Internet Draft Document
Provider Provisioned VPN Working Group
draft-lasserre-vkompella-ppvpn-vpls-02.txt

Marc Lasserre
Riverstone Networks
Vach Kompella
Nick Tingle
Sunil Khandekar
Timetra Networks

Ali Sajassi
Cisco Systems

Pascal Menezes
Terabeam

Loa Andersson
Utfors

Andrew Smith
Consultant

Pierre Lin
Yipes Communication

Juha Heinanen
Song Networks

Giles Heron
PacketExchange Ltd.

Ron Haberman
Masergy, Inc.

Tom S.C. Soon
Yetik Serbest
Eric Puetz
SBC Communications

Nick Slabakov
Rob Nath
Riverstone Networks

Luca Martini
Level 3
Communications

Vasile Radaoca
Nortel Networks

Expires: January 2003
June 2002

Virtual Private LAN Services over MPLS
draft-lasserre-vkompella-ppvpn-vpls-02.txt

1. Status of this Memo

2. Abstract

This document describes a virtual private LAN service (VPLS) solution over MPLS, also known as Transparent LAN Services (TLS). VPLS simulates an Ethernet virtual 802.1D bridge [802.1D-ORIG] [802.1D-REV] for a given set of users. It delivers a layer 2 broadcast domain that is fully capable of learning and forwarding on Ethernet MAC addresses that is closed to a given set of users. Many VLS services can be supported from a single PE node.

3. Conventions

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

Placement of this Memo in Sub-IP Area

RELATED DOCUMENTS

http:// search.ietf.org/internet-drafts/draft-martini-l2circuit-trans-mpls-06.txt

http://search.ietf.org/internet-drafts/draft-martini-l2circuit-encap-mpls-02.txt

http://search.ietf.org/internet-drafts/draft-augustyn-ppvpn-vpls-reqmts-00.txt

WHERE DOES THIS FIT IN THE PICTURE OF THE SUB-IP WORK

PPVPN

WHY IS IT TARGETTED AT THIS WG

The charter of the PPVPN WG includes L2 VPN services and this draft specifies a model for Ethernet L2 VPN services over MPLS.

JUSTIFICATION

Existing Internet drafts specify how to provide point-to-point Ethernet L2 VPN services over MPLS. This draft defines how multipoint Ethernet services can be provided.

4. Table of Contents

5. Overview

Ethernet has become the predominant technology for Local Area Networks (LANs) connectivity and is gaining acceptance as an access technology, specifically in Metropolitan and Wide Area Networks (MAN

and WAN respectively). An Ethernet port is used to connect a customer to the Provider Edge (PE) router acting as an LER. Customer traffic is subsequently mapped to a specific MPLS L2 VPN by configuring L2 FECs based upon the input port ID and/or VLAN index depending upon the VPLS service.

Broadcast and multicast services are available over traditional LANs. MPLS does not support such services currently. Sites that belong to the same broadcast domain and that are connected via an MPLS network expect broadcast, multicast and unicast traffic to be forwarded to the proper location(s). This requires MAC address learning/aging on a per LSP basis, packet replication across LSPs for multicast/broadcast traffic and for flooding of unknown unicast destination traffic.

The primary motivation behind Virtual Private LAN Services (VPLS) is to provide connectivity between geographically dispersed customer sites across MAN/WAN network(s), as if they were connected using a LAN. The intended application for the end-user can be divided into the following two categories:

- Connectivity between customer routers: LAN routing application
- Connectivity between customer Ethernet switches: LAN switching application

[MARTINI-ENCAP] defines how to carry L2 PDUs over point-to-point MPLS LSPs, called VC LSPs. Such VC LSPs can be carried across MPLS or GRE tunnels. This document describes extensions to [MARTINI-ENCAP] for transporting Ethernet/802.3 and VLAN [802.1Q] traffic across multiple sites that belong to the same L2 broadcast domain or VPLS. Note that the same model can be applied to other 802.1 technologies. It describes a simple and scalable way to offer Virtual LAN services, including the appropriate flooding of Broadcast, Multicast and unknown unicast destination traffic over MPLS, without the need for address resolution servers or other external servers, as discussed in [VPLS-REQ].

The following discussion applies to devices that serve as Label Edge Routers (LERs) on an MPLS network that is VPLS capable. The behavior of transit Label Switch Routers (LSRs) that are considered a part of MPLS network is not discussed. The MPLS network provides a number of Label Switch Paths (LSPs) that form the basis for connections between LERs attached to the same MPLS network. The resulting set of interconnected LERs forms a private MPLS VPN where each LSP is uniquely identified at each MPLS interface by a label.

6. Bridging Model for MPLS

An MPLS interface acting as a bridge must be able to flood, forward, and filter bridged frames.

```
+----+                                              +----+
+ C1 +---+      ...........................     +---| C1 |
+----+   |      .                         .     |   +----+
Site A   |   +----+                    +----+   |   Site B
         +---| PE |---- MPLS Cloud ----| PE |---+
             +----+         |          +----+
                .           |             .
                .         +----+          .
                ..........| PE |...........
                          +----+         ^
                            |            |
                            |            +-- Logical bridge
                          +----+
                          | C1 |
                          +----+
                          Site C
```

The set of PE devices interconnected via transport tunnels appears as a single 802.1D bridge/switch to customer C1. Each PE device will learn remote MAC addresses to VC LSP associations and learns directly attached MAC addresses on customer facing ports.

We note here that while this document shows specific examples using MPLS transport tunnels, other tunnels that can be used by pseudo-wires, e.g., GRE, L2TP, IPSEC, etc., can also be used, as long as the originating PE can be identified, since this is used in the MAC learning process.

The scope of the VPLS lies within the PEs in the service provider network, highlighting the fact that apart from customer service delineation, the form of access to a customer site is not relevant to the VPLS [VPLS-REQ].

The PE device is typically an edge router capable of running a signaling protocol and/or routing protocols to exchange VC label information. In addition, it is capable of setting up transport tunnels to other PEs to deliver VC LSP traffic.

6.1. Flooding and Forwarding

One of attributes of an Ethernet service is that all broadcast and destination unknown MAC addresses are flooded to all ports. To achieve flooding within the service provider network, all address unknown unicast, broadcast and multicast frames are flooded over the corresponding pseudowires to all relevant PE nodes participating in the VPLS. In the MPLS environment this means sending the PDU through each relevant VC LSP.

Note that multicast frames are a special case and do not necessarily have to be sent to all VPN members. For simplicity, the default approach of broadcasting multicast frames can be used. Extensions explaining how to interact with 802.1 GMRP protocol, IGMP snooping and static MAC multicast filters will be discussed in a future revision if it is needed.

To forward a frame, a PE must be able to associate a destination MAC address with a VC LSP. It is unreasonable and perhaps impossible to require PEs to statically configure an association of every possible destination MAC address with a VC LSP. Therefore, VPLS-capable PEs must have the capability to dynamically learn MAC addresses on both physical ports and virtual circuits and to forward and replicate packets across both physical ports and virtual circuits.

6.2. Address Learning

Unlike BGP VPNs [BGP-VPN], reachability information does not need to be advertised and distributed via a control plane. Reachability is obtained by standard learning bridge functions in the data plane.

As discussed previously, a pseudowire consists of a pair of uni-directional VC LSPs. When a new MAC address is learned on an inbound VC LSP, it needs to be associated with the outbound VC LSP that is part of the same pair. The state of this logical link can be considered as up as soon as both incoming and outgoing LSPs are established. Similarly, it can be considered as down as soon as one of these two LSPs is torn down.
Standard learning, filtering and forwarding actions, as defined in [802.1D-ORIG], [802.1D-REV] and [802.1Q], are required when a logical link state changes.

6.3. LSP Topology

PE routers typically run an IGP between them, and are assumed to have the capability to establish MPLS tunnels. Tunnel LSPs are set up between PEs to aggregate traffic. VC LSPs are signaled to demultiplex the L2 encapsulated packets that traverse the tunnel LSPs.

In an Ethernet L2VPN, it becomes the responsibility of the service provider to create the loop free topology. For the sake of simplicity, we assume that the topology of a VPLS is a full mesh of tunnel and pseudowires.

6.4. Loop free L2 VPN

For simplicity, a full mesh of pseudowires is established between PEs. Ethernet bridges, unlike Frame Relay or ATM where the termination point becomes the CE node, has to examine the layer 2 fields of the packets to make a switching decision. If the frame is a destination unknown, broadcast or multicast frame the frame must be flooded.

Therefore, if the topology isn't a full mesh, the PE devices may need to forward these frames to other PEs. However, this would require the use of spanning tree protocol to form a loop free topology, that may have characteristics that are undesirable to the provider. The use of a full mesh and split-horizon forwarding obviates the need for a spanning tree protocol.

Each PE MUST create a rooted tree to every other PE router that serve the same L2 VPN. Each PE MUST support a "split-horizon" scheme in order to prevent loops, that is, a PE MUST NOT forward traffic from one pseudowire to another in the same VPN (since each PE has direct connectivity to all other PEs in the same VPN).

Note that customers are allowed to run STP such as when a customer has "back door" links used to provide redundancy in the case of a failure within the VPLS. In such a case, STP BPDUs are simply tunneled through the MPLS cloud.

6.5. LDP Based Signaling

In order to establish a full mesh of pseudowires, all PEs in a VPLS must have a full mesh of LDP sessions.

Once an LDP session has been formed between two PEs, all pseudowires are signaled over this session.

In [MARTINI-SIG], the L2 VPN information is carried in a Label Mapping message sent in downstream unsolicited mode, which contains the following VC FEC TLV. VC, C, VC Info Length, Group ID, Interface parameters are as defined in [MARTINI-SIG].

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    VC tlv     |C|         VC Type             |VC info Length |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      Group ID                                 |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        VC ID                                  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                       Interface parameters                    |
 |                              "                                |
 |                              "                                |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

This document defines a new VC type value in addition to the following values already defined in [MARTINI-SIG]:

VC Type	Description
0x0001	Frame Relay DLCI
0x0002	ATM AAL5 VCC transport
0x0003	ATM transparent cell transport
0x0004	Ethernet VLAN
0x0005	Ethernet
0x0006	HDLC
0x0007	PPP
0x8008	CEM [8]
0x0009	ATM VCC cell transport
0x000A	ATM VPC cell transport
0x000B	Ethernet VPLS

VC types 0x0004 and 0x0005 identify VC LSPs that carry VLAN tagged and untagged Ethernet traffic respectively, for point-to-point connectivity.

We define a new VC type, Ethernet VPLS, with codepoint 0x000B to identify VC LSPs that carry Ethernet traffic for multipoint connectivity. The Ethernet VC Type is described below.
For VC types 0x0001 to 0x000A, The VC ID identifies a particular VC. For the VPLS VC type, the VC ID is a VPN identifier globally unique within a service provider domain.

Note that the VCID as specified in [MARTINI_SIG] is a service identifier, identifying a service emulating a point-to-point virtual circuit. In a VPLS, the VCID is a single service identifier, identifying an emulated LAN segment.

The use of the VCID as the VPN-id creates some challenges for inter-provider VPLS service and this issue will be addressed in the future revision.

6.6. Ethernet VPLS VC Type
6.6.1. VPLS Encapsulation actions

In a VPLS, a customer Ethernet packet without preamble is encapsulated with a header as defined in [MARTINI-ENCAP]. A customer Ethernet packet is defined as follows:

- If the packet, as it arrives at the PE, has an encapsulation that is used by the local PE as a service delimiter, then that encapsulation is stripped before the packet is sent into the VPLS. As the packet exits the VPLS, the packet may have a service-delimiting encapsulation inserted.

- If the packet, as it arrives at the PE, has an encapsulation that is not service delimiting, then it is a customer packet whose encapsulation should not be modified by the VPLS. This covers, for example, a packet that carries customer specific VLAN-Ids that the service provider neither knows about nor wants to modify.

By following the above rules, the Ethernet packet that traverses a VPLS is always a customer Ethernet packet. Note that the two actions, at ingress and egress, of dealing with service delimiters are local actions that neither PE has to signal to the other. They allow, for example, a mix-and-match of VLAN tagged and untagged services at either end, and do not carry across a VPLS a VLAN tag that may have only local significance. The service delimiter may be a VC label also, whereby an Ethernet VC given by [MARTINI-ENCAP] can serve as the access side connection into a PE. An RFC1483 PVC encapsulation could be another service delimiter. By limiting the scope of locally significant encapsulations to the edge, hierarchical VPLS models can be developed that provide the capability to network-engineer VPLS deployments, as described below.

6.6.2. VPLS Learning actions

Learning is done based on the customer Ethernet packet, as defined above. The Forwarding Information Base (FIB) keeps track of the mapping of customer Ethernet packet addressing and the appropriate pseudowire to use. We define two modes of learning: qualified and unqualified learning.

In unqualified learning, all the customer VLANs are handled by a single VPLS, which means they all share a single broadcast domain and a single MAC address space. This means that MAC addresses need to be unique and non-overlapping among customer VLANs or else they cannot be differentiated within the VPLS instance and this can result in loss of customer frames. An application of unqualified learning is port-based VPLS service for a given customer (e.g., customer with non-multiplexed UNI interface where the entire traffic is mapped to a single VPLS instance).

In qualified learning, each customer VLAN is assigned to its own VPLS instance, which means each customer VLAN has its own broadcast domain and MAC address space. Therefore, in qualified learning, MAC addresses among customer VLANs may overlap with each other, but they will be handled correctly since each customer VLAN has its own FIB , i.e., each customer VLAN has its own MAC address space. Since VPLS broadcasts multicast frames, qualified learning offers the advantage of limiting the broadcast scope to a given customer VLAN.

7. MAC Address Withdrawal

It MAY be desirable to remove or relearn MAC addresses that have been dynamically learned for faster convergence.

We introduce an optional MAC TLV that is used to specify a list of MAC addresses that can be removed or relearned using the Address Withdraw Message.

The Address Withdraw message with MAC TLVs MAY be supported in order to expedite learning of MAC addresses as the result of a topology change (e.g., failure of the primary link for a dual-homed MTU-s). If a notification message is sent on the backup link (blocked link), which has transitioned into an active state (e.g., similar to Topology Change Notification message of 802.1w RSTP), with a list of MAC entries to be relearned, the PE will update the MAC entries in its FIB for that VPLS instance and send the message to other PEs over the corresponding directed LDP sessions.

If the notification message contains an empty list, this tells the receiving PE to remove all the MAC addresses learned for the specified VPLS instance except the ones it learned from the sending PE (MAC address removal is required for all VPLS instances that are affected). Note that the definition of such a notification message is outside the scope of the document, unless it happens to come from an MTU connected to the PE as a spoke. In such a scenario, the message will be just an Address Withdraw message as noted above.

7.1. MAC TLV

MAC addresses to be relearned can be signaled using an LDP Address Withdraw Message that contains a new TLV, the MAC TLV. Its format is described below. The encoding of a MAC TLV address is the 6-byte MAC address specified by IEEE 802 documents [g-ORIG] [802.1D-REV].

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |U|F|       Type                |            Length             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      MAC address #1                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                               |      MAC address #2           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                      MAC address #2                           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                              ...                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

U bit
     Unknown bit. This bit MUST be set to 0. If the MAC address format is not understood, then the TLV is not understood, and MUST

be ignored.

F bit
Forward bit. This bit MUST be set to 0. Since the LDP mechanism used here is Targeted, the TLV MUST NOT be forwarded.

Type
Type field. This field MUST be set to 0x0404 (subject to IANA approval). This identifies the TLV type as MAC TLV.

Length
Length field. This field specifies the total length of the TLV, including the Type and Length fields.

MAC Address
The MAC address being removed.

The LDP Address Withdraw Message contains a FEC TLV (to identify the VPLS in consideration), a MAC Address TLV and optional parameters. No optional parameters have been defined for the MAC Address Withdraw signaling.

7.2. Address Withdraw Message Containing MAC TLV

When MAC addresses are being removed or relearned explicitly, e.g., the primary link of a dual-homed MTU-s has failed, an Address Withdraw Message can be sent with the list of MAC addresses to be relearned.

The processing for MAC TLVs received in an Address Withdraw Message is:

For each MAC address in the TLV:

- Relearn the association between the MAC address and the interface/pseudowire over which this message is received
- Send the same message to all other PEs over the corresponding directed LDP sessions.

For an Address Withdraw message with empty list:

- Remove all the MAC addresses associated with the VPLS instance (specified by the FEC TLV) except the MAC addresses learned over this link (over the pseudowire associated with the signaling link over which the message is received)
- Send the same message to all other PEs over the corresponding directed LDP sessions.

The scope of a MAC TLV is the VPLS specified in the FEC TLV in the Address Withdraw Message. The number of MAC addresses can be deduced from the length field in the TLV.

Further descriptions of how to deal with failures expeditiously with different configurations will be described in other documents, such as [FINN-BRIDGING].

8. Operation of a VPLS

We show here an example of how a VPLS works. The following discussion uses the figure below, where a VPLS has been set up between PE1, PE2 and PE3.

Initially, the VPLS is set up so that PE1, PE2 and PE3 have a full-mesh of tunnels between them for carrying tunneled traffic. The VPLS instance is assigned a VCID (a 32-bit quantity that is unique across the provider network across all VPLSs). (Allocation of domain-wide unique VCIDs is outside the scope of this draft).

For the above example, say PE1 signals VC Label 102 to PE2 and 103 to PE3, and PE2 signals VC Label 201 to PE1 and 203 to PE3.

Assume a packet from A1 is bound for A2. When it leaves CE1, say it has a source MAC address of M1 and a destination MAC of M2. If PE1 does not know where M2 is, it will multicast the packet to PE2 and PE3. When PE2 receives the packet, it will have an inner label of 201. **PE2 can conclude that the source MAC address M1 is behind PE1,** since it distributed the label 201 to PE1. It can therefore associate MAC address M1 with VC Label 102.

```
                                                      -----
                                                     /  A1 \
        ----                                    ----CE1    |
       /    \          --------       -------  /     |     |
       | A2 CE2-      /        \     /      PE1     \     /
       \    /   \    /          \---/         \       -----
        ----     ---PE2                        |
                    | Service Provider Network |
                     \          /   \         /
              -----  PE3       /     \       /
              |Agg|_/  --------       -------
             -|   |
      ----  / -----  ----
     /    \/    \   /    \                 CE = Customer Edge Router
     | A3 CE3    --C4 A4 |                 PE = Provider Edge Router
     \    /         \    /                 Agg = Layer 2 Aggregation
      ----           ----
```

8.1. MAC Address Aging

PEs that learn remote MAC addresses need to have an aging mechanism to remove unused entries associated with a VC Label. This is important both for conservation of memory as well as for administrative purposes. For example, if a customer site A is shut down, eventually, the other PEs should unlearn A's MAC address.

As packets arrive, MAC addresses are remembered. The aging timer for MAC address M SHOULD be reset when a packet is received with source MAC address M.

9. A Hierarchical VPLS Model

The solution described above requires a full mesh of tunnel LSPs between all the PE routers that participate in the VPLS service. For each VPLS service, n*(n-1) VCs must be setup between the PE routers. While this creates signaling overhead, the real detriment to large scale deployment is the packet replication requirements for each provisioned VCs on a PE router. Hierarchical connectivity, described in this document reduces signaling and replication overhead to allow large scale deployment.

In many cases, service providers place smaller edge devices in multi-tenant buildings and aggregate them into a PE device in a large Central Office (CO) facility. In some instances, standard IEEE 802.1q (Dot 1Q) tagging techniques may be used to facilitate mapping CE interfaces to PE VPLS access points.

It is often beneficial to extend the VPLS service tunneling techniques into the MTU domain. This can be accomplished by treating the MTU device as a PE device and provisioning VCs between it and every other edge, as an basic VPLS. An alternative is to utilize [MARTINI-ENCAP] VCs or Q-in-Q VCs between the MTU and selected VPLS enabled PE routers. Q-in-Q encapsulation is another form of L2 tunneling technique, which can be used in conjunction with MPLS signaling as will be described later. This section focuses on this alternative approach. The [VPLS] mesh core tier VCs (Hub) are augmented with access tier VCs (Spoke) to form a two tier hierarchical VPLS (H-VPLS).

Spoke VCs may include any L2 tunneling mechanism, expanding the scope of the first tier to include non-bridging VPLS PE routers. The non-bridging PE router would extend a Spoke VC from a Layer-2 switch that connects to it, through the service core network, to a bridging VPLS PE router supporting Hub VCs. We also describe how VPLS-challenged nodes and low-end CEs without MPLS capabilities may participate in a hierarchical VPLS.

9.1. Hierarchical connectivity

This section describes the hub and spoke connectivity model and describes the requirements of the bridging capable and non-bridging MTU devices for supporting the spoke connections.

For rest of this discussion we will refer to a bridging capable MTU device as MTU-s and a non-bridging capable PE device as PE-r. A routing and bridging capable device will be referred to as PE-rs.

9.1.1. Spoke connectivity for bridging-capable devices

As shown in the figure below, consider the case where an MTU-s device has a single connection to the PE-rs device placed in the CO. The PE-rs devices are connected in a basic VPLS full mesh. To participate in the VPLS service, MTU-s device creates a single point-to-point tunnel LSP to the PE-rs device in the CO. We will call this the spoke connection. For each VPLS service, a single spoke pseudowire is setup between the MTU-s and the PE-rs based on [MARTINI-SIG] or its extension [SINGLE-SIDED]. Unlike traditional pseudowires that terminate on a physical (or a VLAN-tagged logical) port at each end, the spoke VC terminates on a virtual bridge instance on the MTU-s and the PE-rs devices.

```
                                                        PE2-rs
                                                        ------
                                                       /      \
                                                      |   --   |
                                                      |  /  \  |
 CE-1                                                 |  \B /  |
  \                                                    \  --  /
   \                                                   /------
    \   MTU-s                         PE1-rs          /   |
     \ ------                         ------         /    |
      /      \                       /      \       /     |
     | \ --   |      VC-1           |   --   |---/      |
     |  /  \--|- - - - - - - - - - -|--/  \  |          |
     |  \B /  |                     |  \B /  |          |
      \ /--  /                       \  --  / ---\      |
       /-----                         ------      \     |
      /                                            \    |
    ----                                            \ ------
   |Agg |                                            /      \
    ----                                            |  --    |
   /    \                                           | /  \   |
  CE-2  CE-3                                        | \B /   |
                                                     \ --   /
 MTU-s = Bridging capable MTU                         ------
 PE-rs = VPLS capable PE                              PE3-rs

 --
/  \
\B / = Virtual VPLS(Bridge)Instance
 --
 Agg = Layer-2 Aggregation
```

The MTU-s device and the PE-rs device treat each spoke connection like an access port of the VPLS service. On access ports, the combination of the physical port and/or the VLAN tag is used to associate the traffic to a VPLS instance while the pseudowire tag (e.g., VC label) is used to associate the traffic from the virtual spoke port with a VPLS instance, followed by a standard L2 lookup to identify which customer port the frame needs to be sent to.

The signaling and association of the spoke connection to the VPLS service may be done by introducing extensions to the LDP signaling as specified in [MARTINI-SIG].

9.1.1.1. MTU-s Operation

MTU-s device is defined as a device that supports layer-2 switching functionality and does all the normal bridging functions of learning and replication on all its ports, including the virtual spoke port. Packets to unknown destination are replicated to all ports in the service including the virtual spoke port. Once the MAC address is learned, traffic between CE1 and CE2 will be switched locally by the MTU-s device saving the link capacity of the connection to the PE-rs. Similarly traffic between CE1 or CE2 and any remote destination is switched directly on to the spoke connection and sent to the PE-rs over the point-to-point pseudowire.

Since the MTU-s is bridging capable, only a single pseudowire is required per VPLS instance for any number of access connections in the same VPLS service. This further reduces the signaling overhead between the MTU-s and PE-rs.

If the MTU-s is directly connected to the PE-rs, other encapsulation techniques such as Q-in-Q can be used for the spoke connection pseudowire. However, to maintain a uniform end-to-end control plane based on MPLS signaling, [MARTINI-SIG] can be used for distribution of pseudowire tags (e.g., Q-in-Q tags or VC labels) between MTU-s and PE-rs

9.1.1.2. PE-rs Operation

The PE-rs device is a device that supports all the bridging functions for VPLS service and supports the routing and MPLS encapsulation, i.e. it supports all the functions described in [VPLS].   The operation on the PE-rs node is identical to that described in [VPLS] with one addition. A point-to-point VC associated with the VPLS is regarded as a virtual port (see discussion in Section 5.6.1 on service delimiting). The operation on the virtual spoke port is identical to the operation on an access port as described in the earlier section. As shown in the figure above, each PE-rs device switches traffic between aggregated access VCs that look like virtual ports and the network side VPLS VCs.

9.1.2. Advantages of spoke connectivity

Spoke connectivity offers several scaling and operational advantages for creating large scale VPLS implementations, while retaining the ability to offer all the functionality of the VPLS service.

- Eliminates the need for a full mesh of tunnels and full mesh of VCs per service between all devices participating in the VPLS service.
- Minimizes signaling overhead since fewer VC-LSPs are required for the VPLS service.
- Segments VPLS nodal discovery. MTU-s needs to be aware of only the PE-rs node although it is participating in the VPLS service that spans multiple devices. On the other hand, every VPLS PE-rs must be aware of every other VPLS PE-rs device and all of it s locally connected MTU-s and PE-r.
- Addition of other sites requires configuration of the new MTU-s device but does not require any provisioning of the existing MTU-s devices on that service.
- Hierarchical connections can be used to create VPLS service that spans multiple service provider domains. This is explained in a later section.

9.1.3. Spoke connectivity for non-bridging devices

In some cases, a bridging PE-rs device may not be deployed in a CO or a multi-tenant building while a PE-r might already be deployed. If there is a need to provide VPLS service from the CO where the PE-rs device is not available, the service provider may prefer to use the PE-r device in the interim. In this section, we explain how a PE-r device that does not support any of the VPLS bridging functionality can participate in the VPLS service.

As shown in this figure, the PE-r device creates a point-to-point tunnel LSP to a PE-rs device. Then for every access port that needs to participate in a VPLS service, the PE-r device creates a point-to-point [MARTINI-ENCAP] VC that terminates on the physical port at the PE-r and terminates on the virtual bridge instance of the VPLS service at the PE-rs.

```
                                                       PE2-rs
                                                       ------
                                                      /      \
                                                     |   --   |
                                                     |  /  \  |
 CE-1                                                |  \B /  |
  \                                                   \  --  /
   \                                                  /------
    \   PE-r                           PE1-rs        /   |
     \ ------                          ------       /    |
      /      \                        /      \     /     |
     | \      |      VC-1           |   --   |---/      |
     |  ------|- - - - - - - - - - - |--/  \  |          |
     |   -----|- - - - - - - - - - - |--\B /  |          |
      \ /    /                        \  --  / ---\      |
       ------                          ------      \     |
      /                                             \    |
    ----                                             \------
   | Agg|                                            /      \
    ----                                            |  --    |
   /    \                                           | /  \   |
  CE-2  CE-3                                        | \B /   |
                                                     \ --   /
 PE-r = Non-Bridging PE (router)                      ------
 PE-rs = VPLS capable PE                               PE3-rs

 --
/  \
\B / = Virtual VPLS(Bridge)Instance
 --
 Agg = Layer-2 Aggregation
```

9.1.3.1. PE-r Operation

The PE-r device is defined as a device that supports routing but does not support any bridging functions. However, it is capable of setting up [Martini-Encap] VCs between itself and the PE-rs. For every port that is supported in the VPLS service, a [MARTINI-ENCAP] VC is setup from the PE-r to the PE-rs. Once the VCs are setup, there is no learning or replication function required on part of the PE-r. All traffic received on any of the access ports is transmitted on the VC. Similarly all traffic received on a VC is transmitted to the access port where the VC terminates. Thus traffic from CE1 destined for CE2 is switched at PE-rs and not at PE-r.

This approach adds more overhead than the bridging capable (MTU-s) spoke approach since a VC is required for every access port that participates in the service versus a single VC required per service (regardless of access ports) when a MTU-s type device is used.

However, this approach offers the advantage of offering a VPLS service in conjunction with a routed internet service without requiring the addition of new MTU device.

9.1.3.2. PE-rs Operation

The operation of PE-rs is independent of the type of device at the other end of the spoke connection. Whether there is a bridging capable device (MTU-s) at the other end of the spoke connection or there is a non-bridging device (PE-r) at the other end of the spoke connection, the operation of PE-rs is exactly the same. Thus, the spoke connection from the PE-r is treated as a virtual port and the PE-rs device switches traffic between the virtual port, access ports and the network side VPLS VCs once it has learned the MAC addresses.

9.2. Redundant Spoke Connections

An obvious weakness of the hub and spoke approach described thus far is that the MTU device has a single connection to the PE-rs device. In case of failure of the connection or the PE-rs device, the MTU device suffers total loss of connectivity.

In this section we describe how the redundant connections can be provided to avoid total loss of connectivity from the MTU device. The mechanism described is identical for both, MTU-s and PE-r type of devices

9.2.1. Dual-homed MTU device

To protect from connection failure of the VC or the failure of the PE-rs device, the MTU-s device or the PE-r is dual-homed into two PE-rs devices, as shown in figure-3. The PE-rs devices must be part of the same VPLS service instance.

An MTU-s device will setup two [MARTINI-ENCAP] VCs (one each to PE-rs1 and PE-rs2) for each VPLS instance. One of the two VC is designated as primary and is the one that is actively used under normal conditions, while the second VC is designated as secondary and is held in a standby state. The MTU device negotiates the VC-labels for both the primary and secondary VC, but does not use the secondary VC unless the primary VC fails. Since only one link is active at a given time, a loop does not exist and hence 802.1D spanning tree is not required.

```
                                                       PE2-rs
                                                       ------
                                                      /      \
                                                     |   --   |
                                                     |  /  \  |
 CE-1                                                |  \B /  |
   \                                                  \  --  /
    \                                                 /------
     \  MTU-s                          PE1-rs        /   |
      \------                          ------       /    |
      /      \                        /      \     /     |
     |   --   |   Primary VC         |   --   |---/      |
     |  /  \--|- - - - - - - - - - - |--/  \  |          |
     |  \B /  |                      |  \B /  |          |
      \  -- \/                        \  --  / ---\      |
       ------\                         ------      \     |
       /      \                                     \    |
      /        \                                     \ ------
     /          \                                     /      \
    CE-2         \                                   |  --    |
                  \     Secondary VC                 | /  \   |
                   - - - - - - - - - - - - - - - - - |-\B /   |
                                                      \ --   /
 MTU-s = Bridging capable MTU                          ------
 PE-rs = VPLS capable PE                               PE3-rs

 --
/  \
\B / = Virtual VPLS(Bridge)Instance
 --
```

9.2.2. Failure detection and recovery

The MTU-s device controls the usage of the VC links to the PE-rs nodes. Since LDP signaling is used to negotiate the VC-labels, the hello messages used for the LDP session can be used to detect failure of the primary VC.

Upon failure of the primary VC, MTU-s device immediately switches to the secondary VC. At this point the PE3-rs device that terminates the secondary VC starts learning MAC addresses on the spoke VC. All other PE-rs nodes in the network think that CE-1 and CE-2 are behind PE1-rs and may continue to send traffic to PE1-rs until they learn that the devices are now behind PE3-rs. The relearning process can take a long time and may adversely affect the connectivity of higher level protocols from CE1 and CE2. To enable faster convergence, the PE3-rs device where the secondary VC got activated may send out a flush message, using the MAC TLV as defined in Section 6, to all other PE-rs devices participating in the VPLS service. Upon receiving the message, all PE-rs flush the MAC addresses associated with that VPLS instance .

9.3. Multi-domain VPLS service

Hierarchy can also be used to create a large scale VPLS service within a single domain or a service that spans multiple domains without requiring full mesh connectivity between all VPLS capable devices. Two fully meshed VPLS networks are connected together using a single LSP tunnel between the VPLS gateway devices. A single VC is setup per VPLS service to connect the two domains together. The VPLS gateway device joins two VPLS services together to form a single multi-domain VPLS service. . The requirements and functionality required from a VPLS gateway device will be explained in a future version of this document.

10. Hierarchical VPLS model using Ethernet Access Network

In the previous section, a two-tier hierarchical model that consists of hub-and-spoke topology between MTU-s devices and PE-rs devices and a full-mesh topology among PE-rs devices was discussed. In this section the two-tier hierarchical model is expanded to include an Ethernet access network. This model retains the hierarchical architecture discussed previously in that it includes MTU-s devices and PE-rs devices and also utilized a full-mesh topology among PE-rs devices. The motivation for an Ethernet access network is that Ethernet-based networks are currently deployed by some service providers to offer VPLS services to their customers. Therefore, it is important to provide a mechanism that allows these networks to integrate with an IP or MPLS core to provide scalable VPLS services. One can categorize Ethernet access networks into the following three groups:

1. Based on existing 802.1q standard (this is comparable to the situation where the customer comes ino on a VLAN-tagged port)
2. Based on an extension to the IEEE 802.1q standard that tunnels 802.1q VLANs using a service provider 802.1q tag (referred to as Q-in-Q)
3. Based on Q-in-Q tunneling with ability to distribute .1q tags using MPLS control plane

For the first category, the MTU-s and all the other nodes in the access network (excluding PE-rs devices) have standard 802.1q Ethernet switch capability. However, the PE-rs device is a VPLS-capable router as described previously.

For the second category, in addition to the functionality described in the category above, the MTU-s and the PE-rs are required to support Q-in-Q tunneling capabilities and the Ethernet nodes in between are required to handle larger data frames (to accommodate the additional encapsulation).

The third category requires the MTU-s and the PE-rs to support LDP signaling for the distribution of Q-in-Q tags (i.e., MTU-s and PE-rs to have MPLS signaling capability, without MPLS encapsulation) in addition to the functionality described in categories 1 and 2 described above. Single-sided signaling [SINGLE-SIDED] may be used to distribute Q-in-Q tags.

It should be noted that since the Ethernet access network can have any arbitrary topology, standard 802.1D Spanning Tree Protocol (STP) may be required for loop detection and prevention. However, the use of spanning tree is topology dependent and may or may not be required.

The connectivity within the service provider core is unchanged. Thus, a PE-rs may need to run STP on its Ethernet access interfaces and split-horizon on its MPLS/IP network interfaces. In a topology where MTU-s devices are directly connected to PE-rs devices, STP is not required on the access network.

The following figure shows a VPLS network and several possible ways of connecting customer CE devices to the network. As it can be seen CEs can be either connected directly to PE-rs (or PE-r) or they can be first aggregated by an MTU-s and then connected to PE-rs or they can be connected via an Ethernet Access network to the PE-rs.

```
    +-----+                                        +-------+    +-----+
    +CE1 +--+                                  +---|MTU-s |----|CE2 |
    +-----+ |    ........................      |   +-------+    +-----+
    VPLS A  |  +-------+              +-------+ |      |        VPLS A
            +--| PE-rs|-- Service ----|PE-rs |-+      |       +-----+
               +-------+   Provider    +-------+       +--------|CE2'|
               / .        Backbone    . \                      +-----+
              /  .          |          .  \      +------+      VPLS B
    +-----+   /   .          |          .   \    / Ether \
    +CE1'+--+    .          |          .    +--| Access  |
    +-----+      .       +------+      .       | Network |
    VPLS B       .........|PE-rs|........       \       /
                          +------+               +------+
                            |                       |
                            |                       |
                          +-----+                +-------+   +-----+
                          |CE3 |                |MTU-s |---|CE3'|
                          +-----+                +-------+   +-----+
                          VPLS A                    |        VPLS B
                                                    |
                                                    |      +-----+
                                                    +------|CE4'|
                                                           +-----+
```

VPLS B

10.1. Port-based v.s. VLAN-based VPLS operation

Where a customer uses a port-based VPLS service, all customer traffic received from that port, regardless of whether it has vlan tags or not, is directed to a single VPLS instance. In the MTU-s, this is done by assigning a service provider VLAN (SP-VLAN) tag to that customer port. If the customer traffic is already tagged, the SP-VLAN serves as the outer tag. The SP-VLAN tag serves as a VPLS identifier which identifies a FIB associated with that particular VPLS. MAC address learning is done using unqualified learning. The customer packets are then forwarded through the FIB to the appropriate pseudowire based on the destination MAC address. In the reverse direction, the pseudowire tag identifies the VPLS instance and thus the FIB. The packet is forwarded to the proper Ethernet port based on the destination MAC address. When the packet leaves the PE-rs toward the MTU-s, it will be appended with the SP-VLAN tag associated with that VPLS.

Where a customer uses a VLAN-based VPLS service, if the traffic within each customer VLAN is to be isolated from each other and each one has its own broadcast domain, then each customer VLAN is mapped to a single VPLS instance. If the Service Provider assigns the customer VLAN tags, then the Service provider can ensure the uniqueness of these VLAN tags among different customers and a given customer VLAN tag can be used as a VPLS identifier. However, if customers assigns their own VLAN tags independently, then the MTU-s MUST map each customer VLAN into a unique SP-VLAN. Subsequently, the SP-VLAN will be used as a VPLS identifier to index the proper FIB and to forward traffic based on destination MAC address. The operation of PE-rs in this case remains same as before.

The following shows the Q-in-Q tunneling encapsulation which is applied when Ethernet data plane is used between MTU-s and PE-rs.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   MAC Dest. Address                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       MAC DA cont.            |   MAC Source Address          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        MAC SA cont.                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Ether Type = 0x8100       |      SP-VLAN          |SP .1p |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Ether Type = 0x8100       |      CE-VLAN          |CE .1p |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Ether Type / Length      |          Payload              |
```

```
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Payload                            |
 |                               "                               |
```

```
   |                              "                                |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

11. Significant Modifications

Between rev 01 and this one, the WG mailing comments and merging with draft-sajassi-vpls-architectures-00.txt led to the following changes:

- o update MAC TLV section to conform to 802.1d bridging
- o add Q-in-Q section
- o remove qualified learning
- o align with L2 framework terminology
- o clean up descriptions, typos
- o updated references

12. Acknowledgments

We wish to thank Joe Regan, Kireeti Kompella, Anoop Ghanwani, Joel Halpern, Rick Wilder,Jim Guichard, Steve Phillips, Norm Finn, and Eric Rosen for their valuable feedback.

13. Security Considerations

Security issues resulting from this draft will be discussed in greater depth at a later point. It is recommended in [RFC3036] that LDP security (authentication) methods be applied. This would prevent unauthorized participation by a PE in a VPLS. Traffic separation for a VPLS is effected by using VC labels. However, for additional levels of security, the customer MAY deploy end-to-end security, which is out of the scope of this draft.

14. Intellectual Property Considerations

This document is being submitted for use in IETF standards discussions.

15. Full Copyright Statement

copyrights defined in the Internet Standards process must be

16. References

[MARTINI-ENCAP] "Encapsulation Methods for Transport of Ethernet Frames Over IP and MPLS", draft-martini-ethernet-encap-mpls-00.txt, Work in progress, April 2002.

[MARTINI-SIG] "Transport of Layer 2 Frames Over MPLS", draft-martini-l2circuit-trans-mpls-09.txt, Work in progress, April 2002.

[802.1D-ORIG] Original 802.1D - ISO/IEC 10038, ANSI/IEEE Std 802.1D-1993 **"MAC Bridges".**

[802.1D-REV] 802.1D - "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision. This is a revision of ISO/IEC 10038: 1993, 802.1j-1992 and 802.6k-1992. It incorporates P802.11c, P802.1p and P802.12e." ISO/IEC 15802-3: 1998.

[802.1Q] 802.1Q - ANSI/IEEE Draft Standard P802.1Q/D11, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", July 1998.

[BGP-VPN] Rosen and Rekhter, "BGP/MPLS VPNs". RFC 2547, March 1999

[VPLS-REQ] "Requirements for Virtual Private LAN Services (VPLS)", draft-ietf-ppvpn-vpls-requirements-00.txt Work in progress.

[RFC3036] "LDP Specification", L. Andersson, et al. RFC 3036. January 2001.

[SINGLE-SIDED] "Single-Sided Signaling for L2VPN", draft-rosen-ppvpn-l2-signaling-01.txt, Work in Progress, February 2002.

[DIR-AUTO] "DNS/LDP Based VPLS", Juha Heinanen, draft-heinanen-dns-ldp-vpls-00.txt, Work in Progress, January 2002.

[BGP-AUTO] "Using BGP as an Auto-Discovery Mechanism for Network-based VPNs", Ould-Brahim, et. al., draft-ietf-ppvpn-bgpvpn-auto-02.txt, Work in Progress, January 2002.

[FINN-BRIDGING] "Bridging and VPLS", draft-finn-ppvpn-bridging-vpls-00.txt, Work in Progress, June 2002.

17. Authors' Addresses

Marc Lasserre
Riverstone Networks
5200 Great America Pkwy
Santa Clara, CA 95054
Email: marc@riverstonenet.com

Vach Kompella
TiMetra Networks
274 Ferguson Dr.
Mountain View, CA 94043
Email: vkompella@timetra.com

Sunil Khandekar
TiMetra Networks
274 Ferguson Dr.
Mountain View, CA 94043
Email: sunil@timetra.com

Nick Tingle
TiMetra Networks
274 Ferguson Dr.
Mountain View, CA 94043
Email: ntingle@timetra.com

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

Loa Andersson
Utfors Bredband AB
Rasundavagen 12 169 29 Solna
Email: loa.andersson@utfors.se

Pascal Menezes
Terabeam
2300 Seventh Ave
Seattle, WA 98121
Email: Pascal.Menezes@Terabeam.com

Pierre Lin

Andrew Smith
Consultant
Email: ah_smith@acm.org

Giles Heron
PacketExchange Ltd.
The Truman Brewery
91 **Brick Lane**
LONDON E1 6QL
United Kingdom
Email: giles@packetexchange.net

Juha Heinanen
Song Networks, Inc.
Email: jh@lohi.eng.song.fi

Tom S. C. Soon
SBC Technology Resources Inc.
4698 **Willow Road**
Pleasanton, CA 94588
Email: sxsoon@tri.sbc.com

Yetik Serbest
SBC Communications
9505 **Arboretum Blvd.**
Austin TX 78759
serbest@tri.sbc.com

Eric Puetz
SBC Communications
9505 **Arboretum Blvd.**
Austin TX 78759
puetz@tri.sbc.com

Ron Haberman
Masergy Inc.
2901 **Telestar Ct.**
Falls Church, VA 22042
Email: ronh@masergy.com

Luca Martini
Level 3 Communications, LLC.
1025 **Eldorado Blvd.**
Broomfield, CO, 80021
Email: luca@level3.net

Nick Slabakov
Riverstone Networks
5200 **Great America Pkwy**

Santa Clara, CA 95054
Email: nslabakov@riverstonenet.com

Rob Nath
Riverstone Networks
5200 Great America Pkwy
Santa Clara, CA 95054
Email: rnath@riverstonenet.com

Vasile Radaoca
Nortel Networks
600 Technology Park
Billerica MA 01821
Email: vasile@nortelnetworks.com