White Paper

OptiSwitch Master®
MPLS/VPLS – VPN solution

Introduction

OptiSwitch Master® is a modular IP/MPLS platform based on network processors that offers carrier-class design with rich-set of features to meet Metro Ethernet networks demands.
Metro Ethernet Service providers invariably need to establish private networks between two or more locations in Metro areas. OptiSwitch Master® incorporates a standard Multi-Protocol Label Switching (MPLS) technology that offers a flexible way to meet demands for such VPNs, as well as other custom demands that are beyond the current standards.
MPLS functionality is performed on all data plane interfaces and offers the following solutions:

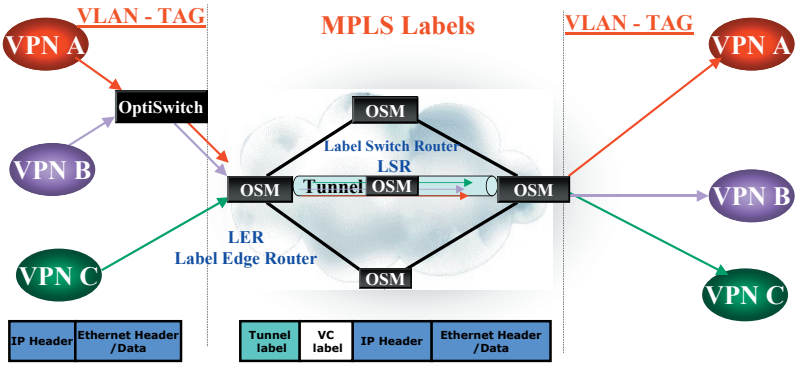
1. Layer 2 VPN with point-to-point Virtual Circuit (VC) based on IETF Martini draft.
2. VPLS Multi-point VPN based on draft-lasserre-vkompella-ppvpn-vpls.
3. Traffic Engineering.
4. Bandwidth reservation and policing.
5. Differentiated Services (E-LSP).
6. Subscriber management integration into an MPLS scheme.

The objective of this document is to define the OSM MPLS/VPLS functionality and identify its benefits in various networking environments.

What is MPLS?

MPLS means Multi Protocol Label Switching. A label (a number) is placed in a packet header and is used in place of an address (an IP address, usually) to direct the traffic to its destination.
The basic idea is to take the customer's Ethernet packets, and move these packets seamlessly to other locations without modifying them.
An MPLS domain is built of LERs (Label Edge Routers) that reside at the edge of MPLS domain and interior LSRs (Label Switch Routers) that are located within the MPLS domain. The LERs need to deal with both MPLS frames and native-mode user traffic while Interior LSRs needs to forward only MPLS frames (Figure 1).

Following are main functions performed in a flow on an MPLS network:
1. The Ingress Label Edge Router (LER) examines the inbound IP packets, classified packet to a Forwarding Equivalence Class (FEC), generates MPLS header and assigns (binds) initial label.
2. All the other routers inside the MPLS domain look at labels only, not at the IP address



3. Interior Label Switch Router (LSR) forwards MPLS packets using label swapping (the processing is always on the top label)
4. The Egress LER removes the MPLS header and forwards the packet based on the IP destination addre

With MPLS it is possible to overcome the major drawbacks of conventional routing:
1. Connectionless IP does not support traffic engineering.
2. It is difficult to implement QoS architectures with IP.

Additionally, MPLS has other Advantages:
1. Scalable solution - Labels are local and many IP addresses can be associated with one or few labels.
2. Simple solution – The interior Label Switch Routers perform simple label switching. Only the edge device makes the more complicated task of classifying the packets into FEC and binding a label.
3. Lower latency – Usually label-switching is a simple task comparing to Longest prefix match and IP forwarding.

Layer 2 VPN Services

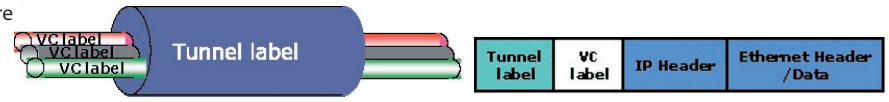
Layer 2 VPNs are established by one or more point-to-point transparent tunnels. Subscribers Layer 2 traffic sent through the MPLS VPNs is moved seamlessly across a core network running MPLS.
The OSM's MPLS VPNs solution provides a high-bandwidth cost effective alternative to legacy Telco circuit leased lines.

The OSM offers the following functions at the provider edge:
1. MPLS signaling to establish layer 2 tunnels and to define their parameters (draft-martini-l2circuit-trans-mpls-08)
2. MPLS data encapsulation to forward service-specific data over the MPLS backbone (draft-martini-l2circuit-encap-mpls-04)
3. Binding Subscribers to MPLS VPNs.
4. Provision of QoS and SLA services for subscribers VPNs.

What is Martini Draft ?

Martini draft is a method for transporting layer 2 customer data over a scalable provider MPLS network. The idea is to use MPLS in order to emulate virtual channels (VCs) and mask from the user the fact, that the same physical link is being shared by other users.
MPLS technology was adapted by IETF to provide virtual circuit (VC) provisioning over multi-protocol networks. In legacy ATM networks VCs defined connection-oriented service. With Martini draft, the same functionality is provided by Ethernet in an MPLS networks. MPLS Layer 2 VC actually extends the customer LAN across an MPLS network.
In order to pass frames transparently from the VC ingress to the VC egress the whole Ethernet frame is first encapsulated with a VC label that identify the VC on both ends. Another label (Tunnel label) is used for forwarding the frame along the established Label Switch Path (LSP). The interior LSRs forwards the frame according to the Tunnel label till the frame arrives to the egress LER. Then the Tunnel label is popped and according to the VC label (which is popped also) the OSM knows the outgoing interface/VLAN identifier and delivers Ethernet frames to the destination.

Figure



OSM supports MPLS layer 2 Virtual Circuit (VC) based on draft-martini-l2circuit-trans-mpls-08.txt and draft-martini-l2circuit-encap-mpls-04.txt.

What are MPLS VPNs (Martini) Advantages?

1. Provider's network is transparent to customer networks; therefore there is no need for complicated configuration (routing protocols) on customer side.
2. Scaleable solutions for Service Provider to implement
3. Common MPLS backbone does not require any special customer configuration. VC is configured only at the LERs. Interior LSRs do not maintain customer VC information.
4. Layer 2 tunneling service supports any Layer 2 or Layer 3 traffic.
5. Low-cost solution for Provider & Customer.

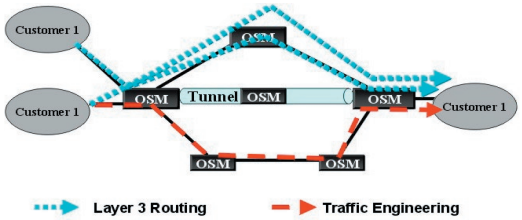
In essence, the MPLS VPNs based on Martini draft provides transparent L2 VPN services that can connect seamlessly customer's remote branches. The customer's network administrator has complete control over how the network is running without any protocol interaction with the provider network.

MPLS and Signaling

Traffic Engineering (TE) can be used to resolve congestion and improve network utilization. Routing protocols usually create a single "shortest path" and all the traffic is sent through that path. The consequence is that the "shortest path" becomes congested while in the same time "longer" paths become underutilized. Now instead of adding more and more bandwidth to avoid congestion, the TE approach is to "put the traffic where the bandwidth is" (see figure 3). It implies the ability to diversify routes and to "explicitly" route traffic.

MPLS Traffic Engineering allows explicit routing and set-up of LSPs. It also provides control over how LSPs are recovered in the event of failure. Such functionality enables value-added services like Traffic engineered VPNs, Service Level Agreements (SLA) and Multi-media over IP solution (VoIP).
In order to implement MPLS Traffic Engineering, enhancements were added to the routing protocols and to the MPLS signaling protocols.
The traditional routing protocol is extended to provide explicit route selection while preserving predefined constraints. Examples for such constraints are bandwidth requirements, include or exclude nodes, include or exclude specific links. The goal of constraint-based routing is to compute a path from a given node to another, such that the path doesn't violate the constraints and is still optimal.

Figure 3.



The enhancements to the MPLS signaling protocols to allow explicit constraint-based routing produced the following extended protocols:
1. Resource Reservation Protocol – Traffic Engineering (RSVP-TE)
2. Constrained Routing enabled Label Distribution Protocol (CR-LDP).

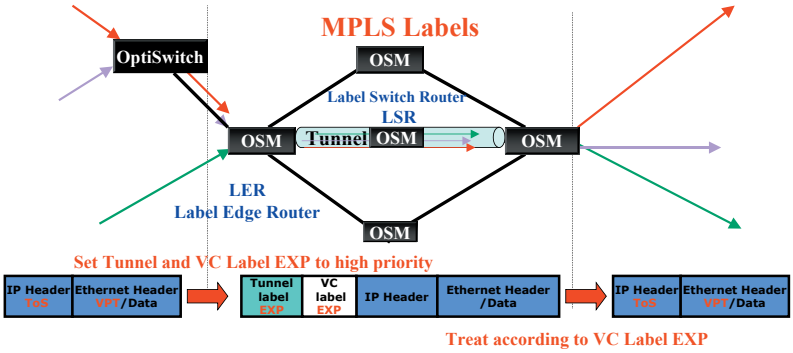
The enhanced Signaling protocol can provide:
1. Coordinate label distribution
2. Explicit routes (strict & loose)
3. Bandwidth reservation
4. Class of Service
5. Preemption of existing LSPs
6. Loop prevention
7. Protection LSP

Using the above technology and protocols the OSM is able to provide many of the new services that Service Providers seek to offer rely on TE functions. Examples are bandwidth assurance, diverse routing, load balancing, path redundancy, preparing alternative path for fast recovery and other services necessary for providing QoS.

MPLS and QoS Functionality

MPLS is a QoS-enabling technology that forces application flows into connection-oriented paths and provides mechanisms for Traffic Engineering and bandwidth guarantees along these paths.
As explained in the previous paragraph, the OSM has the ability to create traffic engineered LSP called tunnels. These tunnels can be created using either CR-LDP (LDP tunnels) or RSVP-TE (RSVP tunnels). One of the important constrains that the administrator can define for a tunnel is the amount of bandwidth needed for the tunnel. While the tunnel is established the bandwidth is reserved on all the OSMs along the path. If according to the internal admission control there isn't enough bandwidth available on one of the OSMs, that tunnel would either fail or replace an existing tunnel with lower priority.
After the tunnel creation the OSM use rate-limit to police the traffic sent through the tunnel and to make sure it doesn't cross the reserved bandwidth boundary as specified in the tunnel definition.
Another important feature of the OSM is the ability to provide differentiated service level to specific flows that use the same Virtual Circuit (VC). Since VC is used for Layer 2 VPNs and the traffic is not necessarily IP packets, the OSM uses the 802.1Q Tag VPT bits to classify packets to service levels. Then the EXP bits in the MPLS header encapsulation is marked with an equivalent value (see figure 4). When the frame is label switched from one LSR to the other, it receives priority based on the EXP bits value.

Figure 4.



What are the Advantages of an OSM MPLS QoS ?

1. Bandwidth reservation for CR-LDP and RSVP-TE trunks.
2. Policing MPLS VPN bandwidth reservation.
3. Support E-LSPs.
4. Option to map either 802.1Q VPT bits or IP DSCP bits to MPLS EXP bits.
5. Option to mark MPLS EXP bits to specific value.
6. EXP bits are mark on both Tunnel and VC labels (important for PHP).
7. VC ingress/egress accounting.

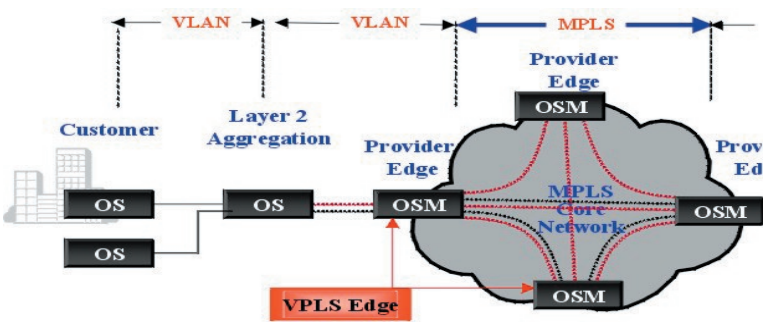
What is VPLS?

Virtual Private LAN Service (VPLS) is a class of VPN that allows connection of multiple sites in a single bridged domain over a provider IP/MPLS network (see figure 5). All customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS delivers a layer 2 broadcast domain that is fully capable of learning and forwarding according to Ethernet MAC addresses. VPLS instance performs learning, filtering and forwarding actions on logical interfaces and Virtual Circuits(VCs) exactly like an Ethernet switch. Customer connection can be Fast Ethernet or Gigabit interface that can support service-level agreement with on-the-fly rate-limit control.
As with MPLS/BGP VPN technology, VPLS is a multipoint-to-multipoint service. The difference is that at the
connection between the provider edge and customer devices there is no IP protocol interaction. To simplify operation, the connection behaves in the same manner as an Ethernet Bridged connection. The customer views the service provider network as a set of Ethernet switches. The core network consists of transit LSRs, whose function is to provide provider-edge-to-provider-edge connectivity over an MPLS core.
The OSM VPLS implementation is based on IETF draft-Lassere-vkompella-ppvpn-vpls-02.txt.

VPLS Signaling

VPLS discovery methods have not been finalized yet in an existing standard proposal. Still, the vendors use several techniques such as BGP, DNS, LDP, and RADIUS to solve the discovery challenge.
The implementation in the OSM is based on the auto-discovery algorithm described in draft-sodder-ppvpn-vhls-02. It consist 2 steps:
1. Identify all the other VPLS-speaking routers in the network and open session with them.
2. Exchange VPLS service Ids over those sessions, to learn which VC should be opened to which peer.

Figure 5.



What are the Main Advantages of a VPLS Service ?

1. Transparent, protocol independent, multipoint service.
2. Ethernet LAN/WAN interfaces that offers reduction in total cost of ownership.
3. Eliminates L2 protocol conversion between LAN and WAN
4. No training required on WAN technologies such as FR or ATM
5. Customers maintain complete control over their own switching or routing between branches, offering easier configuration and debugging in case of problems.
6. Adding new sites is simplified; no re-configuration at existing sites required.
7. Granular bandwidth on-the-fly provisioning from 64Kbps to 1Gbps for each subscriber connected to an VPLS instant.

The key feature of VPLS is simplicity. Instead of requiring customers to connect to an IP network, with the complexity of IP routing protocols, they connect with raw Ethernet, which allows a wider range of network architectures, protocols, and capabilities. All of this is provisioned using standards-based Ethernet and MPLS gear.

How a VPLS Service is Implemented in OSM ?

Once the OSM receives a configuration of a VPLS instance with a list of peers, it created VCs (Pseudowires) to each peer. All the VPLS VCs are signaled with the VPLS ID. The VPLS instance can then assigned to a logical interface. The OSM maintain a separate Layer 2 learning table for each logical interface. For specific VPLS instance this table contains MAC addresses learned from the VPLS VCs or from the logical interface ports attached to this VPLS instance. Once a frame is received on a specific logical interface port or VC the OSM search the corresponding logical interface learning table, for an entry matching the frames destination MAC. If such entry exists, the frame is forwarded according to the entry's data to the appropriate PseudoWire or logical interface port. If it doesn't, the frame is flooded on all the interface ports and VCs that belong to the same VPLS instance.
In order to populate the learning table the OSM search the learning table also for the frame source MAC. If a matching entry is found the PseudoWire or port is compared to the PW or port from which the frame arrived. If it matches the entry is updated. In case a matching entry is not found, a new entry is created and added to the learning table.
The VPLS procedure is quite similar to a regular Ethernet switch. The difference is that instead of ports we have logical interfaces ports, subscribers or VCs.
Another useful feature that is found on the OSM is the ability to limit the learning table size per logical interface. This feature is very important to the service provider who wants to prevent from a specific service user to fill the entire learning table with it's own MAC addresses, abusing the service and create Denial of Service (DoS).
Similar to the L2 VPNs the "hard work" is done by the LERs. The interior LSRs are making simple label switching and running LDP.

Who gain theVPLS application?

VPLS is a new revenue generating service that can provide cost-effective solution to a vast number of Enterprise customers. VPLS is especially important in today's soft economy, where profitability is key. Instead of cost-prohibitive routers and IP-tunneling equipment, simple Ethernet switching gear may be used to build the access and back-end networks, allowing higher bandwidth service at a lower cost of deployment. With VPLS, both point-to-point and multipoint solutions become available. Service providers can also leverage Class-of-Service (CoS) technology to provide priority services.
The carriers can provide cost-effective connectivity for multi-location customers. In many cases, utility companies will provide a metropolitan service to other local providers. In such cases, VPLS is extremely useful since it allows customers to build their networks independently of physical locations.

Subscriber management and MPLS/VPLS

The OSM can act as a provider edge router terminating up to 64K subscribers. Each subscriber is identified according to its source port and 802.1Q tag. The same tag used on different ports is treated as separate subscribers. It means the OSM subscriber scheme breaks the 4K global tags limitation.
Each subscriber can be connected to a Layer 2 point-to-point VPN based on martini draft, or to be connected to a logical interface (together with other subscribers) that belongs to a VPLS instance.
Subscribers on different OSMs connected to the same VPLS instance can send layer 2 frames to each other, as if they are connected to the same switch. In the same time this traffic is separated from traffic that belongs to other VPLS instances.
Each subscriber has a set of counters that can be used for admission control, network engineering and billing purposes.

Summary

In light of the abovementioned VPN services supported by the OSM product line, we can see the pros and cons of the solutions. The facts point out that there are subsets of technologies that enable new private data services to be offered across standards-based packet networks. There are differences in technological and economical advantages that depend on a specific customer need, but we can see that the VPLS will probably be the dominant and promising solution for the future. The IETF standardization process is moving forward and it is only a matter of time before VPLS receives industry recognition.