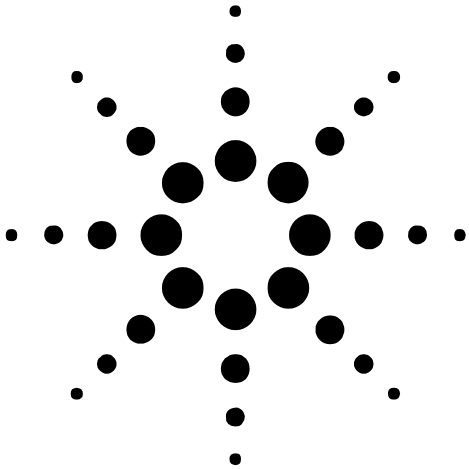

Testing Edge Services: VPLS over MPLS

White Paper

Introduction

Virtual Private LAN Services (VPLS) is an emerging technology for transparently connecting corporate LANs over the Internet so they appear and behave to customers like a single bridged Ethernet LAN. Combining the simplicity of Ethernet backbone LAN technology with the scalability and security of the MPLS core, VPLS is a viable alternative for enterprises seeking a cost-effective VPN solution. However, VPLS adds to the requirements of Provider Edge (PE) routers, and these requirements must be thoroughly tested!

This paper provides a basic understanding of how VPLS works and describes some key scenarios for testing the functionality and scalability of VPLS implementations.

Agilent Technologies

The VPLS over MPLS Story

Based on the IETF Internet draft, *Virtual Private LAN Services over MPLS* (draft-lasserre-vkompella-ppvpn-vpls-xx.txt), VPLS is a Layer-2 VPN application to connect enterprise LANs in geographically-dispersed sites over a service provider's MPLS network. This multipoint LAN-to-LAN connection is made possible through a combination of Ethernet and MPLS technologies, plus extensions to draft-martini-12circuit-trans-mpls-xx.txt, which defines the transport of Layer-2 frames over an MPLS network using point-to-point virtual circuits (VCs).

VPLS in a nutshell

Perhaps the best way to explain VPLS is to show how these three technologies fit together. Figure 1 shows a VPLS system for two customer VPNs — VPN A and VPN B — both spread out across three sites. For each VPN at each site, a Customer Edge (CE) device connects to the Provider Edge (PE) router via a point-to-point access connection.

Ethernet. On the access side, Ethernet serves as the framing technology between the CE device and the PE router in the service provider's Point of Presence (POP) or Central Office (CO). Frames can include IEEE 802.1Q Ethernet VLAN tags, which allow customers to segment their networks and assign quality of service priorities to LAN traffic. VPLS also supports "QinQ" encapsulation, where a second VLAN tag is added as a service delimiter. In fact, from the customer's perspective, the entire VPN looks like a single Ethernet LAN, with the PE acting as a bridge that switches frames on the basis of their Layer-2 destination MAC addresses.

MPLS and VPLS virtual circuits (VCs). On the provider's side, however, PEs also function as Label Edge Routers (LERs) with a full mesh of Label Switched Paths (LSPs) to all other PEs in the VPLS network. LDP or RSVP-TE is used to set up pairs of LSPs in each direction. Each PE is configured to establish a targeted LDP session (T-LDP) with every other PE in the network. This T-LDP session is used to establish virtual circuits (called VC LSPs) between each pair of customer sites in the VPN. Once all tunnel and VC LSPs are established, customer Ethernet or Ethernet VLAN frames are transported through the core network using a two-label stack. The outer LSP label directs the packet to the PE, and the inner VC label directs the packet to the CE access port or sub-interface.

Forwarding, flooding, and address learning. Like Ethernet switches, VPLS-enabled PEs dynamically learn the MAC addresses of the customer frames they process. PEs maintain a Forwarding Information Base (FIB) for each VPN and forward frames by associating a destination MAC address to a VC LSP (for traffic going into the core network), or a sub-interface or access port (for traffic coming from the core network). Broadcast frames and unicast frames with unknown destination MAC addresses are replicated and flooded across all VC LSPs or sub-interfaces/access ports.

The remainder of this section explains in more detail the provisioning, encapsulating, forwarding, and learning tasks of a VPLS-enabled PE router.

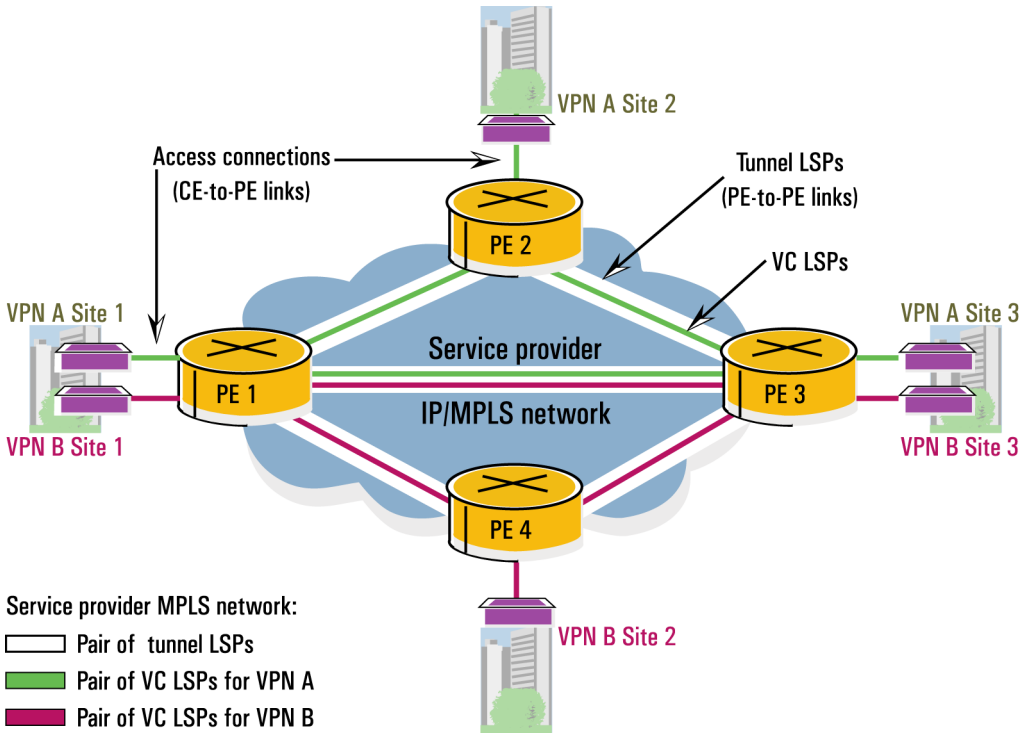

Figure 1: LAN-to-LAN interconnection with VPLS

Provisioning an MPLS-based VPLS service

Today VPLS is still an IETF work in progress. Since VPLS auto-discovery is not yet deployed, VPLS remains a manually configured service. Although tunnel LSPs are automatically created by the link LDP (or RSVP-TE) sessions, PEs must be configured to establish targeted LDP sessions and VC LSPs with other PEs in the VPLS (also called a VPLS *instance*).

VC LSPs are signaled over T-LDP sessions through the exchange of LDP Label Mapping Messages that associate a Forwarding Equivalency Class (FEC) with the VC label used by a PE for a particular VPLS instance. The FEC element within the message identifies the type of VC as "Ethernet VPLS" — a VC LSP that transports tagged or untagged Ethernet traffic for multipoint connectivity. The FEC also provides a unique VC ID to identify the customer VPN. This inner VC label allows PEs to demultiplex VCs and forward traffic to the correct CE access port or sub-interface. (It also means that a single tunnel LSP can carry VC LSPs for different customers, or multiple, differentiated VC LSPs for the same customer.) When this protocol exchange is finished, each PE is aware of its peers and knows which labels to use when sending customer traffic to any other PE in the VPLS.

Encapsulating and forwarding frames

Figure 2 shows how packets are encapsulated as they progress through a VPLS system. The CE device, which can be a switch or router, first encapsulates the traffic in Layer-2 Ethernet frames, then forwards it to the attached PE router, using either a direct physical link (e.g., Ethernet frames sent over 100BaseTX) or a logical link (e.g., Ethernet frames encapsulated in an ATM PVC, Frame Relay DLCI, or MPLS-based VC). Regardless of the access protocol used between the CE and PE, Ethernet is always the Service Protocol Data Unit in a VPLS system.

Access ingress lookup. For each incoming frame, the ingress PE strips the access header (if present), along with the Ethernet Preamble, Frame Check Sequence (FCS), and IEEE 802.1Q VLAN header, if the frame uses a VLAN tag as a service delimiter. Based on the access port on which the frame arrived plus the frame's destination MAC address and VLAN tag (if present), the PE selects the VC and tunnel LSPs, inserting the correct inner VC label and outer tunnel label. Naturally, any encapsulation required by the PE's outgoing interface is also added (not shown in illustration).

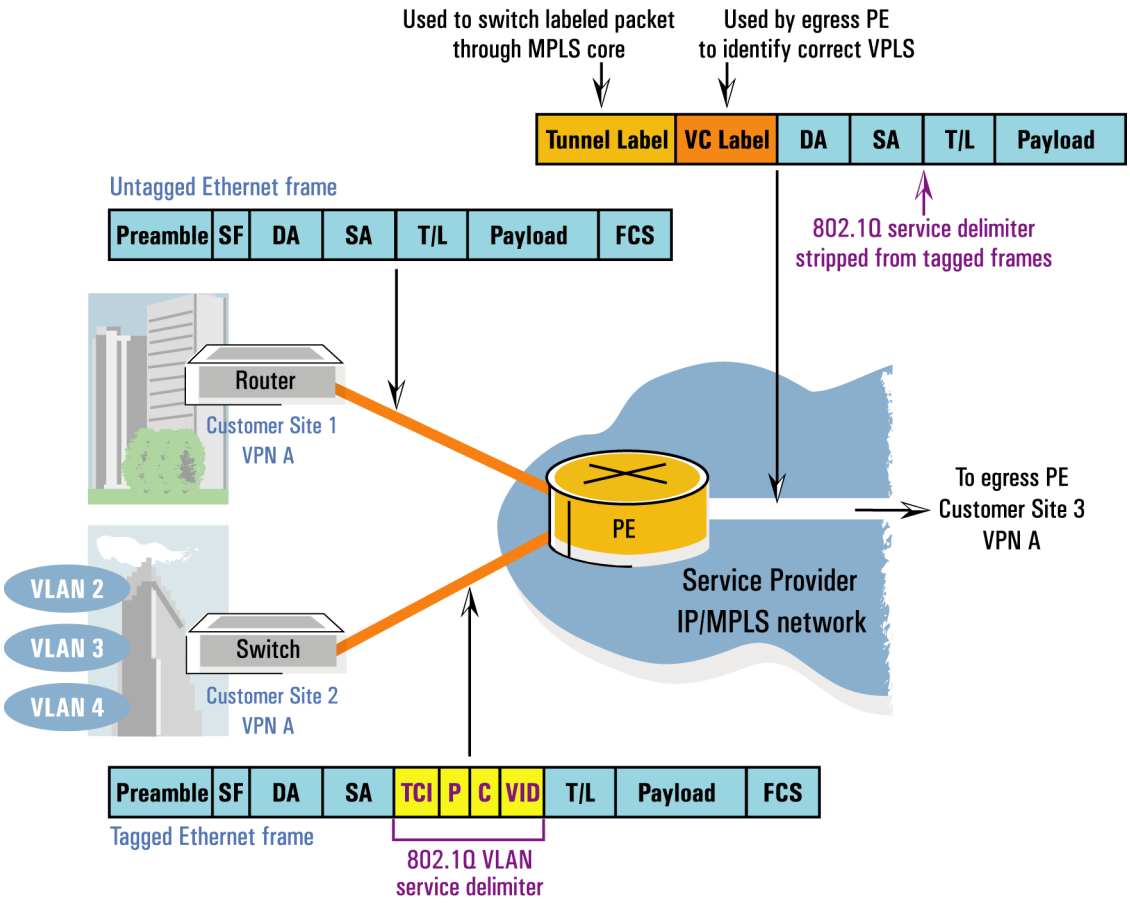

Figure 2: Packet encapsulations

Intermediate LSR switching. The intermediate LSRs in the provider's MPLS core network (also called Provider (P) routers) are not aware of the VPLS service. They simply use the tunnel label to switch the labeled packets through the network to the egress PE, swapping the label at each hop.

Network ingress lookup. When the egress PE finally receives the packet, it strips the outer label and inspects the inner one. From the VC LSP on which the packet arrived and the information in the VC label, the PE determines the VPLS instance to which the frame belongs, the outgoing access port or sub-interface to use, and — if the frame was originally VLAN-tagged — the VLAN header information to insert before forwarding the frame to the attached CE device.

Multicast and broadcast support. A VPLS service achieves one-to-many or many-to-many connectivity by replicating frames at the ingress PE, then using the full-mesh VC LSPs to flood labeled packets to all other PEs in the VPLS instance. Both broadcast frames and unicast frames with unknown destination MAC addresses are handled this way. Although the default action for multicast frames is also to broadcast them, more efficient ways are currently being developed.

MAC address learning

For each VPLS, a PE device maintains a separate Forwarding Information Base (FIB) that contains all the addresses and interface identifiers it has learned, plus any other information it needs to forward VPLS traffic to these addresses. PEs learn MAC addresses from the source addresses in traffic sent by other PEs in the VPLS. However, if several local sites belonging to the same VPN are directly attached, a PE will also use its CE access ports or sub-interfaces for address learning.

When a PE first receives a frame on an access port, it conducts a FIB lookup on the destination MAC address. If an entry for this address exists in the forwarding table, the PE uses the information to attach label values and identify the correct egress port. If the FIB does not contain an entry, the PE replicates the frame and floods it to every other PE in the VPLS instance, using the VC labels that were signaled by the PEs when the VCs were established.

When each egress PE receives the labeled packet, it "learns" the source MAC address then conducts a FIB lookup on the destination address. In a similar fashion to the ingress procedure, the PE forwards the frame to the right CE device if an entry exists, otherwise it floods the frame to each attached access device belonging to the same VPLS.

Figure 3 illustrates the forwarding of frames with known MAC destination addresses and the flooding of frames with unknown addresses. It also shows some of the information a VPLS-capable PE stores in its FIB table to make forwarding decisions.

To speed convergence when topology changes occur, PEs use LDP Address Withdraw Messages to signal addresses that other PEs need to relearn or remove from their FIBs. A FEC TLV in this message identifies the VPLS in question, and a new MAC TLV lists the MAC addresses and associated interfaces or VC LSPs. An Address Withdraw Message containing a MAC TLV with an empty address list means the receiving PE should delete all addresses for the VPLS specified in the FEC TLV, except those learned from the PE sending the message. PEs also use an aging mechanism for source addresses learned from remote PEs so they can be "unlearned" (removed from the FIB) if unused for a specific period of time.

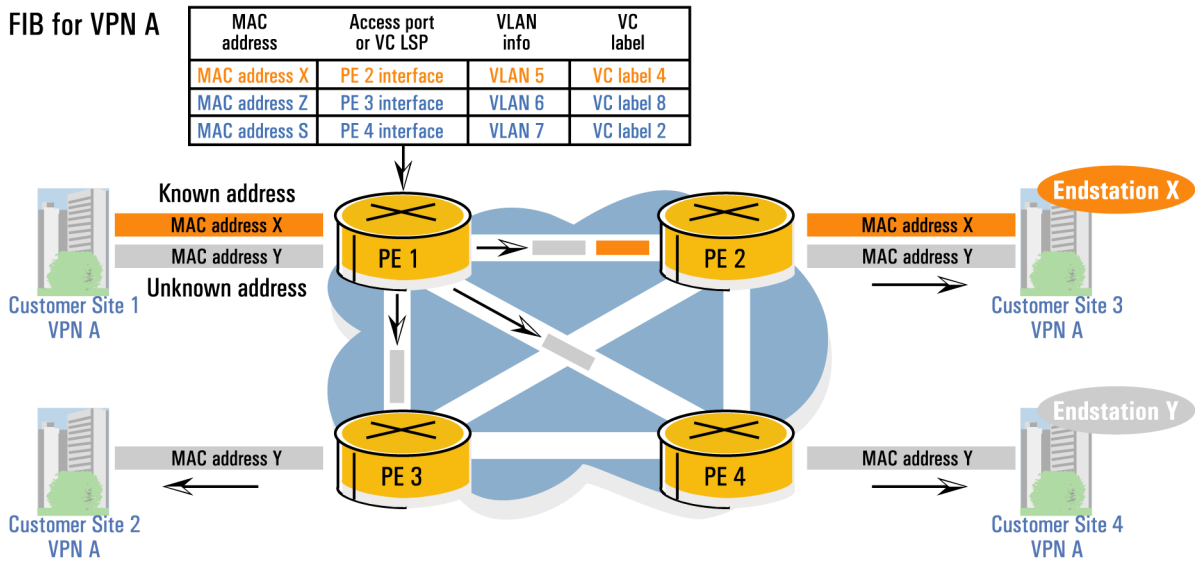

Figure 3: Processing of frames with known and unknown MAC destination addresses

Hierarchical VPLS (H-VPLS)

The VPLS model described in the previous section relies on a full mesh of tunnel and VC LSPs to implement any-to-any connectivity. However, when large-scale VPLSs are deployed, the signaling overhead to set up these LSPs can be high, and the replication demands on PE routers processing incoming broadcast, multicast, and "unknown" unicast frames are even more considerable. To address these scalability issues, a hierarchical model of VPLS connectivity, called hierarchical VPLS (H-VPLS), is also defined in draft-lasserre-vkompella-ppvpn-vpls-xx.txt.

In this model, illustrated in Figure 4, service providers locate smaller edge devices (switches or routers) in multi-tenant unit buildings (MTUs) to aggregate customer VPLS traffic before sending it to the PE in the POP or CO. The MTU and PE devices connect via a single point-to-point tunnel, then signal a virtual "spoke" Martini VC (also called a *pseudowire*) over this tunnel for each VPLS, using the spoke VC label to associate traffic with a particular VPLS instance. If the access network is Ethernet, a service provider-inserted VLAN tag can serve as the VPLS identifier instead.

A full mesh of VCs, known as "hub" VCs, are still required in the core between PEs participating in the VPLS instance, but in H-VPLS they only need to be set up on a per-spoke basis, rather than a per-VPLS basis, since the MTU devices handle traffic demultiplexing between the VPLS customers they serve. The hierarchy imposed by the H-VPLS hub-and-spoke model reduces the number of VC LSPs in the provider's MPLS core network and significantly relieves the replication and signaling burdens of PEs in large VPLS implementations. Another application for this type of VC spoke connection is to interconnect VPLS services that span two Metro networks.

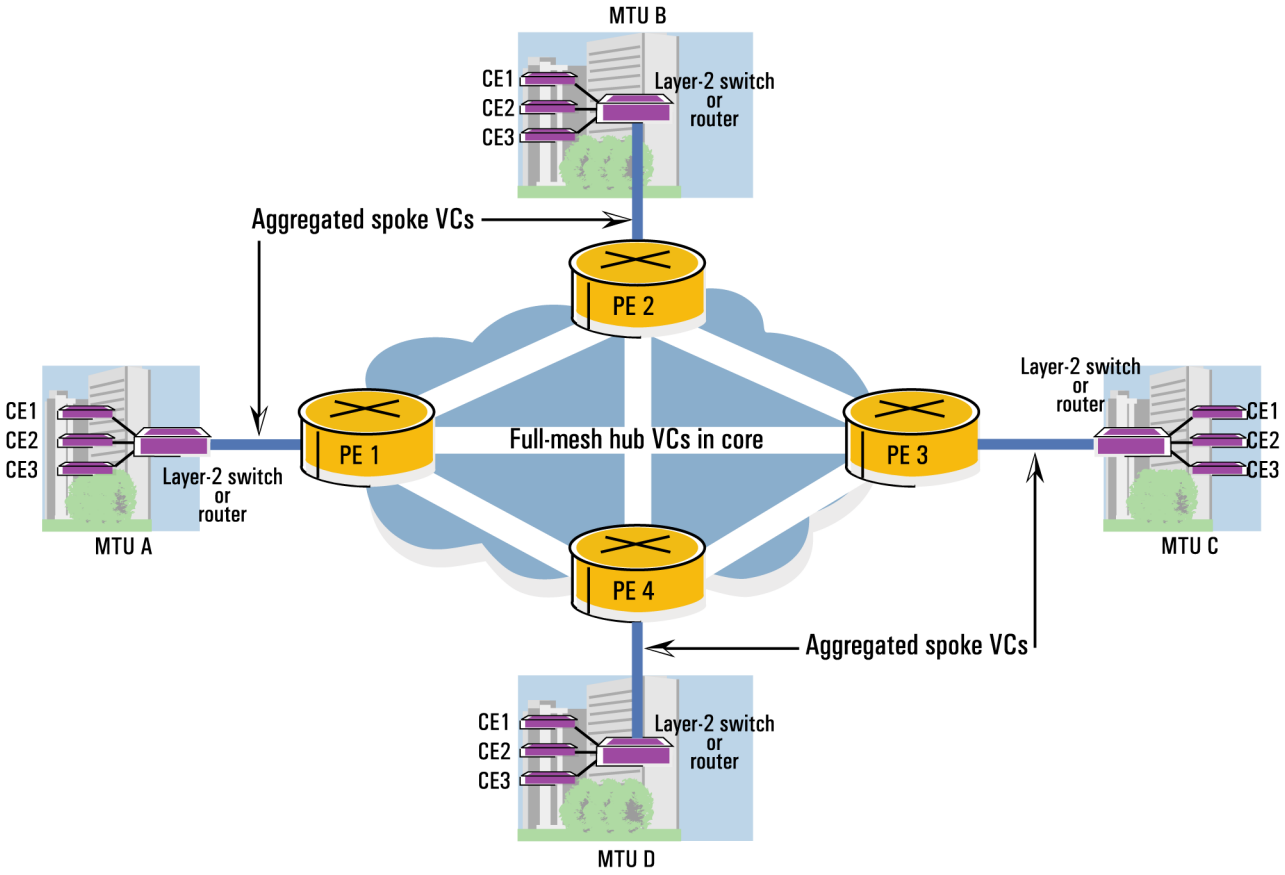

Figure 4: Two-tiered hierarchical VPLS model — hub and spokes

VPLS over MPLS Test Challenges

This section describes two common scenarios for testing the VPLS capabilities of a PE router — VPLS functionality and VPLS scalability. Both scenarios require a tester that can simulate the topology of a service provider's MPLS network and support the necessary routing and signaling protocols. The tester should also be able to emulate VPLS customer traffic by generating multiple Layer-2 VLAN-tagged or native Ethernet streams at wire speed, then conduct real-time performance measurements on this traffic. Finally, the tester should provide an easy way to detect VPN leakage by inspecting label stacks and verifying forwarding accuracy.

In both scenarios described below, the device under test (DUT) is a VPLS-enabled Provider Edge (PE) router.

Scenario 1: Testing VPLS functionality

This test measures the basic functional capabilities of a VPLS-capable PE router — specifically, its ability to (a) set up a full mesh of VPLS VC LSPs over pre-established tunnel LSPs; (b) learn MAC addresses and populate a VPLS FIB table; and (c) correctly encapsulate and forward (or flood) VPLS traffic containing both known and unknown MAC destination addresses. The test requires two test ports.

First, the test topology is set up, with one test port configured as a local CE device attached to the DUT via a point-to-point link, and a second test port used to advertise a simulated provider OSPF or IS-IS network comprising a mesh of Provider (P) and Provider Edge (PE) routers, with CE devices configured behind the PE routers to simulate remote VPN sites in the VPLS. The FIB of each simulated CE device is populated with a set of MAC addresses to simulate VPLS customer endstations. Using LDP or RSVP-TE, a full mesh of ingress and egress LSP tunnels is set up between the DUT and all PE routers. This test configuration is illustrated in Figure 5.

The second step is to establish Extended Discovery LDP sessions between all PE routers, then exchange LDP Label Mapping Messages in Downstream Unsolicited mode to distribute VC labels and VPLS FEC information. This protocol exchange results in the establishment of a full mesh of VC LSPs in both directions.

Next, labeled packets containing source MAC addresses from the simulated remote VPN sites are sent from the second test port to the DUT. The DUT should learn the addresses — i.e., create entries in its FIB for each one.

Unlabeled Layer-2 Ethernet frames (VLAN-tagged or untagged, depending on test needs) can now be sent from the local VPN site on the first test port to addresses in the remote VPN sites on the second test port to verify the DUT's ability to encapsulate and forward the traffic with the correct tunnel and VC LSP labels. Two-stack labeled traffic is sent in the reverse direction from the second test port to addresses in the attached local VPN on the first test port to verify that the DUT can pop labels and insert the correct VLAN tag information, if required. Finally, traffic containing unknown MAC destination addresses is sent from the first test port to verify the DUT's replicating and flooding capabilities.

Statistics are taken during each these steps to report the number of lost frames, mislabeled frames, frames with incorrect VLAN tags, and missing or incorrect entries in the DUT's FIB.

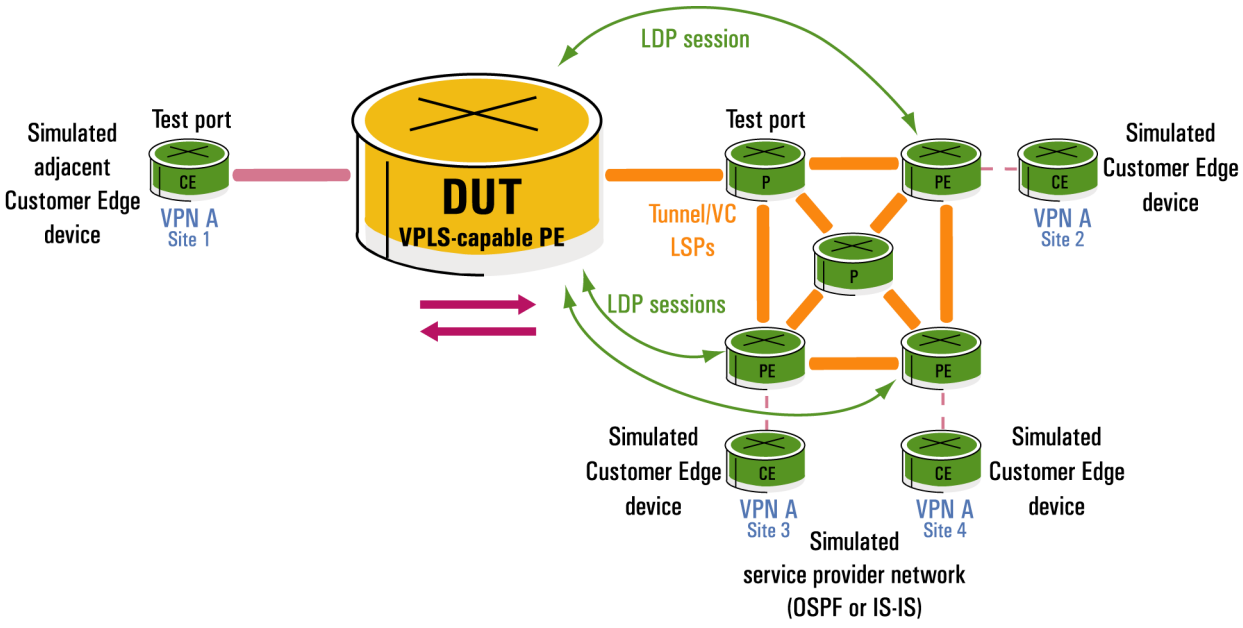

Figure 5: Testing VPLS functionality

Scenario 2: Testing VPLS scalability

This test builds on the first scenario to determine how many VPLS VPNs a VPLS-capable PE router can establish and maintain. It also tests for VPN leakage under stressful conditions — a key test scenario for VPLS VPNs.

In order to simulate the large number of VPLS VPNs required, the tester should have the ability to support multiple sub-interfaces on a single physical interface. (Sub-interfaces can be implemented with a Gigabit Ethernet interface using VLANs.)

The test topology is set up as illustrated in Figure 6. Sub-interfaces on the first test port simulate separate local VPLS VPNs connected to the DUT via point-to-point links. As in the previous scenario, a simulated provider OSPF or IS-IS network comprising a mesh of Provider (P) and Provider Edge (PE) routers is advertised from the second test port. CE devices configured behind the PE routers simulate a second VPN site for each VPLS VPN.

After verifying that the DUT can accurately forward traffic between customer sites for one VPN, the strategy of this test is to keep setting up more and more VPNs, as follows:

- Additional sub-interfaces on the first test port are configured to simulate new local VPN customers.
- The topology on the second test port is expanded as required to add a remote VPN site for each new VPN customer on the first test port.
- A full mesh of tunnel and VC LSPs is established for each new VPLS VPN.
- Traffic is sent from each new CE device on the second test port to the DUT, so new VPLS FIBs can be created and populated.

The test continues to increase the number of VPLS VPNs by the same increment until the maximum number of VPNs is reached (e.g., 10,000 or more). At each iteration, traffic is sent in both directions and measurements taken to verify correct label stack encapsulation, and accurate forwarding to VC LSPs and sub-interfaces.

This scenario is particularly important because it answers *the* critical question for network equipment manufacturers and service providers: *Under stressful Internet conditions, can a VPLS-enabled PE router set up T-LDP sessions and VC LSPs, learn MAC addresses, replicate frames, and encapsulate and forward customer traffic without VPN leakage?*

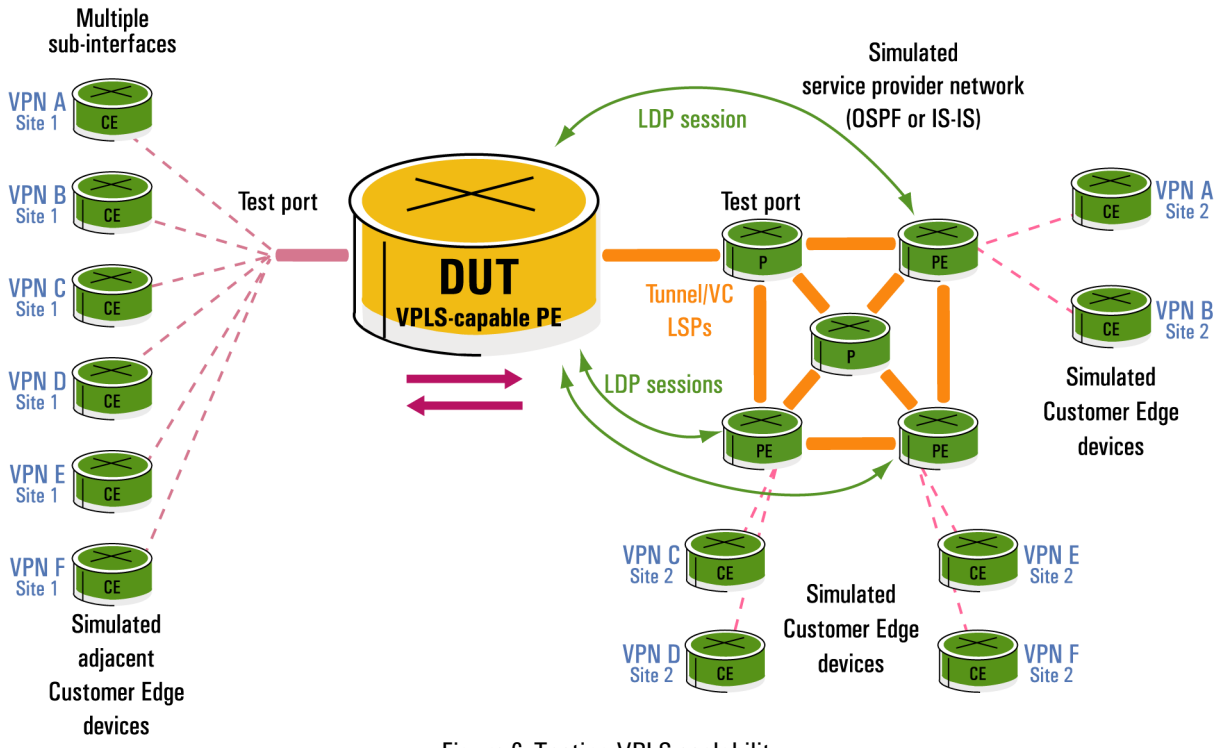

Figure 6: Testing VPLS scalability

Conclusion

VPLS adds a new level of complexity to a PE router's already considerable control-plane and packet processing demands. Besides functioning as an MPLS Label Edge Router (LER) that provisions LSP tunnels and pushes/pops labels, the PE must serve as an Ethernet bridge, with all the learning, filtering, forwarding, and flooding requirements this entails. It must also implement the necessary LDP signaling extensions required by VPLS. On top of all this, a VPLS-enabled PE must ensure customer VPN security.

Network equipment manufacturers need to rigorously test all aspects of their VPLS implementations, and service providers should verify and evaluate these claims as well. To this end, test equipment should measure up to the same stringent demands. The tester should be able to provide the right access interfaces; generate and measure multiple Layer-2 streams in real time; support the routing and signaling protocols and extensions necessary to establish tunnel LSPs, T-LDP sessions, and VC LSPs; and scale to tens of thousands of simulated VPNs and hundreds of thousands of VCs.

Because configuring tests can be a laborious process, the tester should also provide a fast and easy way to set up the VPNs, modify network topologies, vary traffic loads, and display test results. The burden of testing complex technologies such as VPLS can be greatly alleviated with a powerful and usable test system.

United States:
Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:
Agilent Technologies Canada Inc.
2660 Matheson Blvd. E
Mississauga, Ontario
L4W 5M2
1-877-894-4414

Europe:
Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-2323
United Kingdom
07004 666666

Japan:
Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura-Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:
Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #950
Miami, Florida 33126
U.S.A.
Tel: (305) 269-7500
Fax: (305) 267-4286

Asia Pacific:
Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 3197-7777
Fax: (852) 2506-9233

Australia/New Zealand:
Agilent Technologies Australia Pty Ltd
347 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

www.agilent.com/comms/RouterTester

February 3, 2003.
5988-8867EN

Agilent Technologies