devices.

(R12) VPWS OAM MUST allow a VPWS service aware device to discover other devices that share the same VPWS service instance(s) within a given OAM domain.

7.2. Connectivity Fault Management

VPWS Service is realized by exchanging service frames/packets between devices that support the same VPWS service instance. To allow the exchange of service frames, connectivity between these service aware devices is required.

7.2.1. Connectivity Fault Detection

To ensure service, pro-active connectivity monitoring is required. Connectivity monitoring facilitates connectivity fault detection.

(R13a) VPWS OAM MUST allow pro-active connectivity monitoring between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

(R13b) VPWS OAM mechanism SHOULD allow detection of misbranching or misconnections.

7.2.2. Connectivity Fault Verification

Once a connectivity fault is detected, connectivity fault verification may be performed.

(R13c) VPWS OAM MUST allow connectivity fault verification between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

7.2.3. Connectivity Fault Localization

Further, localization of connectivity fault may be carried out. This may amount to identifying the specific AC and/or PW that is resulting in the VPWS connectivity fault.

(R13d) VPWS OAM MUST allow connectivity fault localization between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

7.2.4. Connectivity Fault Notification and Alarm Suppression

Typically, when connectivity fault is detected and optionally verified, service device may notify the NMS (Network Management System) via alarms.

However, a single transport/network fault may cause multiple services to fail simultaneously causing multiple service alarms. Therefore, OAM must allow service level fault notification to be triggered at the client layer as a result of transport/network faults in the service layer. This fault notification should be used for the suppression of service level alarms at the client layer.

For example, if an AC fails, both local CE and local PE which are connected via AC may detect the connectivity failure. The local CE must notify the remote CE about the failure while the local PE must notify the remote PE about the failure.

(R13e) VPWS OAM MUST MUST support fault notification to be triggered as a result of transport/network faults. This fault notification SHOULD be used for the suppression of redundant service level alarms.

(R13f) VPWS OAM SHOULD support fault notification in backward direction, to be triggered as a result of transport/network faults. This fault notification SHOULD be used for the suppression of redundant service level alarms.

7.3. Frame Loss

A VPWS service may be considered degraded if service-layer frames/packets are lost during transit between the VPWS service aware devices. To determine if a VPWS service is degraded due to frame/packet loss, measurement of frame/packet loss is required.

(R14) VPWS OAM MUST support measurement of per-service frame/packet loss between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

7.4. Frame Delay

A VPWS service may be sensitive to delay experienced by the VPWS service frames/packets during transit between the VPWS service aware devices. To determine if a VPWS service is degraded due to frame/packet delay, measurement of frame/packet delay is required.

VPWS frame/packet delay measurement can be of two types:
- One-way delay
One-way delay is used to characterize certain applications like multicast and broadcast applications. The measurement for one-way delay usually requires clock synchronization between two devices in question.
- Two-way delay
Two-way delay or round-trip delay does not require clock synchronization between two devices involved in measurement and is usually sufficient to determine the frame/packet delay being experienced.

(R15a) VPWS OAM MUST support measurement of per-service two-way frame/packet delay between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

(R15b) VPWS OAM SHOULD support measurement of per-service one-way frame/packet delay between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

7.5. Frame Delay Variation

A VPWS service may be sensitive to delay variation experienced by the VPWS frames/packets during transit between the VPWS service aware devices. To determine if a VPWS service is degraded due to frame/packet delay variation, measurement of frame/packet delay variation is required. For frame/packet delay variation measurements, one-way mechanisms are considered to be sufficient.

(R16) VPWS OAM MUST support measurement of per-service frame/packet delay variation between two VPWS service aware devices that support the same VPWS service instance within a given OAM domain.

7.6. Availability

A service may be considered unavailable if the service frames/packets do not reach their intended destination (e.g. connectivity is down or frame/packet loss is occurring) or the service is degraded (e.g. frame/packet delay and/or delay variation threshold is exceeded).

Entry and exit conditions may be defined for unavailable state. Availability itself may be defined in context of service type. Since availability measurement may be associated with connectivity, frame/packet loss, frame/packet delay and frame/packet delay variation measurements, no additional requirements are specified currently.

7.7. Data Path Forwarding

If the VPWS OAM frames flow across a different path than the one used by VPWS service frames/packets, accurate measurement and/or determination of service state may not be made. Therefore data path, i.e. the one being taken by VPWS service frames/packets, must be used for the VPWS OAM.

(R17a) VPWS OAM frames MUST be forwarded along the same path as the VPWS service/data frames.

(R17b) VPWS OAM MUST be forwarded using the transfer plane (data plane) as regular VPWS service/data frames/packets and must not rely on control plane messages.

7.8. Scalability

Mechanisms developed for VPWS OAM need to be such that per-service OAM can be supported even though the OAM may only be used for limited VPWS service instances, e.g. premium VPWS service instance, and may not be used for best-effort services.

(R18) VPWS OAM MUST be scalable such that a service aware device can support OAM for each VPWS service that is supported by the device.

7.9. Extensibility

Extensibility is intended to allow introduction of additional OAM functionality in future such that backward compatibility can be maintained when interoperating with older version devices. In such a case, VPWS service OAM with reduced functionality should still be possible. Further, VPWS service OAM should be such that OAM incapable devices in the middle of the OAM domain should be able to forward the VPWS OAM frames similar to the regular VPWS service/data frames/packets.

(R19a) VPWS OAM MUST be extensible such that new functionality and information elements related to this functionality can be introduced in future.

(R19b) VPWS OAM MUST be defined such that devices not supporting the OAM are able to forward the VPWS OAM frames in a similar fashion as the regular VPWS service/data frames/packets.

7.10. Security

VPWS OAM frames belonging to an OAM domain originate and terminate within that OAM domain. Security implies that an OAM domain must be capable of filtering OAM frames. The filtering is such that the VPWS OAM frames are prevented from leaking outside their domain. Also, VPWS OAM frames from outside the OAM domains should be either discarded (when such OAM frames belong to same or lower-level OAM domain) or transparently passed (when such OAM frames belong to a higher-level OAM domain).

(R20a) VPWS OAM frames MUST be prevented from leaking outside their OAM domain.

(R20b) VPWS OAM frames from outside an OAM domain MUST be prevented from entering the OAM domain when such OAM frames belong to the same level or lower-level OAM domain.

(R20c) VPWS OAM frames from outside an OAM domain MUST be transported transparently inside the OAM domain when such OAM frames belong to the higher-level OAM domain.

7.11. Transport Independence

VPWS service frame/packets delivery is carried out across transport infrastructure, also called network infrastructure. Though specific transport/network technologies may provide their own OAM capabilities, VPWS OAM must be independently supported as many different transport/network technologies can be used to carry service frame/packets.

(R21a) VPWS OAM MUST be independent of the underlying transport/network technologies and specific transport/network OAM capabilities.

(R21b) VPWS OAM MAY allow adaptation/interworking with specific transport/network OAM functions. For example, this would be useful to allow Fault Notifications from transport/network layer(s) to be sent to the VPWS service layer.

7.12. Application Independence

VPWS service itself may be used to carry application frame/packets. The application may use its own OAM; VPWS OAM must not be dependent on application OAM. As an example, a VPWS service may be used to carry IP traffic; however, VPWS OAM should not assume IP or rely on the use of IP level OAM functions.

(R22a) OAM MUST be independent of the application technologies and specific application OAM capabilities.

7.13. Prioritization

VPWS service could be composed of several data flows each related to a given usage/application with specific requirements in term of connectivity and/or performances. Dedicated VPWS OAM should be applicable to these flows.

(R23) VPWS OAM SHOULD support configurable prioritization for OAM packet/frames to be compatible with associated VPWS service packets/frames.

8. VPLS (V)LAN Emulation OAM Requirements

8.1. Partial-mesh of PWs

As indicated in [BRIDGE-INTEROP], VPLS service OAM relies upon bidirectional Ethernet links or (V)LAN segments and failure in one direction or link results in failure of the whole link or (V)LAN segment. Therefore, when partial-mesh failure occurs in (V)LAN emulation, either the entire PW mesh should be shutdown when only an entire VPLS service is acceptable or a subset of PWs should be shutdown such that the remaining PWs have full connectivity among them, when partial VPLS service is acceptable.

(R13a) PW OAM for PWs related to a (V)LAN emulation MUST allow detection of partial-mesh failure condition.

(R13b) PW OAM for PWs related to a (V)LAN emulation MUST allow the entire mesh of PWs to be shutdown upon detection of a partial-mesh failure condition.

(R13c) PW OAM for PWs related to a (V)LAN emulation MUST allow the subset of PWs to be shutdown upon detection of a partial-mesh failure condition in a manner such that full mesh is present across the remaining subset.

Note: Shutdown action in R13b and R13c may not necessarily involve withdrawal of labels etc.

8.2. PW Fault Recovery

As indicated in [BRIDGE-INTEROP], VPLS service OAM fault detection and recovery relies upon (V)LAN emulation recovery such that fault detection and recovery time in (V)LAN emulation should be less than the VPLS service fault detection and recovery time to prevent unnecessary switch-over and temporary flooding/loop within customer OAM domain that is dual-homed to provider OAM domain.

(R14a) PW OAM for PWs related to a (V)LAN emulation MUST support a fault detection time in the provider OAM domain faster than the VPLS fault detection time in the customer OAM domain.

(R14b) PW OAM for PWs related to a (V)LAN emulation MUST support a fault recovery time in the provider OAM domain faster than the VPLS fault recovery time in the customer OAM domain.

8.3. Connectivity Fault Notification and Alarm Suppression

When connectivity fault is detected in (V)LAN emulation, PE devices may notify the NMS (Network Management System) via alarms. However, a single (V)LAN emulation fault may result in CE devices or U-PE devices detecting connectivity fault in VPLS service and therefore also notifying the NMS. To prevent multiple alarms for the same fault, (V)LAN emulation OAM must provide alarm suppression capability in the VPLS service OAM.

(R15) PW OAM for PWs related to a (V)LAN emulation MUST support interworking with VPLS service OAM to trigger fault notification and allow alarm suppression in the VPLS service upon fault detection in (V)LAN emulation.

9. OAM Operational Scenarios

This section highlights how the different OAM mechanisms can be applied as per the OAM framework for different L2VPN services.

9.1. VPLS OAM Operational Scenarios

```
     ---                                                   ---
    /   \         ------      -------      ----           /   \
    | A CE--     /      \    /       \    /    \       --CE A |
    \   /   \   /        \  /         \  /      \     /   \   /
     ---     --UPE        NPE          NPE        UPE--     ---
                \         / \          / \      /
```

```
                 \      /    \       /    \    /
                  ------      -------      ----
```

```
                         Customer OAM domain
 (C)    MEP---MIP--------------------------------MIP---MEP

                  Service Provider(SP) OAM domain
 (D)          MEP--------MIP-----------MIP-------MEP

                 SP OAM       SP OAM       SP OAM
 (D1)         MEP-MIP--MEP|MEP-------MEP|MEP-----MEP
                 domain       domain       domain

                 Operator    Operator     Operator
 (E)          MEP-MIP--MEP|MEP-------MEP|MEP-----MEP
                OAM domain   OAM domain   OAM domain

                              MPLS OAM   MPLS OAM
 (F)                      MEP--MIP-----MEP--MIP--MEP
                               domain      domain
```

           Figure 10: VPLS OAM Domains, MEPs & MIPs

Among the different MEs identified in Figure 5, for VPLS OAM in Customer OAM domain, [IEEE 802.1ag] and [Y.1731] Ethernet OAM mechanisms can be applied, to meet various requirements identified in Section 6. The mechanisms can be applied across Figure 10 (C) MEs.

Similarly, inside the Service Provider OAM domain, [IEEE 802.1ag] and [Y.1731] Ethernet OAM mechanisms can be applied across Figure 10 (D) MEs to meet functional requirements identified in Section 6.

It may be noted that in the interim, when [IEEE 802.1ag] and [Y.1731] capabilities are not available across the PE devices, the fault management option using segment OAM introduced in Section **5.2.3 can be applied, with the limitations cited below. In this** option, the Service Provider can run segment OAM across the Figure **10 (D1) MEs. The OAM mechanisms across the Figure 10 (D1) MEs can be** non-Ethernet e.g. VCCV, or BFD when network technology is MPLS. The Service Provider can monitor each sub-network segment ME using the native technology OAM and by performing interworking across the segment MEs, attempt to realize end-to-end monitoring between a pair of VPLS end-points. However, such mechanisms do not fully utilize the data plane forwarding as experienced by native (i.e. Ethernet) service PDUs and therefore monitoring is severely limited in the sense that monitoring at Figure 10 (D1) and interworking across them could lead to an indication that the ME between VPLS end-points is functional while the customer may be experiencing end-to-end connectivity issues in the data plane.

Inside the Network Operator OAM domain, [IEEE 802.1ag] and [Y.1731]

Ethernet OAM mechanisms can also be applied across Figure 10 (E) MEs to meet functional requirements identified in Section 6. In addition, the network operator could decide to use native OAM mechanisms e.g. VCCV or BFD across Figure 10 (F) MEs for additional monitoring or as an alternative to monitoring across Figure 10 (E) MEs.

10. Acknowledgments

The authors would like to thank Deborah Brungard, Vasile Radoaca, Lei Zhu, Yuichi Ikejiri, Yuichiro Wada, and Kenji Kumaki for their reviews and comments.

Authors would also like to thank Shahram Davari, Norm Finn, Dave Allan, Thomas Nadeau, Monique Morrow, Yoav Cohen, Marc Holness, Malcolm Betts, Paul Bottorff, Hamid-ould Brahim, Lior Shabtay, and Dan Cauchy for their feedback.

12. IANA Considerations

This document has no actions for IANA.

11. Security Considerations

This document takes into account the security considerations and imposes requirements on solutions to prevent OAM messages from leaking outside an OAM domain and for OAM domains to be transparent to OAM frames from higher OAM domains, as specified in Section 6.10 and 7.10.

For additional levels of security, the solutions may be required to encrypt and/or authenticate OAM frames inside an OAM domain however solutions are out of the scope of this draft.

13. References

13.1 Normative References

[IEEE 802.1ad] "IEEE Standard for Local and metropolitan area networks - virtual Bridged Local Area Networks, Amendment 4: Provider Bridges", 2005

[IEEE 802.1ag] "IEEE Standard for Local and metropolitan area networks - virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management", 2007

[IEEE 802.1ah] "IEEE Standard for Local and metropolitan area networks - virtual Bridged Local Area Networks, Amendment 6: Provider Backbone Bridges", 2008

[Y.1731] "ITU-T Recommendation Y.1731 (02/08) - OAM functions and mechanisms for Ethernet based networks", February 2008

[L2VPN-FRWK] "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664

[L2VPN-REQ] "Service Requirements for Layer-2 Provider Provisioned Virtual Private Networks", RFC 4665

[L2VPN-TERM] "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026

[MEF10.1] "Ethernet Services Attributes: Phase 2", MEF 10.1, 2006

[NM-Standards] "TMN Management Functions", M.3400, February 2000

[VPLS-BGP] "Virtual Private LAN Service", RFC 4761, Jan 2007

[VPLS-LDP] "Virtual Private LAN Services over MPLS", RFC 4762, Jan 2007

13.2 Informative References

[BRIDGE-INTEROP] "VPLS Interoperability with CE Bridges", draft-ietf-l2vpn-vpls-bridge-interop-05.txt, Work in progress, March 2010

[L2VPN-SIG] "Provisioning, Autodiscovery, and Signaling in L2VPNs", draft-ietf-l2vpn-signaling-08.txt, Work in progress, May 2006

[MS-PW Arch] "An Architecture for Multi-segment Pseudowire Emulation Edge-to-Edge", draft-ietf-pwe3-ms-pw-arch-04.txt, Work in progress, June 2008

[RFC2544] "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, 1999

A1. Appendix 1 - Alternate Management Models

In consideration of the management models that can be deployed besides the hierarchical models elaborated in this document, this section highlights some alternate models that are not recommended due to their limitations, as pointed out below. These alternatives have been highlighted as potential interim models while the network equipments are upgraded to support full functionality and meet the requirements set forward by this document.

A1.1. Alternate Model 1 (Minimal OAM)

In this model, the end-to-end service monitoring is provided by applying CE to CE ME in the Service Provider OAM Domain.

A MEP is located at each CE interface that is part of the VPWS service, as shown in Figure A1.1 (B). The network operators can carry out segment (e.g. PSN Tunnel ME, etc.) monitoring independent of the VPWS end-to-end service monitoring, as shown in Figure A1.1 (D).

The advantage of this option is that VPWS service monitoring is limited to CEs. The limitation of this option is that the localization of faults at the VPWS Service level.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+


(B)  MEP-----------------------------------------------MEP
(D)  MEP-------MEP|MEP------------------MEP|MEP--------MEP
```

Figure A1.1: VPWS MEPs & MIPs - Minimal OAM

A1.2. Alternate Model 2 (Segment OAM Interworking)

In this model, the end-to-end service monitoring is provided by interworking OAM across each segment. Typical segments involved in this case include two AC MEs and PW ME, as shown in Figure A1.2 (C). These segments are expected in the Service Provider OAM Domain. An interworking function is required to transfer the OAM information flows across the OAM segments for the purposes of end-to-end monitoring. Depending on whether homogenous VPWS is deployed or heterogeneous VPWS is deployed, the interworking function could be straightforward or more involved.

In this option, the CE and PE interfaces support MEPs for AC and PW MEs and no MIPs are involved at the Service Provider OAM Level, as shown in Figure A1.2 (C). The network operators may run segment OAM by having MEPs at Network Operator OAM level, as shown in Figure A1.2 (D).

The limitations of this model are that it requires interworking across the OAM segments and does not conform to the OAM layering principles, where each OAM layer ought to be independent of the other. For end-to-end OAM determinations, the end-to-end service frame path is not necessarily exercised. Further, it requires interworking function implementation for all possible technologies across access and core that may be used to realize end-to-end services.

```
     |<--------------- VPWS <AC1,PW,AC2> -------------->|
     |                                                  |
     |          +----+                  +----+          |
+----+          |    |==================|    |          +----+
|    |---AC1----|............PW..............|--AC2-----|    |
| CE1|          |PE1 |                  | PE2|          |CE2 |
+----+          |    |==================|    |          +----+
                +----+     PSN Tunnel   +----+


(C)  MEP-------MEP|MEP------------------MEP|MEP--------MEP
(D)  MEP-------MEP|MEP------------------MEP|MEP--------MEP
```

    Figure A1.2: VPWS MEPs & MIPs - Segment OAM Interworking

Authors' Addresses

Ali Sajassi
Cisco Systems, Inc.
170 **West Tasman Drive**
San Jose, CA 95134
Email: sajassi@cisco.com

Dinesh Mohan
Nortel
3500 **Carling Ave**
Ottawa, ON K2H8E9
Email: mohand@nortel.com

Simon Delord
Uecomm
658 **Church St**
Richmond, VIC, 3121, Australia
E-mail: sdelord@uecomm.com.au

Philippe Niger
France Telecom
2 **av. Pierre Marzin**
22300 **LANNION, France**
E-mail: philippe.niger@francetelecom.com

Samer Salam
Cisco Systems, Inc.
170 **West Tasman Drive**
San Jose, CA 95134
Email: ssalam@cisco.com