MPLS VPN Services

PW, VPLS and BGP MPLS/IP VPNs

Technology White Paper

Serge-Paul Carrasco

Abstract

Organizations have been demanding virtual private networks (VPNs) instead of costly leased lines and, Ethernet and IP services instead of DS1 and DS3 services from their service providers.

MPLS is now the best way for service providers to respond to those customer demands by providing Pseudo Wires (PW) services, Virtual Private LAN Services (VPLS) or Layer 2 MPLS VPNs and IP VPNs or Layer 3 MPLS VPNs.

The Growing Deployment of Multi Protocol Label Switching (MPLS) Services

MPLS emerged initially in the late 90s as a traffic engineering technology for the core of the Internet. Since the burst of the Telecom bubble in 2001, service providers have realized that the Internet was not growing so fast anymore and traffic engineering was less needed.

However, the demand from enterprise networks for more Internet Protocol (IP) and Ethernet services and in particular Virtual Private Networks (VPNs), cheaper than leased-lines, has given to MPLS a new life beyond traffic engineering.

MPLS has strongly emerged as the best technology to provide initially IP VPNs also called Layer 3 VPNs and now PW (Pseudo Wires) and VPLS (Virtual Private LAN Services) also called Layer 2 VPNs.

For service providers, MPLS VPNs are definitely the revenue generating application. For enterprise networks, VPNs enables them to save costs by moving away from expensive legacy leased lines. In addition, MPLS VPNs enable enterprise networks to switch from legacy Frame Relay (FR) and Asynchronous Transfer Mode (ATM) VPNs to MPLS VPNs in order to accommodate their growth in native IP and Ethernet connectivity.

Service providers generally offer the MPLS service through their provider edge (PE) routers. The enterprise IP networks are connected to their service provider networks through their customer edge (CE) routers.

MPLS Label Switching Fundamentals

Fundamentally, MPLS provides connection-oriented capability to IP, through label switching. MPLS is independent of the layer data link (Ethernet, ATM or FR). In MPLS networks, packets are forwarded based on their forwarding equivalence class (FEC) as they enter the MPLS network.

The FEC to which the packet is assigned is encoded as a short fixed length value known as label. An FEC is basically a flow of IP packets forwarded over the same path and mapped through the same labels. A label-switched path (LSP) is a simplex layer 2 tunnel like an ATM or FR PVC which defines the path followed by labeled packets assigned to the same FEC. Labels can be stacked to provide a hierarchy of LSPs.

MPLS can use different distribution label framework. Present protocols for label distribution include: Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP) and Border Gateway Protocol (BGP).

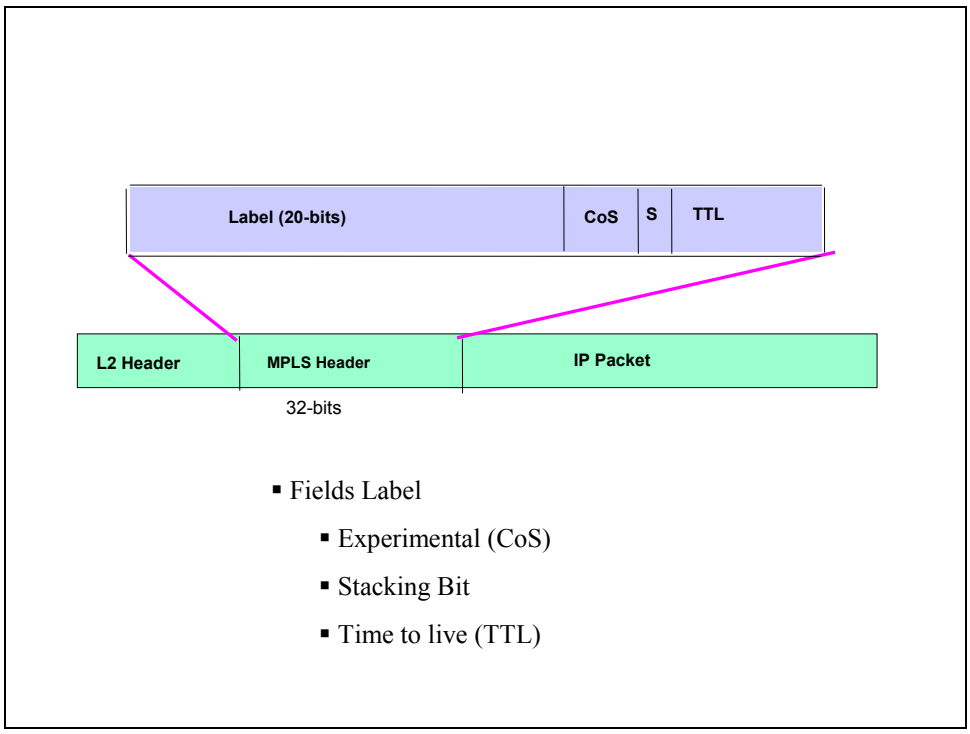

Figure 1: MPLS Label

MPLS Pseudo-Wires Services

A pseudo wire (PW) service provides a layer 2 point-to-point service. The purpose of an MPLS PW is to emulate a legacy or a new service over an MPLS LSP. Present services supported by MPLS PW include Ethernet/VLAN, PPP/HDLC, Frame Relay and ATM services.

All services are emulated like virtual circuits (VCs). The VC provides all the functions required to fully emulate the original service (in particular for FR and ATM operations).

PW uses the Martini encapsulation to carry the service over MPLS. The encapsulation provides two label layers: one for the emulated service and, another one for the LSP underlying tunnel.

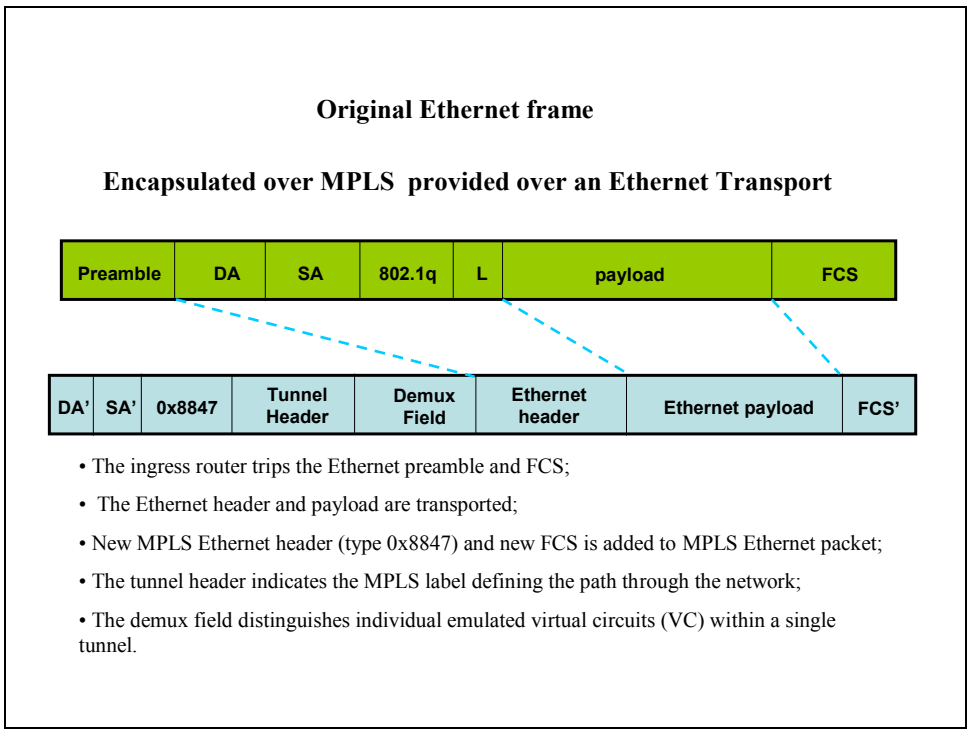

Figure 2: Ethernet over MPLS (EoMPLS) Martini Encapsulation

The PW accomplishes mainly three functions:

- Encapsulation of circuit data or PDUs at the ingress;
- Carrying the encapsulated data across the tunnel;
- Managing the signaling, timing, order, OAM and specific aspects of the service.

The end-user does not have to change its previous layer 2 protocol from its CE to the PE to access the PW.

PW technology is defined in the IETF Working Group Pseudo Wire Emulation Edge to Edge (PWE3).

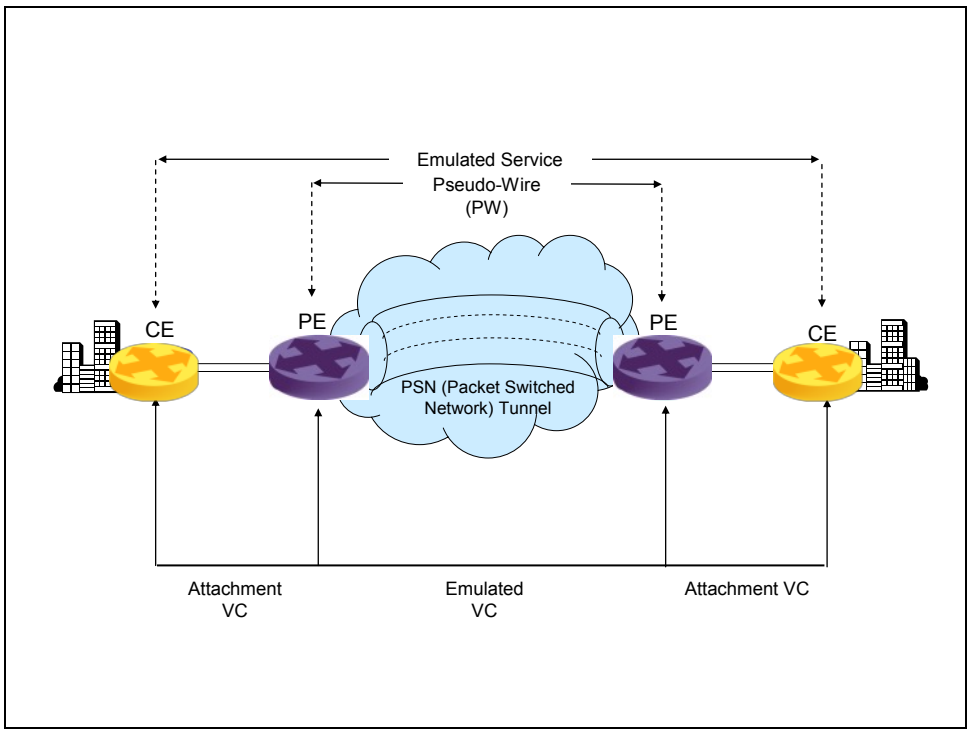

Figure 3: PW Network Reference Design

MPLS Layer 2 VPNs Services: Virtual Private LAN Services (VPLS)

The primary goal of VPLS is to provide connectivity between dispersed enterprise sites across a MPLS metro network, as if they were connected using a LAN. VPLS can be seen as if the MPLS metro network operates as a switch or bridge.

VPLS emulates the various LANs services over an MPLS transport network. It creates a layer 2 broadcast domain basically through an Ethernet learning bridge model provided by the MPLS network.

Broadcast and multicast are two important LANs services used by Ethernet but are not supported by MPLS. VPLS extends the Martini encapsulation for transporting Ethernet and VLANs traffic across multiple sites that belong to the same LAN by providing in particular broadcast and multicast capabilities.

In order to do so, PE devices are required to dynamically learn MAC addresses on physical ports and on VC LSPs. And, MAC address are learned and aged on a per LSP basis. To support standard Ethernet bridging, packet are replicated across LSPs for broadcast and multicast traffic and for flooding of unknown unicast traffic.

VPLS is a layer 2 MPLS VPN and an alternative to layer 3 MPLS VPN for two business reasons:

- First, a number of customers, especially large ones mainly for security reasons, do not want to outsource their routing tables as required per RFC 4364;

- Second, Ethernet as a replacement service to legacy DS1 and DS3 services is more and more demanded by enterprise customer to service providers. Most Service Providers have been offering Ethernet through Transparent LAN Services (TLS). Unfortunately, TLS is a point-to-point service. VPLS on the other hand is a multipoint-to-multipoint service;

VPLS are defined presently through multiple drafts in the Layer 2 VPN working group of the IETF (L2VPN).

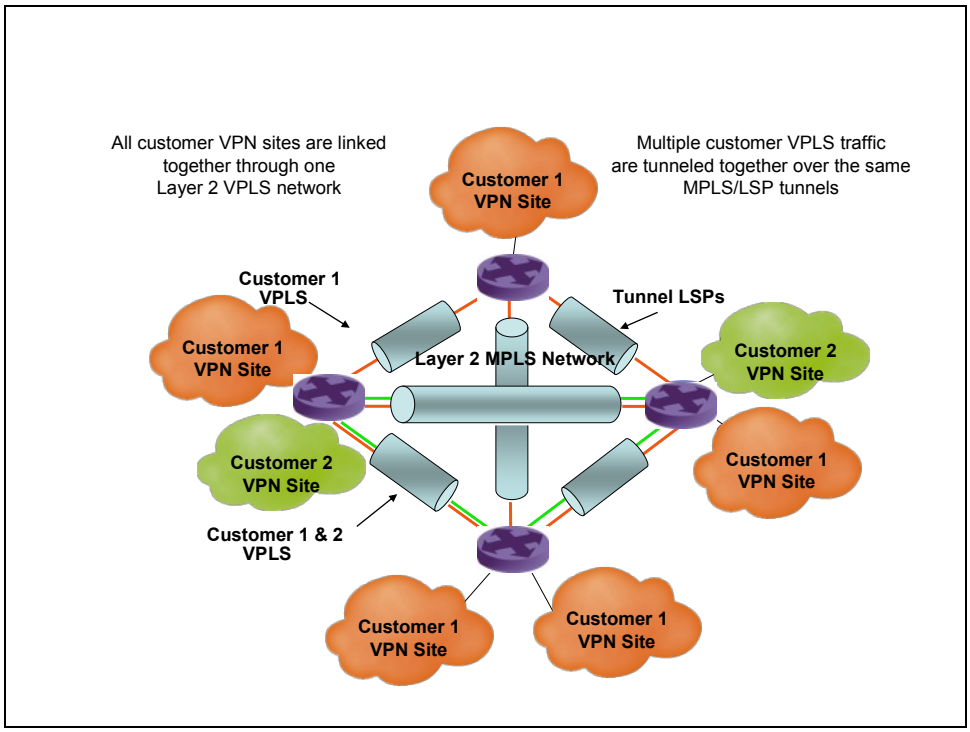

Figure 4: VPLS Network Reference Design

MPLS Layer 3 VPNs Services: BGP/MPLS IP VPNs (RFC 4364)

Service providers have been supplying IP VPNs to their commercial enterprise customers using their MPLS backbones.

Enterprise VPN routes are communicated from the CE to the PE using an Interior Gateway Protocol (IGP) such as the Open Shortest Path Protocol (OSPF) or an Exterior Gateway Protocol such as Exterior Border Gateway Protocol (eBGP).

The service provider's PE propagates the VPN routes, called VPN routing and forwarding (VRF) to its PE peers using Interior BGP (iBGP). The enterprise VPN traffic is forwarded between the PEs connected to the enterprise site of the customer's VPN using MPLS Label Switched Paths (LSPs) in a mesh topology.

Since enterprise networks can use private addresses that cannot be routed over the service provider Internet network, PE routers need to create a new address format using a route distinguisher and the end-user IPv4 prefix address. Multi-Protocol Extensions to iBGP (MP-BGP) is used to carry those created addresses.

BGP/MPLS IP VPNs are defined in RFC 4364 and part of the Layer 3 VPN working group of the IETF (L3VPN).

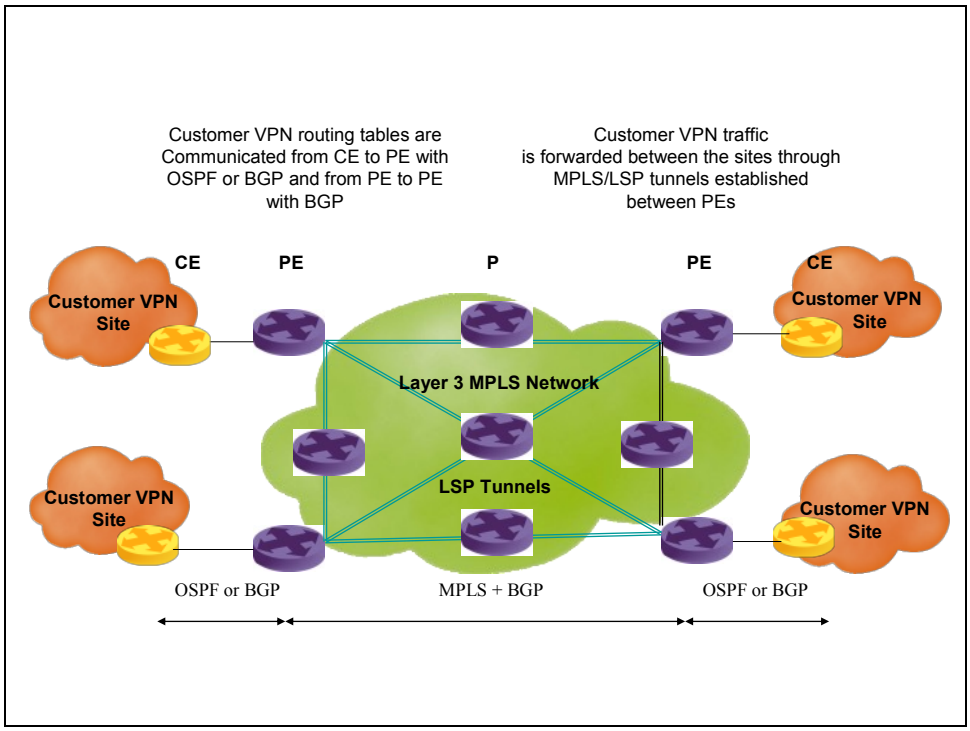

Figure 5: IP VPNs Network Reference Design

References

- IETF:
  - MPLS:
    - RFC 3031: "Multi protocol Label Switching Architecture"
    - RFC 4448: "Encapsulation Methods for Transport of Ethernet over MPLS Networks"
    - RFC 3985: "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture"
    - RFC 4364: "BGP/MPLS IP Virtual Private Networks (VPNs)"
    - Draft: "VPLS using LDP"
    - Draft: "VPLS using BGP for Auto-Discovery and Signaling"
- Books:
  - "ATM & MPLS Theory & Application" David McDysan and Dave Paw, Mc Graw Hill.

Acronyms

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CE	Customer Edge
FEC	Forwarding Equivalence Class
FR	Frame Relay
IP	Internet Protocol
LAN	Local Area Network
LSP	Label Switched Path
MPLS	Multi Protocol Label Switching
OAM	Operations Administration & Maintenance
PVC	Permanent Virtual Circuit
PW	Pseudo-Wires
PE	Provider Edge
RSVP	Resource Reservation Protocol
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network
VPLS	Virtual LAN Private Services

