                   Layer 2 Virtual Private Network (L2VPN)
              Operations, Administration, and Maintenance (OAM)
                         Requirements and Framework

Abstract

   This document provides framework and requirements for Layer 2 Virtual
   Private Network (L2VPN) Operations, Administration, and Maintenance
   (OAM). The OAM framework is intended to provide OAM layering across
   L2VPN services, pseudowires (PWs), and Packet Switched Network (PSN)
   tunnels. This document is intended to identify OAM requirements for
   L2VPN services, i.e., Virtual Private LAN Service (VPLS), Virtual
   Private Wire Service (VPWS), and IP-only LAN Service (IPLS).
   Furthermore, if L2VPN service OAM requirements impose specific
   requirements on PW OAM and/or PSN OAM, those specific PW and/or PSN
   OAM requirements are also identified.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6136.

Table of Contents

1. Introduction

   This document provides framework and requirements for Layer 2 Virtual
   Private Network (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)
   Configuration Management, c) Accounting Management, d) Performance
   Management, and e) Security Management.

This document 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 and 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, misconfiguration, etc.
Typically, a lightweight protocol is desirable to detect the fault
and thus it would be prudent to verify the fault via a 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. A fault notification mechanism can be
used in conjunction with a 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 the server layer to
      the client layer network(s) using the fault notification format
      appropriate to the client layer

   - Sending a backward fault notification at the server layer, if
      applicable, in the reverse direction

   - Sending a backward fault notification at the 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 the network/services under consideration. Performance Management can be used to verify the compliance to both the service-level 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: Virtual Private LAN Service (VPLS), (Virtual Private Wire Service (VPWS), and IP-only LAN Service (IPLS).

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

1.1. Specification of Requirements

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 [RFC2119].

1.2. Relationship with Other OAM Work

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

-   IEEE Std. 802.1ag-2007 [IEEE802.1ag] 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.

2. Terminology

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

   AIS   Alarm Indication Signal

   IPLS   IP-only LAN Service

   ME   Maintenance Entity, which is defined in a given OAM
                domain and represents an entity requiring management

   MEG   Maintenance Entity Group, which represents MEs belonging
                to the same service instance and is also called
                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 and respond to certain OAM frames
                but does not initiate or terminate them.

   OAM Domain   OAM Domain represents a region over which OAM frames can
                operate unobstructed.

   QinQ   802.1Q tag inside another 802.1Q tag

   RDI   Remote Defect Indication

   VPLS   Virtual Private LAN Service

   VPWS   Virtual Private Wire Service

3. L2VPN Services and Networks

   Figure 1 shows an L2VPN reference model as described in [L2VPN-REQ].
   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
```
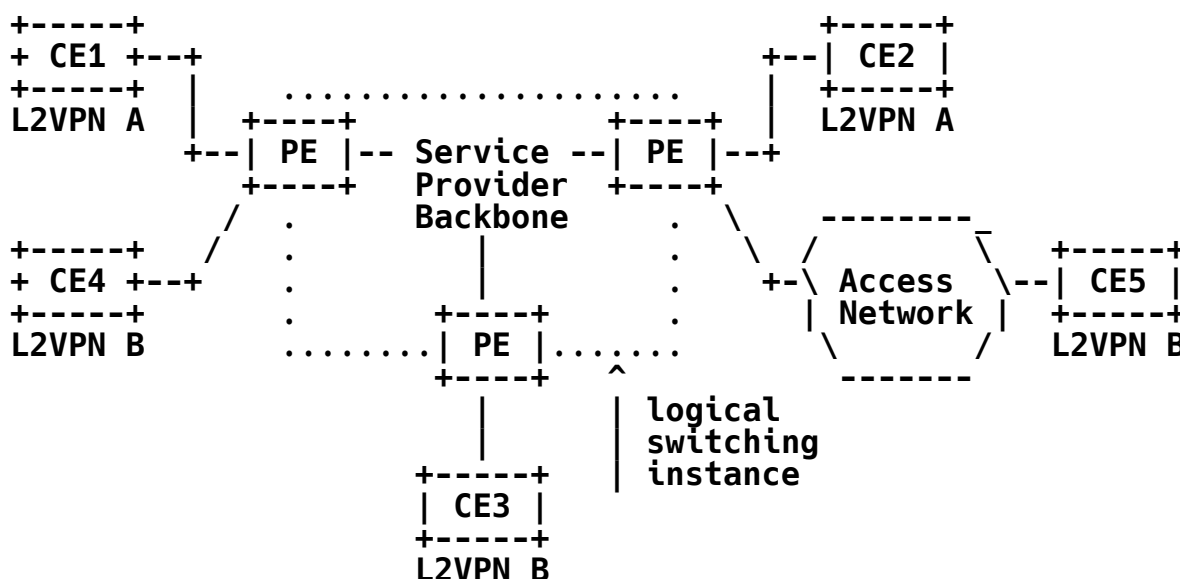
                    Figure 1: L2VPN Reference Model

   [L2VPN-FRWK] specifies VPWS, VPLS, and IPLS. VPWS is a point-to-
   point service where Customer Edges (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 were
   connected via a bridged LAN. IPLS is a special VPLS that is used to
   carry only IP service packets.

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

4. L2VPN OAM Framework

4.1. OAM Layering

   The point-to-point or bridged LAN functionality is emulated by a
   network of Provider Edges (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 the same administrative organization,
or they can belong to different administrative organizations.

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

4.2. OAM Domains

When discussing OAM tools for L2VPNs, it is important to provide OAM
capabilities and functionality over each domain for which a service
provider or a network operator is responsible. It is also important
that OAM frames not be 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 the 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, with an
interface at the boundary of an OAM domain, shall block outgoing OAM
frames, filter out incoming OAM frames whose domain level is lower or
the same as 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 a customer OAM
domain, a service provider OAM domain, and network operator OAM
domains 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
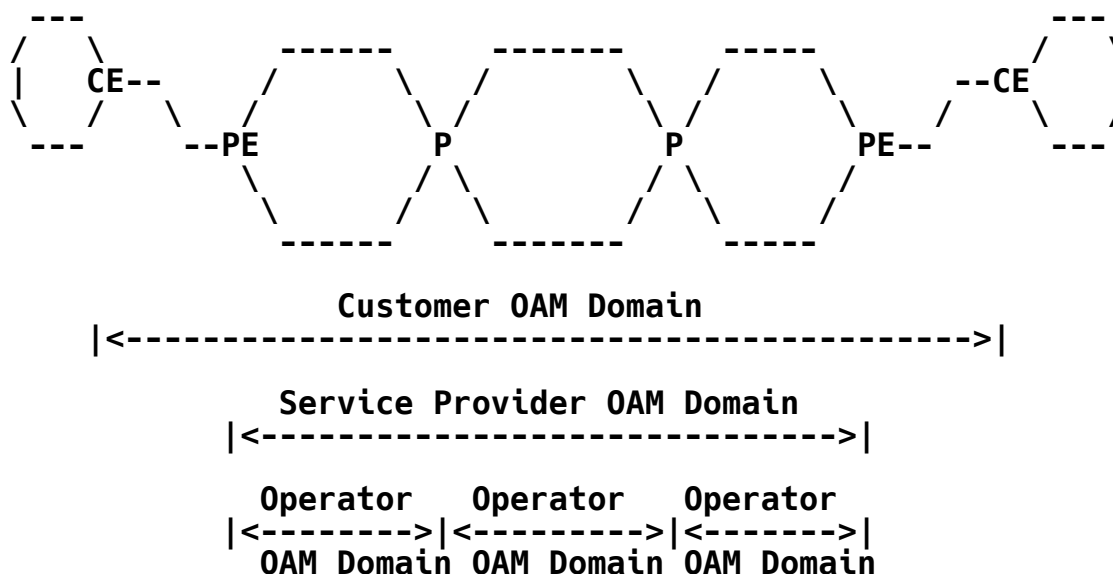
                      Figure 2: OAM Domains

   The OAM Domains can be categorized as follows:

     - Hierarchical OAM Domains: Hierarchical OAM Domains result from
        OAM Layering and imply a contractual agreement among the OAM
        Domain owning entities. In Figure 2, the customer OAM domain,
        the service provider OAM domain, and the operator OAM domains
        are hierarchical.

     - Adjacent OAM Domains: Adjacent OAM Domains are typically
        independent of each other and do not have any relationship
        among them. In Figure 2, the different operator OAM domains
        are independent of each other.

4.3. 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 Group
   (MEG), where a MEG consists of a set of Maintenance Entities (MEs)

associated with the same service instance. An ME is a point-to-point
association between a pair of MEPs and represents a monitored entity.
For example, in a VPLS that involves n CEs, all the MEs associated
with the VPLS 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, the VPWS ME in the customer OAM domain can
overlap with the Attachment Circuit (AC) ME, PW ME, and another AC ME
in service provider OAM domain. Similarly, the PW ME can overlap
with different ME in operator OAM domains.

4.4. MEP and MIP Identifiers

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

5. OAM Framework for VPLS

Virtual Private LAN Service (VPLS) is used in different contexts,
such as the following: 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.

5.1. VPLS as Service/Network

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

Throughout this document, whenever the term "VPLS" is used by itself,
it refers to the service as opposed to network or LAN emulation.

A VPLS instance is also analogous to a VLAN provided by IEEE 802.1Q
networks since each VLAN provides a Virtual LAN service to its Media
Access Control (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
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 as defined in
[L2VPN-REQ], which is from AC to AC, including bridge module, VPLS
forwarder, and the associated PWs for this service. This document
specifies the framework and requirements for such OAM mechanisms.

5.1.2. 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 in H-VPLS with MPLS/IP access, or it 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, distributed topology, 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 document.

5.1.3. VPLS as (V)LAN Emulation

Sometimes VPLS also refers to (V)LAN emulation. In this context,
VPLS only refers to the full mesh of PWs with split horizon that
emulates a LAN segment over a 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 their associated full mesh of

      PWs and the ability to detect and notify a partial mesh failure.
      This document also covers the OAM framework and requirements for such
      OAM mechanisms.

5.2. 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. For example, the access network on one side can
      be a bridged network, e.g., [IEEE802.1ad], as described in Section 11
      of [VPLS-LDP]. The access network can also be a [IEEE802.1ah]-based
      bridged network. The access network on the 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
      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 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, 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 Metro
      Ethernet Forum (MEF), which address Ethernet network and service OAM.

5.2.1. VPLS OAM Layering

      Figure 3 shows an example of a VPLS (with two CEs 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. The service provider
      network is segmented into a core network and two types of access
      networks. In 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. In Figure 3,
      (B) shows the service/network view at the Ethernet MAC layer marked
      by E.

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

	CE----UPE--B--B--NPE---P--P---NPE---P----UPE----CE
(A)	CE----UPE--B--B--NPE---P--P---NPE---P----UPE----CE
(B)	E------E---E--E---E-----------E----------E-----E
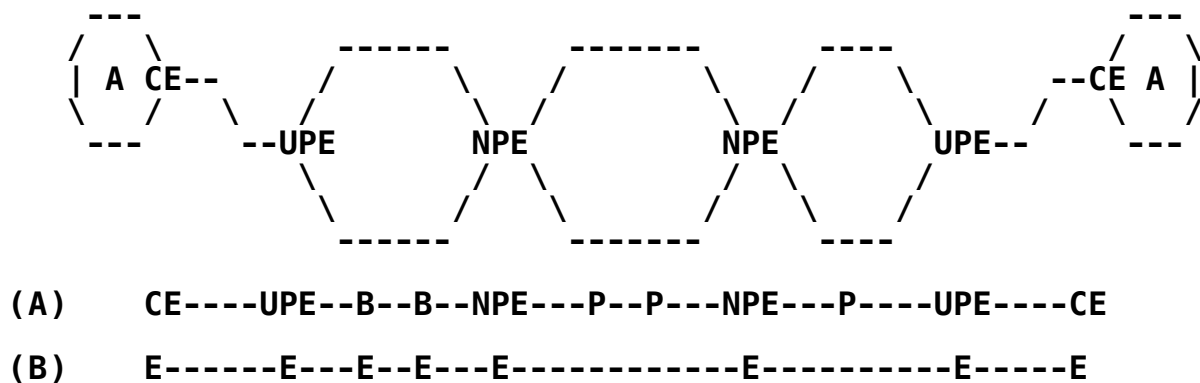
              Figure 3: VPLS-Specific Device View

   As shown in (B) of Figure 3, only the devices with Ethernet
   functionality are visible to OAM mechanisms operating at the 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 the
   transport layer, and it is outside the scope of this document.

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

5.2.2. VPLS OAM Domains

   As described in the previous section, a VPLS 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
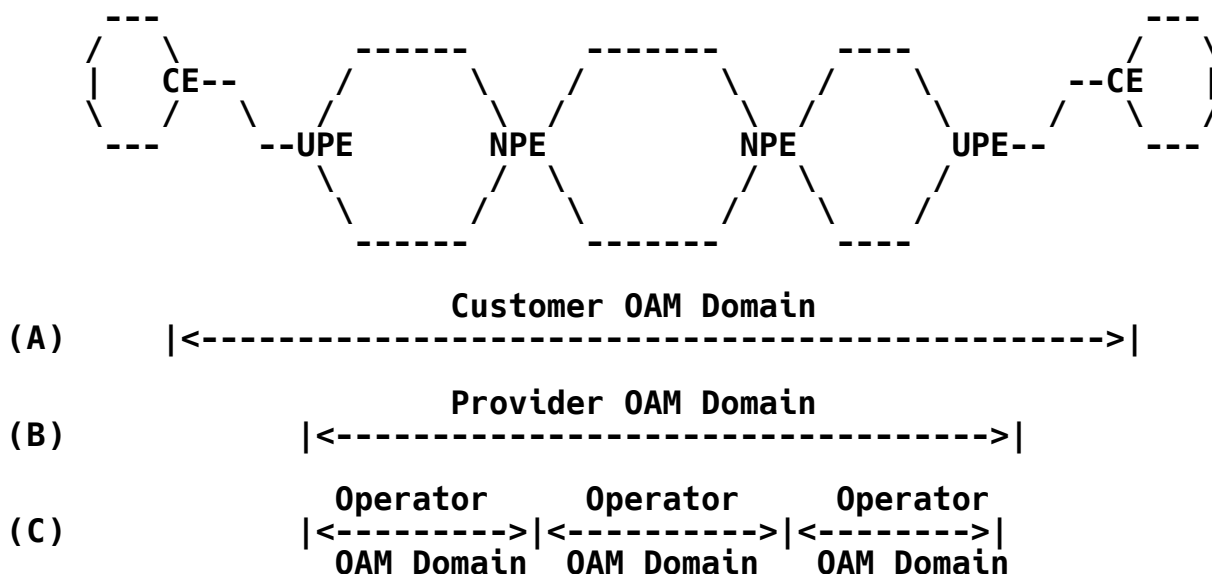
                     Figure 4: VPLS OAM Domains

5.2.3. VPLS MEPs and MIPs

   As shown in Figure 5, (C) represents those MEPs and MIPs that are
   visible within the customer domain. The MIPs associated with (C) are
   expected to be implemented in the bridge module/VPLS forwarder of a
   PE device, as per [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 [L2VPN-FRWK]. (E) represents the MEPs and MIPs
   visible within each operator domain, where MIPs only exist in an
   Ethernet access network (i.e., an MPLS access network does not 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;
   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
```
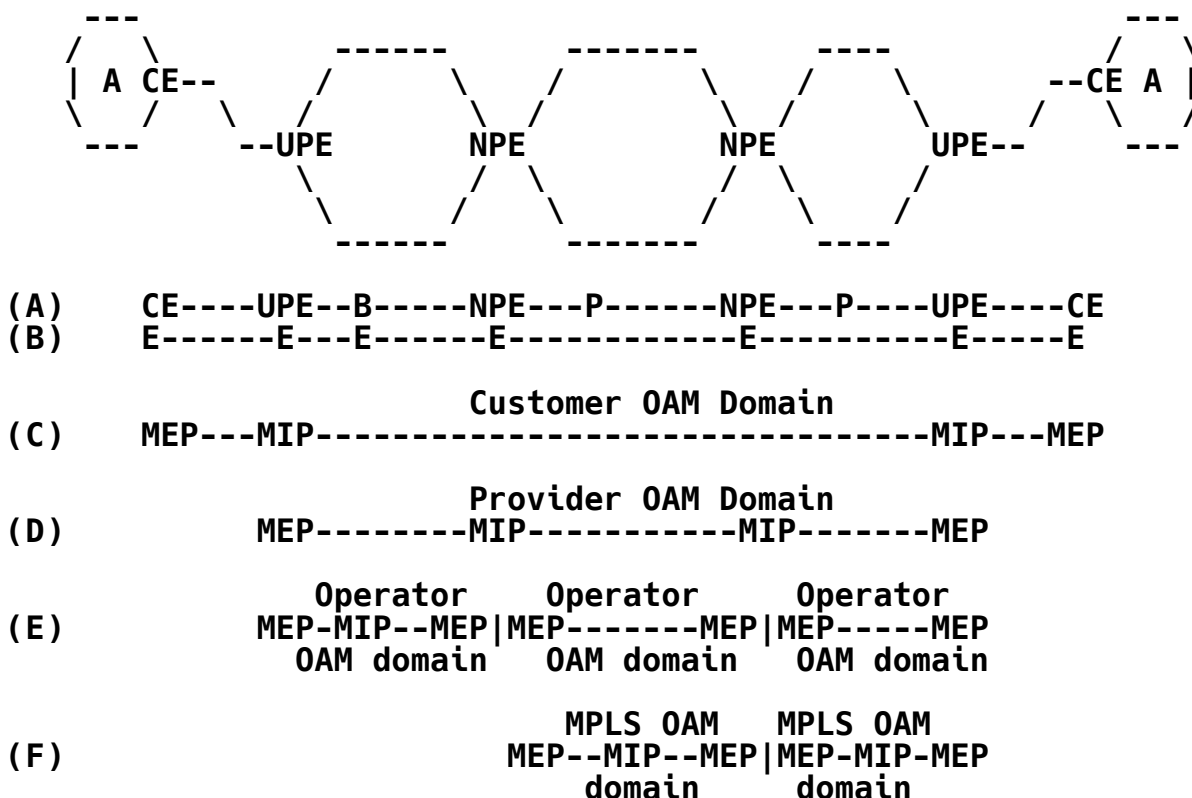
                Figure 5: VPLS OAM Domains, MEPs, and MIPs

5.2.4. VPLS MEP and MIP Identifiers

   In VPLS, for the Ethernet MAC layer, the MEPs and MIPs should be
   identified with their Ethernet MAC addresses and Maintenance Entity
   Group Identifier (MEG ID). As described in [VPLS-LDP], a VPLS
   instance can be identified in an Ethernet domain (e.g., 802.1ad
   domain) using a 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 a specific MEG. For unicast Ethernet
   OAM frames, the destination MAC address represents the destination
   MEP in that domain for a specific MEG. For multicast Ethernet OAM
   frames, the destination MAC addresses correspond to all MEPs in that
   domain for a specific MEG.

6. 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 (ACs) and
a single PW between two PEs.

```
        |<------------- VPWS1 <AC11,PW1,AC12> ------------>|
        |                                                  |
        |          +----+                     +----+       |
 +----+ |          |====================|          +----+
 |    | |---AC11---|PE1 |.......PW1........ |PE2 |--AC12----|    |
 |CE1 | |          |    |                   |    |          |CE2 |
 |    | |---AC21---|    |.......PW2........  |    |--AC22----|    |
 +----+ |          |====================|          +----+
        |          +----+   PSN Tunnel    +----+       |
        |                                                  |
        |<------------- VPWS2 <AC21,PW2,AC22> ------------>|
```
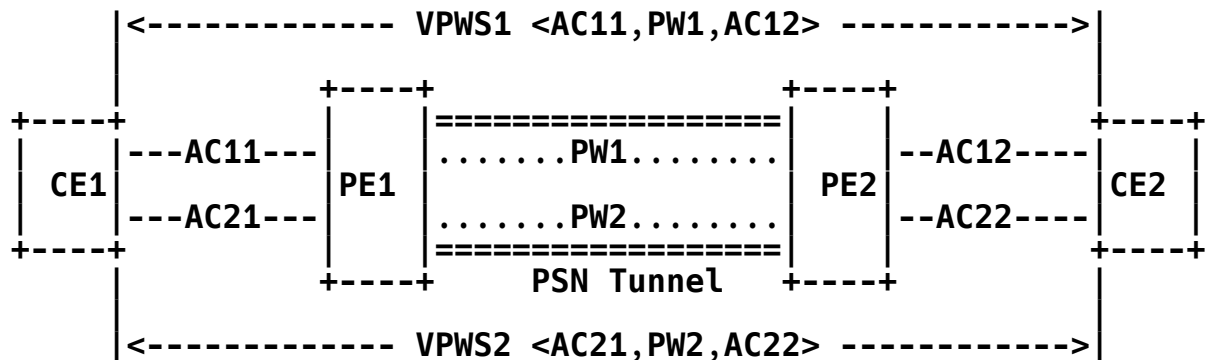
                    Figure 6: VPWS Reference Model

6.1. VPWS as Service

VPWS can be categorized as follows:

- VPWS with homogeneous ACs (where both ACs are same type)

- VPWS with heterogeneous ACs (where the ACs are of different
  Layer-2 encapsulation)

Further, the VPWS can itself be classified as follows:

- Homogeneous VPWS (when two ACs and PW are of the same type)

- Heterogeneous VPWS (when at least one AC or PW is a 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.

Throughout this document, whenever the term "VPWS" is used by itself,
it refers to the service.

6.2. 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 the CE and PE
on one side can be an Ethernet-bridged network, an ATM network, etc.
In common scenarios, it could simply be a point-to-point interface
such as Ethernet Physical Layer (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 multiple such networks may be associated with a single
administrative domain.

6.2.1. VPWS OAM Layering

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

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 (A) in Figure 7,
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, such as Ethernet VPWS, which is offered across an
ATM AC, ATM PW, and Ethernet AC. In this case, the PE that is
attached to ATM AC and ATM PW may be transparent to the client
Ethernet service PDUs. On the other hand, the PE that 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 (B) in Figure 7, 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
```
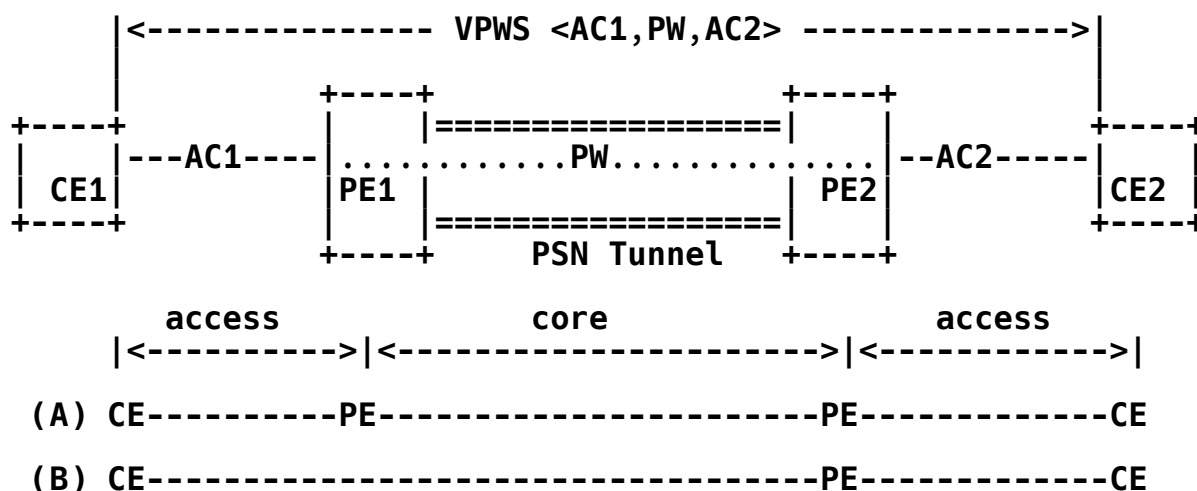
                  Figure 7: VPWS-Specific Device View

6.2.2. VPWS OAM Domains

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

   Figures 8a and 8b depict 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, 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)              |<---------------->|
```
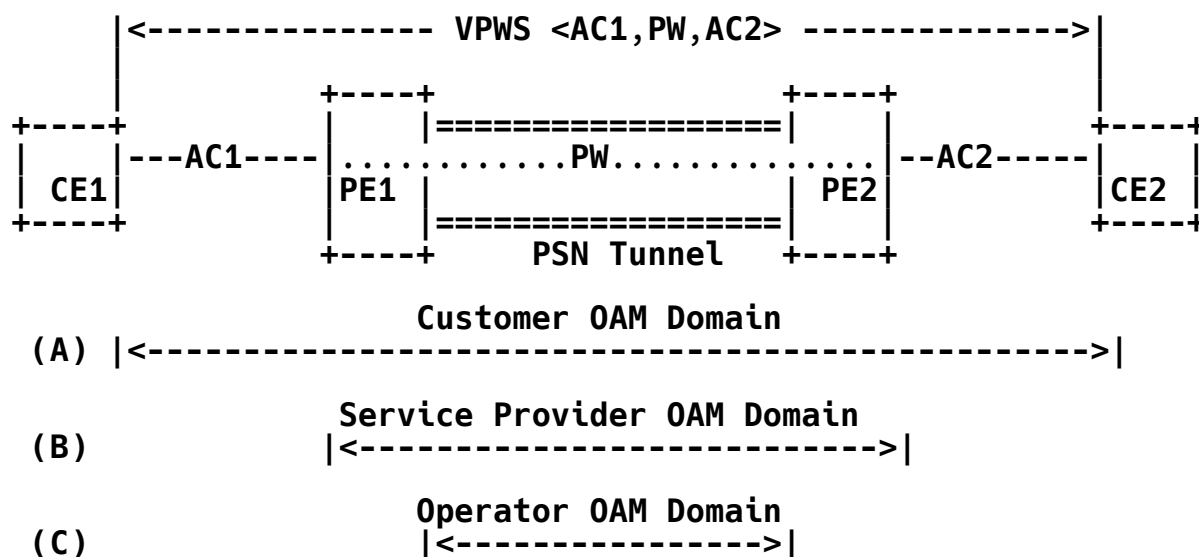
                Figure 8a: VPWS OAM Domains - Management Model 1

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 ME spans between the CEs in the service provider OAM
domain, as shown by (B) in Figure 8b. The service provider OAM
domain may additionally monitor the AC MEs and PW MEs individually,
as shown by (C) in Figure 8b. The network operators may be
responsible for managing the access service MEs (e.g., access
tunnels) and core PSN Tunnel MEs, as shown by (D) in Figure 8b. The
distinction between (C) and (D) in Figure 8b 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; 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
```
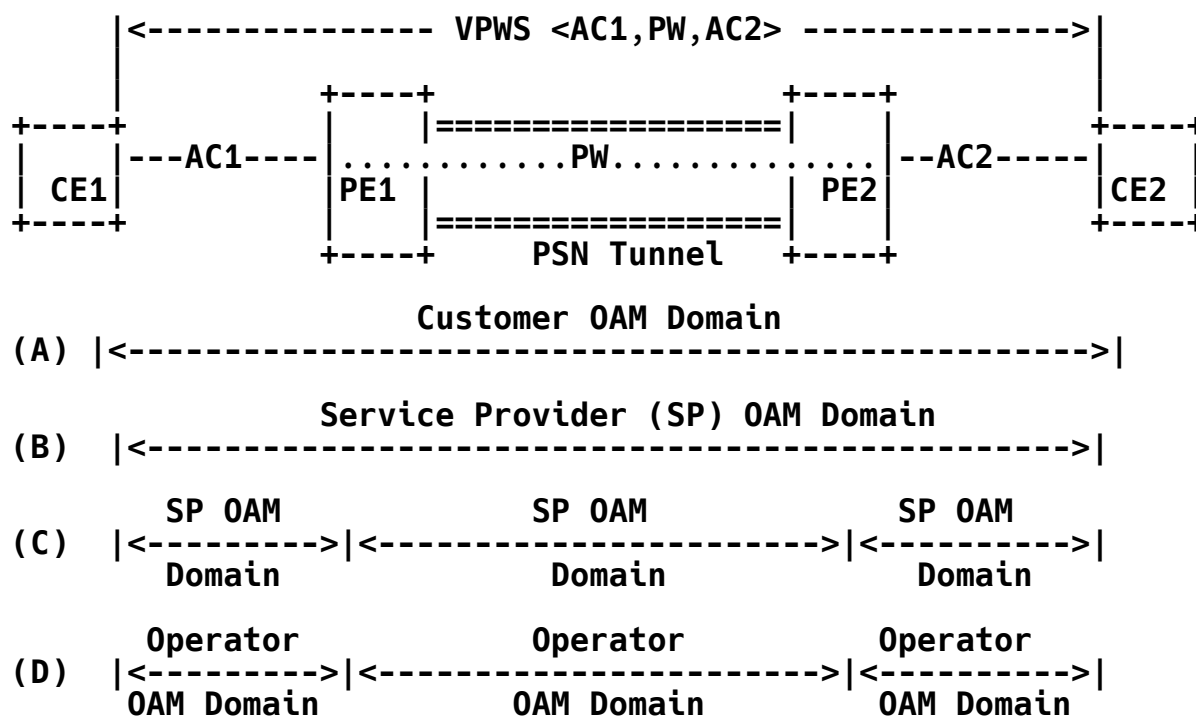
                Figure 8b: VPWS OAM Domains - Management Model 2

   Note: It may be noted that unlike VPLS OAM Domain in Figure 4, where
   multiple operator domains may occur between the User-facing PE (U-PE)
   devices, VPWS OAM domain in Figures 8a and 8b highlights a single
   operator domain between PE devices. This is since, unlike the
   distributed VPLS PE case (D-VPLS), where VPLS-aware U-PEs and
   Network-facing PEs (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 switched PEs
   are typically not aware of native service.

6.2.3. VPWS MEPs and 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 an 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 in Section 4.2 for
hierarchical OAM domains. This is shown in (B) and (C) in Figure 8b.

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 (B1) and (B2) in
Figure 9. In addition, PE interfaces may support MIPs at the end-to-
end service provider OAM level when PEs are client service aware, as
shown in (B2) in Figure 9. As an example, if one considers an end-
to-end Ethernet line service offered using ATM transport (ATM over
MPLS PW), then the PEs are considered to be Ethernet service unaware
and therefore cannot support any Ethernet MIPs. (B1) in Figure 9
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. (B2)
in Figure 9 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 (C)
in Figure 9. Operators may also run segment OAM by having MEPs at
network operator OAM level, as shown in (D) in Figure 9.

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, (B2) and (D) in Figure 9
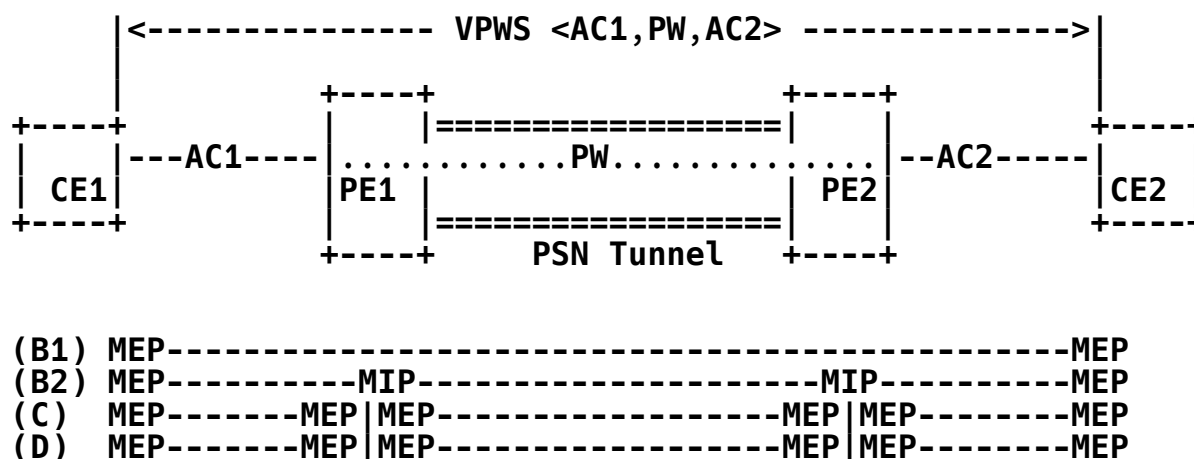may be adequate in some cases.

```
        |<--------------------- 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 and MIPs

6.2.4. 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 to the VPWS instance and in the context of their
   corresponding OAM domains.

7. VPLS OAM Requirements

   These requirements are applicable to VPLS PE offering VPLS as an
   Ethernet Bridged LAN service, as described in Section 5.1.1.
   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, they 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 VPLS-aware device to learn about other devices
   that support the same VPLS instance within a given domain.

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

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

7.2. Connectivity Fault Management

   VPLS is realized by exchanging service frames/packets between devices
   that support the same VPLS 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, proactive connectivity monitoring is required.
   Connectivity monitoring facilitates connectivity fault detection.

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

7.2.2. 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-aware devices that support the same VPLS instance within a given
   OAM domain.

7.2.3. Connectivity Fault Localization

   Further, localization of connectivity fault may be carried out.

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

7.2.4. Connectivity Fault Notification and Alarm Suppression

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

   However, a single transport/network fault may cause multiple services
   to fail simultaneously, thereby 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.

7.3. Frame Loss

   A VPLS may be considered degraded if service-layer frames/packets are
   lost during transit between the VPLS-aware devices. To determine if
   a VPLS 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-aware devices that support the same VPLS
   instance within a given OAM domain.

7.4. Frame Delay

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

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

   1) 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 the two
       devices in question.

   2) Two-way delay or round-trip delay does not require clock
       synchronization between the 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-aware devices that support the
   same VPLS instance within a given OAM domain.

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

7.5. Frame Delay Variation

   A VPLS may be sensitive to delay variation experienced by the VPLS
   frames/packets during transit between the VPLS-aware devices. To
   determine if a VPLS 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-aware devices that support the same
   VPLS 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 VPLS OAM frames flow across a different path than the one used
   by VPLS 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 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 frames.

7.8. 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 instances, e.g., premium VPLS instances, and may not be used for
best-effort VPLSs.

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

7.9. Extensibility

Extensibility is intended to allow introduction of additional OAM
functionality in the 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 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 data frames/packets.

(R8a) VPLS OAM MUST be extensible such that new functionality and
information elements related to this functionality can be introduced
in the 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 data frames/packets.

7.10. 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 the same level or to a 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 to a 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 a
higher-level OAM domain.

7.11. Transport Independence

VPLS 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 layer.

7.12. Application Independence

VPLS 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 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.

8. 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, they 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.

8.1. Discovery

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

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

8.2. Connectivity Fault Management

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

8.2.1. Connectivity Fault Detection

To ensure service, proactive connectivity monitoring is required.
Connectivity monitoring facilitates connectivity fault detection.

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

(R13b) VPWS OAM mechanism SHOULD allow detection of mis-branching or
mis-connections.

8.2.2. 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-aware devices that support the same VPWS instance within a
given OAM domain.

8.2.3. 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-aware devices that support the same VPWS instance within a
   given OAM domain.

8.2.4. Connectivity Fault Notification and Alarm Suppression

   Typically, when a connectivity fault is detected and optionally
   verified, the 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 the local CE and the local PE,
   which are connected via the 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 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.

8.3. Frame Loss

   A VPWS may be considered degraded if service-layer frames/packets are
   lost during transit between the VPWS-aware devices. To determine if
   a VPWS 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-aware devices that support the same VPWS
   instance within a given OAM domain.

8.4. Frame Delay

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

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

1) 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 the two
   devices in question.

2) Two-way delay or round-trip delay does not require clock
   synchronization between the 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-aware devices that support the
same VPWS instance within a given OAM domain.

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

8.5. Frame Delay Variation

A VPWS may be sensitive to delay variation experienced by the VPWS
frames/packets during transit between the VPWS-aware devices. To
determine if a VPWS 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-aware devices that support the same
VPWS instance within a given OAM domain.

8.6. 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.

8.7. Data Path Forwarding

If the VPWS OAM frames flow across a different path than the one used by VPWS 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 frames/packets, must be used for the VPWS OAM.

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

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

8.8. 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 instances, e.g., premium VPWS 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 that is supported by the device.

8.9. Extensibility

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

(R19a) VPWS OAM MUST be extensible such that new functionality and information elements related to this functionality can be introduced in the 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 data frames/packets.

8.10. 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 the same level or to a
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 to a 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 a
higher-level OAM domain.

8.11. Transport Independence

VPWS 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 layer.

8.12. Application Independence

VPWS 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 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.

8.13. Prioritization

VPWS could be composed of several data flows, each related to a given usage/application with specific requirements in terms of connectivity and/or performance. 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 packets/frames.

9. VPLS (V)LAN Emulation OAM Requirements

9.1. Partial-Mesh of PWs

As indicated in [BRIDGE-INTEROP], VPLS 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 shut down when only an entire VPLS is acceptable or a subset of PWs should be shut down such that the remaining PWs have full connectivity among them when partial VPLS is acceptable.

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

(R13b) PW OAM for PWs related to a (V)LAN emulation MUST allow the entire mesh of PWs to be shut down 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 shut down 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.

9.2. PW Fault Recovery

As indicated in [BRIDGE-INTEROP], VPLS 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 fault detection and recovery time to prevent unnecessary switch-over and temporary flooding/loop within the customer OAM domain that is dual-homed to the 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.

9.3. Connectivity Fault Notification and Alarm Suppression

When a 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 a connectivity fault in VPLS 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 OAM.

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

10. OAM Operational Scenarios

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

10.1. 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
```
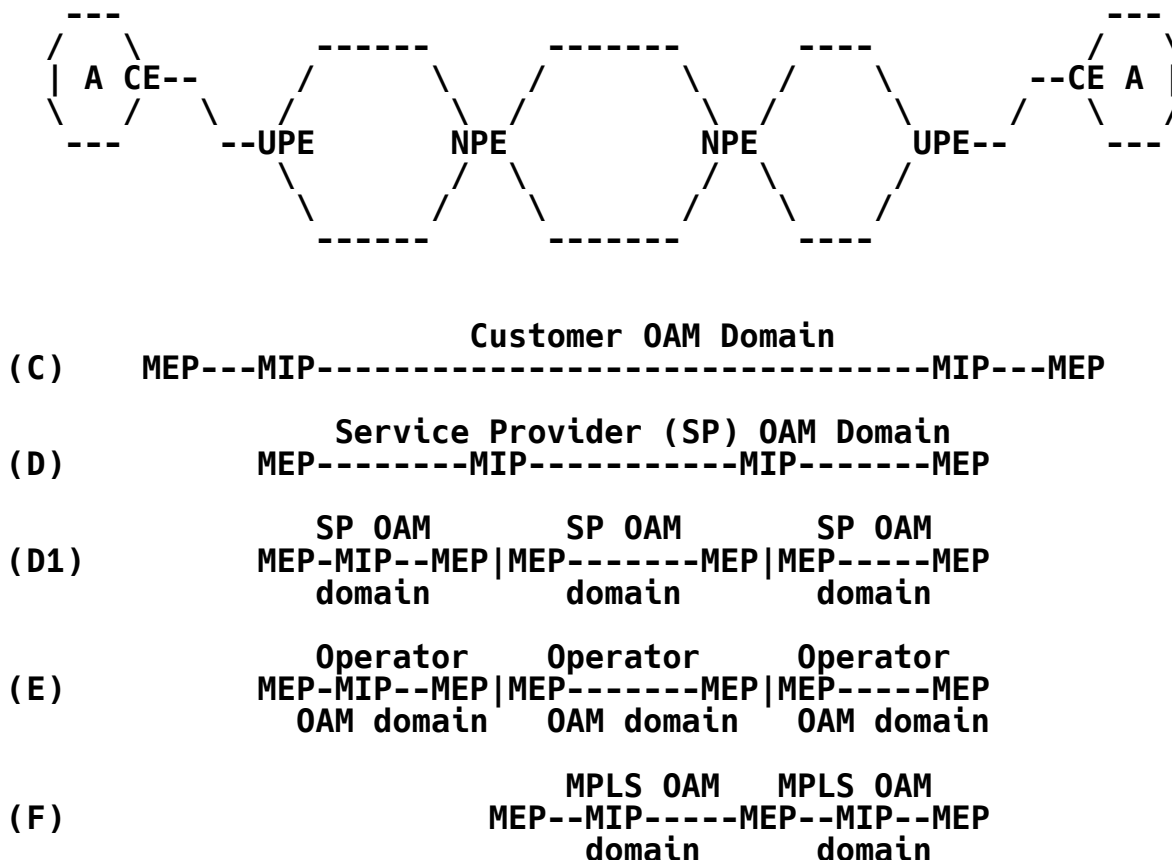
            Figure 10: VPLS OAM Domains, MEPs, and MIPs

   Among the different MEs identified in Figure 5 for VPLS OAM in the
   customer OAM domain, [IEEE802.1ag] and [Y.1731] Ethernet OAM
   mechanisms can be applied to meet the various requirements identified
   in Section 7. The mechanisms can be applied across (C) in Figure 10
   MEs.

   Similarly, inside the service provider OAM domain, [IEEE802.1ag] and
   [Y.1731] Ethernet OAM mechanisms can be applied across (D) MEs in
   Figure 10 to meet the functional requirements identified in Section
   7.

   It may be noted that in the interim, when [IEEE802.1ag] and [Y.1731]
   capabilities are not available across the PE devices, the Fault
   Management option using segment OAM introduced in Section 6.2.3 can
   be applied, with the limitations cited below. In this option, the
   service provider can run segment OAM across the (D1) MEs in Figure

10. The OAM mechanisms across the (D1) MEs in Figure 10 can be non-
Ethernet, e.g., Virtual Circuit Connectivity Verification (VCCV), or
Bidirectional Forwarding Detection (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 endpoints. However, such mechanisms do not
fully exercise the data plane forwarding constructs as experienced by
native (i.e., Ethernet) service PDUs. As a result, service
monitoring ((D1) in Figure 10) is severely limited in the sense that
it may lead to an indication that the ME between VPLS endpoints is
functional while the customer may be experiencing end-to-end
connectivity issues in the data plane.

Inside the network operator OAM domain, [IEEE802.1ag] and [Y.1731]
Ethernet OAM mechanisms can also be applied across MEs in (E) in
Figure 10 to meet the functional requirements identified in Section
7. In addition, the network operator could decide to use native OAM
mechanisms, e.g., VCCV or BFD, across (F) MEs for additional
monitoring or as an alternative to monitoring across (E) MEs.

11. Security Considerations

This specification assumes that L2VPN components within the OAM
domain are mutually trusted. Based on that assumption,
confidentiality issues are fully addressed by filtering to prevent
OAM frames from leaking outside their designated OAM domain.
Similarly, authentication issues are addressed by preventing OAM
frames generated outside a given OAM domain from entering the domain
in question. Requirements to prevent OAM messages from leaking
outside an OAM domain and for OAM domains to be transparent to OAM
frames from higher OAM domains are specified in Sections 7.10 and
8.10.

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

12. Contributors

In addition to the authors listed above, the following individuals also contributed to this document.

Simon Delord
Uecomm
658 Church St
Richmond, VIC, 3121, Australia
EMail: sdelord@uecomm.com.au

Philippe Niger
France Telecom
2 av. Pierre Marzin
22300 LANNION, France
EMail: philippe.niger@francetelecom.com

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

13. Acknowledgements

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

The 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.

14. References

14.1. Normative References

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

[IEEE802.1ad]   "IEEE Standard for Local and metropolitan area
                 networks - Virtual Bridged Local Area Networks,
                 Amendment 4: Provider Bridges", 2005.

[IEEE802.1ag]   "IEEE Standard for Local and metropolitan area
                 networks - Virtual Bridged Local Area Networks,
                 Amendment 5: Connectivity Fault Management", 2007.

   [IEEE802.1ah]   "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]   Andersson, L., Ed., and E. Rosen, Ed., "Framework
                     for Layer 2 Virtual Private Networks (L2VPNs)", RFC
                     4664, September 2006.

   [L2VPN-REQ]   Augustyn, W., Ed., and Y. Serbest, Ed., "Service
                     Requirements for Layer 2 Provider-Provisioned
                     Virtual Private Networks", RFC 4665, September 2006.

   [L2VPN-TERM]   Andersson, L. and T. Madsen, "Provider Provisioned
                     Virtual Private Network (VPN) Terminology", RFC
                     4026, March 2005.

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

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

   [VPLS-BGP]   Kompella, K., Ed., and Y. Rekhter, Ed., "Virtual
                     Private LAN Service (VPLS) Using BGP for Auto-
                     Discovery and Signaling", RFC 4761, January 2007.

   [VPLS-LDP]   Lasserre, M., Ed., and V. Kompella, Ed., "Virtual
                     Private LAN Service (VPLS) Using Label Distribution
                     Protocol (LDP) Signaling", RFC 4762, January 2007.

14.2. Informative References

   [BRIDGE-INTEROP] Sajassi, A. Ed., Brockners, F., Mohan, D., Ed., and
                     Y. Serbest, "VPLS Interoperability with CE Bridges",
                     Work in Progress, October 2010.

   [L2VPN-SIG]   Rosen, E., Davie, B., Radoaca, V., and W. Luo,
                     "Provisioning, Auto-Discovery, and Signaling in
                     Layer 2 Virtual Private Networks (L2VPNs)", RFC
                     6074, January 2011.

   [MS-PW-Arch]   Bocci, M. and S. Bryant, "An Architecture for Multi-
                     Segment Pseudowire Emulation Edge-to-Edge", RFC
                     5659, October 2009.

   [RFC2544]   Bradner, S. and J. McQuaid, "Benchmarking
                        Methodology for Network Interconnect Devices", RFC
                        2544, March 1999.

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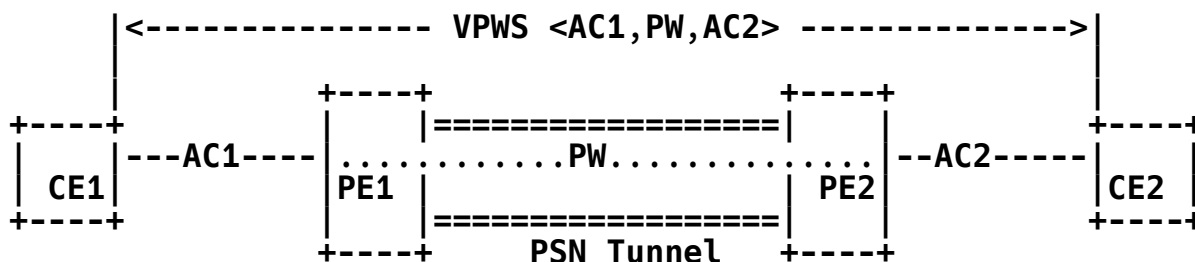
   In consideration of the management models that can be deployed
   besides the hierarchical models elaborated in this document, this
   appendix highlights some alternate models that are not recommended
   due to their limitations, as pointed out below. These alternatives
   have been highlighted as potential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

A.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, as
   shown in (B) in Figure A.1. 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 (D) in Figure A.1.

   The advantage of this option is that VPWS monitoring is limited to
   CEs. The limitation of this option is that the localization of
   faults is at the VPWS 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 A.1: VPWS MEPs and MIPs (Minimal OAM)
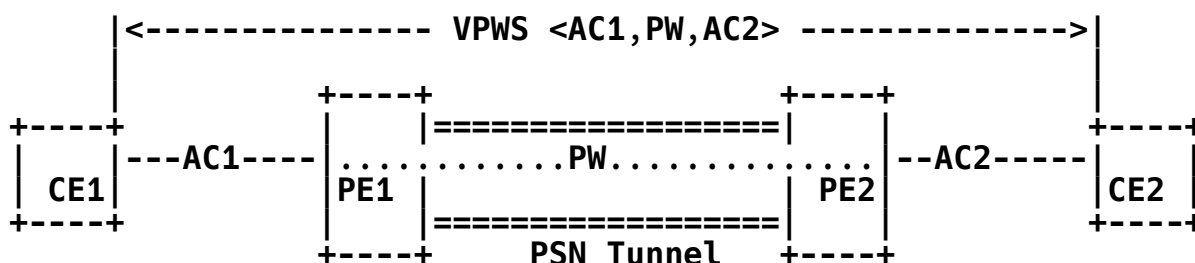
A.2. Alternate Model 2 (Segment OAM Interworking)

   In this model, end-to-end service monitoring is provided by
   interworking OAM across each segment. Typical segments involved in
   this case include two AC MEs and a PW ME, as shown in (C) in Figure
   A.2. 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 (C) in Figure A.2. Network operators may run segment OAM by having MEPs at the network operator OAM level, as shown in (D) in Figure A.2.

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 others. 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 A.2: VPWS MEPs and MIPs (Segment OAM Interworking)

Authors' Addresses

   Ali Sajassi (editor)
   Cisco Systems, Inc.
   170 West Tasman Drive
   San Jose, CA 95134
   USA
   EMail: sajassi@cisco.com

   Dinesh Mohan (editor)
   Nortel
   Ottawa, ON K2K3E5
   EMail: dinmohan@hotmail.com