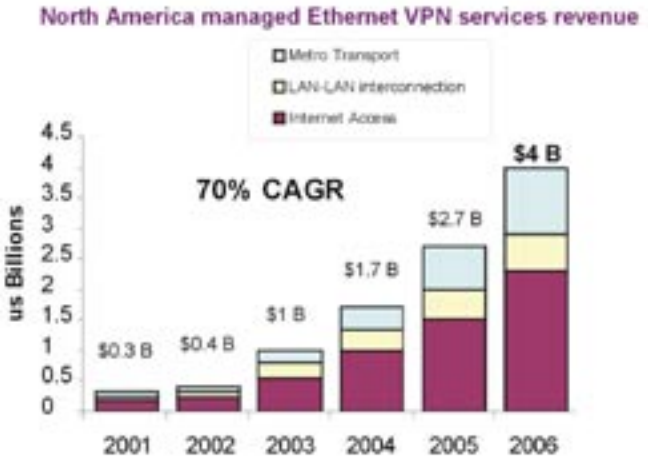
OptiSwitch Master Multipoint VPLS Solution

Abstract

The ever-growing demand from business customers for higher bandwidth network services to inter-connecting multiple offices on one private LAN has forged the creation of a new multipoint Virtual Private Network (VPN) service, called Virtual Private LAN Service, which is capable of carrying Transparent LAN Service over VPN. Carriers and service providers have been offering VPN services based on traditional TDM, Frame Relay, and ATM for some time now. The cost of operating separate networks to provide these services, and the need to provide services that consume more bandwidth on existing network infrastructures is forcing them to move to newer, more cost-effective technologies, namely, IP and MPLS.
The emergence of IP/MPLS networks based on Ethernet technology, together with the development of new standards within the IETF PPVPN working group enables TLS service providers to offer both bandwidth and carrier-class VPN services together with Internet access on a single packet-switched Ethernet infrastructure, resulting in the combined benefits of new service offerings and improved operational efficiency.

VPN Market Directions

The dominating VPN technology for enterprise customers in the domain of Wide Area Networks (WANs) is still the Private leased-line services based on Time-Division Multiplexing (TDM), Frame Relay and ATM. The revenue from the existing Frame Relay and ATM services continue to grow as many enterprise customers still choose these technologies to implement VPN WAN solutions. TDM, Frame Relay and ATM services, therefore, are going to continue to be an important source of revenue for carriers for many years to come.



Ethernet – a Cost-effective Alternative Infrastructure

Ethernet services, especially within the Metro domain, are expected to become one of the fastest growing markets in the coming years, due to the low-cost and high-speed of the services from which the end customer can benefit.

VPLS Multipoint LAN services

Virtual Private LAN Service (VPLS) according to Internet Draft (ID) lasserre-vkompella-ppvpn-vpls-02.txt, is an L2-based VPN that allows the connection of multiple sites in a single bridged domain over a provider managed IP/MPLS network. All customer sites belonging to a VPLS service instance appear to be on the same LAN, regardless of their location.
VPLS offers a balance between point-to-point Frame Relay service on one hand and Rfc2547 IP VPN services. VPLS customers maintain complete control over their IP routing system and the carrier is freed of the burden to maintain or know the customer's IP routing scheme.
VPLS offers the following advantages:

- Transparent service for all protocols
- Uses the same LAN/WAN interface L2 Ethernet protocol type and reduces the total cost of ownership
- No L2 protocol conversion is required between LAN and WAN technologies
- Customers maintain complete control over their IP routing
- Set a clear demarcation of functionality between service provider and customer
- Facilitates troubleshooting
- Eases provisioning using MRV's unique VPLS auto-discovery protocol
- Flexible subscriber bandwidth allocation from 64 Kbps to 1 Gbps (compared to FR 'step-function' in DS1/DS3 multiples)

VPN Services

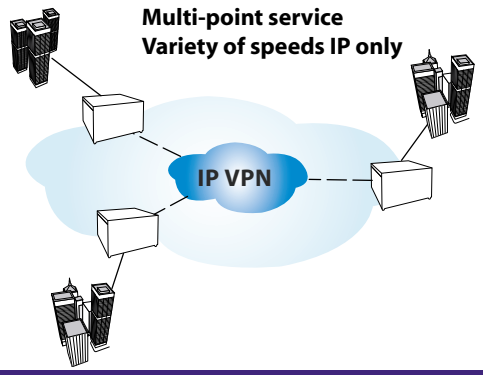
Customers can subscribe to any of the following VPN types:

Frame Relay

Frame relay has been the most common service offering in the industry. Since the service provider simply offers site-to-site links that could be a full mesh or hub topology, the customers have to design, manage, and maintain their own WAN access router equipment.

IP VPN

IP VPN services have been deployed by more than 80 carriers worldwide between multiple sites. IP VPNs are dynamic, flexible, and scalable, and can be delivered over existing services such as leased lines, Frame Relay, as well as ATM. The IP VPN services are based on RFC2547 and are used to interconnect customer routers at each site. However, the service provider has to terminate each site and set up routing between these sites. The service provider has to become involved with the customer's routing plan, which means that the customer may call the service provider to debug each routing problem even though the problem is within the customer's own network. This service does not suit some customers, who may be reluctant to give up control of their IP routing system to the service provider. This dilemma is resolved by VPLS.



MRV VPLS Solutions

MRV VPLS Auto discovery

Auto-discovery is absolutely critical in enabling service providers to keep operation simple and cost-effective, as it automates the creation of the LSP mesh. This is of major importance as it supports the automatic creation of the LSP mesh.
MRV supports the VPLS connectivity draft lassere-Vkompella, currently the dominant draft.
MRV also supports the unique auto-discovery protocol (based on the draft sodder) over LDP which makes VPLS implementation simple.

Vendors	Implemented Draft	Signaling Protocol	Auto discovery Protocol
Juniper	Draft Kompella	VPLS BGP	BGP
MRV, Alcatel, Riverstone,Tellabs & etc….	Draft Lasserre- Vkompella	VPLS LDP	None
MRV	Draft-sodder-ppvpn-vhls-02.txt	VPLS LDP	LDP

Protocols used by Vendors to Perform Auto-discovery

To understand MRV's auto-discovery feature, suppose that a new subscriber is added to a VPLS service by the carrier. By using MRV's auto-discovery, the subscriber is simply added to the VPLS service.
For performing auto-discovery, MRV exploits LDP, which in any case is the vehicle used for VPLS connectivity according to draft lassere Vkompella. Auto-discovery finds newly connected VPLS PE routers and adds the new subscribers to the correct VPLS instance. The alternative is to carry out all the above in a difficult manual manner.
In addition, the existing PE routers are "aware" of the new PE router and these PE members have all the requisite information needed to establish LSPs with the new PE router automatically.
In the event the subscriber leaves the service, the auto-discovery protocol automatically removes the connections to it.

VPLS Signaling

VPLS discovery methods have not been finalized yet in an existing standard proposal. Still, the vendors use several vehicles such as BGP, DNS, LDP, and RADIUS to overcome the discovery challenge.
The implementation in the OSM is based on the auto-discovery algorithm described in draft-sodder-ppvpn-vhls-02. It consists of two steps:

1. Identify all the other VPLS-speaking routers in the network and open a session with them.
2. Exchange VPLS service IDs over those sessions to learn which VC should be opened to which peer.

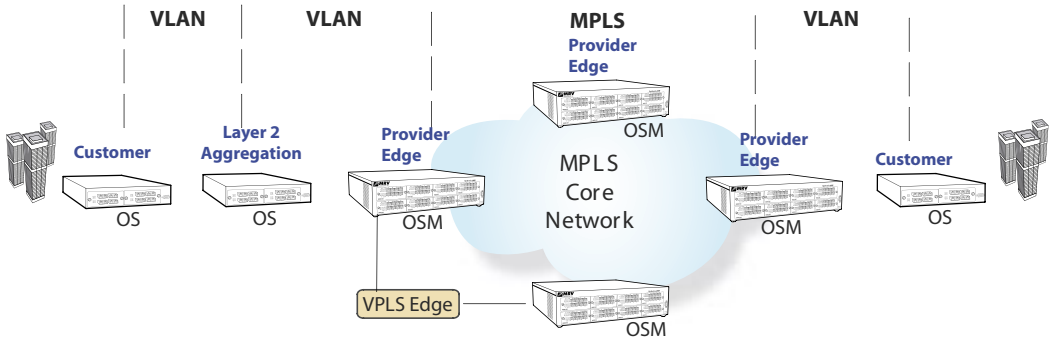
The most attractive feature of VPLS is simplicity. Instead of requiring customers to connect to an IP network, with the complexity of IP routing protocols, they connect with raw Ethernet, which allows a wider range of network architectures, protocols, and capabilities. All of this is provisioned using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

VPLS Service Implementation

VPLS services are implemented in the MRV's OSM family of routers. Once the OSM receives a configuration of a VPLS instance with a list of peers, it creates VCs (Pseudowires) to each peer. All the VPLS VCs are signaled with the VPLS ID. The VPLS instance can then be assigned to a logical interface. The OSM maintains a separate Layer 2 learning table for each logical interface. For specific VPLS instances, 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 searches the corresponding logical interface learning table, for an entry matching the frame's destination MAC. If such an entry exists, the frame is forwarded according to the entry's data to the appropriate PseudoWire or logical interface port. If it does not, the frame is flooded on all the interface ports as well as on VCs that belong to the same VPLS instance.
In order to populate the learning table, the OSM searches the learning table also for the frame's 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 interface ports, subscribers, and VCs.
Another useful feature of the OSM is its ability to limit the learning table size per logical interface. This feature is particularly important to the service provider who wants to prevent a specific service user from saturating the entire learning table with his/her own MAC addresses, and consequently abusing the service and creating Denial-of-Service (DoS) attacks.
As in the case of the L2 VPNs, the "hard work" is done by the LERs. The interior LSRs perform simple label switching and running of the LDP.

Subscriber Management and MPLS/VPLS

The OSM can act as a provider edge-router terminating subscribers. Each subscriber is identified according to source port and/or 802.1Q tag. The same tag used on different ports is treated as separate subscribers. This means that the OSM subscriber scheme overcomes the 4K global tags limitation.
Each subscriber can be connected to a Layer 2 point-to-point VPN based on the martini draft, or 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. Concurrently, 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.



Conclusion

VPLS has received widespread industry support from both vendors and service providers and is becoming one of the fastest emerging VPN services.
It offers flexible connectivity and a cost-effective solution for enterprise customers and carriers, VPLS simplifies the network management and reduces involvement of the service provider in the customer IP scheme.
VPLS enables the carrier/service provider to implement a scalable VPN solution from 64 Kb/s to 1 Gb/s.
MRV's auto-discovery protocol enables simple and easy VPLS service discovery and automatically adds new PE routers to an existing VPLS service.