Virtual Private LAN Service

VPLS Example
Description

VPLS is much like VPWS from a network point of view, but it is designed to support a multipoint topology rather than a point-to-point topology. Since MPLS PWs are point-to-point, VPLS depends on a mesh of PWs between all of the provider edge devices. The provider edge devices act as Label Edge Routers (LERs) as with VPWS but the LER are logically front-ended with a function that looks like an Ethernet Switch.

Each PE includes a logical element called a VSI (Virtual Switch Instance). The VSI emulates an IEEE 802.1Q Bridge. In other words, the VSI handles C-TAG frames, learns the customer MAC addresses and makes the forwarding decision. Once a destination or set of destinations is determined, the appropriate frame is encapsulated with the tunnel and PW headers. When there is a need to multicast or broadcast, the ingress PE replicates the frames and sends a copy to each egress PE. In this manner, the service “virtually bridges” the customer end-points, simulating a private LAN.

Resiliency is also provided by the MPLS LSP and PW layers which can be considered to be independent of the VPLS service instance. Services are denoted in the same manner as for VPWS, as is CoS ID.

Multiple VPLS instances – one per service or L2VPN – can use the same network infrastructure.

VPLS provides support for all six MEF-defined Carrier Ethernet service types. The L2CP handling capabilities are virtually the same as for provider bridging, as both incorporate a bridge component that handles customer C-Tag frames.

The CEN (Carrier Ethernet Network) does not use xSTP (variants of Spanning Tree Protocol) for forwarding or resiliency. The Customer xSTP is not tunneled across the VPLS-based CEN.

E-Tree is naturally supported by VPLS. The concept of hub (root) and spoke (leaf) is also part of the VPLS standard.

Support for the various Ethernet services is summarized in the table below