VPLS/L2VPNs:
Virtual Private LAN Services using
Logical PE Architecture

Abstract
Consider a common network scenario in the metro area where the service provider offers Virtual Private LAN services (VPLS) known also as Transparent LAN services (TLS) to a large number of customers attached to low-cost Ethernet provider devices. These devices specialized mostly for Ethernet based functions (e.g., MAC learning, etc) may not have adequate resources and functions compared to provider devices offering large scale layer-2 or layer-3 VPN services. Consider also the case where those devices are themselves attached to either switched Ethernet networks or through uplinks to other provider edge devices, which are attached to a core IP/MPLS network infrastructure. The problem is how to provide a network-based VPLS solution that scales to a large number of VPLSs, each with a large number of customer ports while at the same time the solution should be cost-effective at service provider network-edges. This draft introduces the "Logical PE" architecture to effectively address this problem.

1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

2. Introduction

Consider a common network scenario in the metro area where the service provider offers Virtual Private LAN services (VPLS) known also as Transparent LAN services (TLS) to a large number of customers attached to low-cost Ethernet provider devices. These devices specialized mostly for Ethernet based functions (e.g., MAC learning, etc) may not have adequate resources and functions compared to provider devices offering large scale layer-2 or layer-3 VPN services. Consider also the case where those devices are themselves attached to either switched Ethernet networks or through uplinks to other provider edge devices, which are attached to a core IP/MPLS network infrastructure. The problem is how to provide a network-based VPLS solution that scales to a large number of VPLSs, each with a large number of customer ports while at the same time the solution should be cost-effective at service provider network-edges. This draft introduces the "Logical PE" architecture to effectively address this problem.

Architecting a scalable network based VPLS solution faces challenges related to the nature of the Ethernet technology itself and the network-based VPLS mechanisms used. Most of existing VPLS solutions attempt to address the VPLS architecture within a problem space similar to the layer-3 and point-to-point layer-2 VPN. Although the layer-3/2 VPN problem space is indeed part of the VPLS problem space, it doesn't fully meet all the
Layer-2 VPN solutions extend the concept of traditional layer-2 circuits to accommodate VPN constructs like membership, auto-discovery, tunneling, and topology discovery. The mechanisms developed within these solutions (e.g., [BGP-AD]) can greatly benefit scaling VPLS architectures. VPLS Scalability is addressed mostly from aggregation and auto-discovery mechanisms. Aggregation offers the ability to multiplex multiple VPNs over shared network pipes. Auto-discovery provides the ability to dynamically discover the VPN members and hence simplifies service provisioning within the network (e.g., single ended provisioning).

An Ethernet VPLS based solution is required to meet the scaling requirement where the PEs facing customer devices and attached to a core network need to perform MAC learning for all the VPLS services. In addition to providing VPLS services, the PEs may also be used to provide other VPN services (like layer-3 VPNs or point to point L2VPNs).

One way of achieving both scaling and cost objectives is to distribute some of the VPLS and VPN functions like MAC learning, auto-discovery, and aggregation among low-cost Ethernet based provider edge devices (facing customer devices) and high capacity core provider edge devices (attached to service provider core network). A service provider may want to use a "logical PE" function based on association between PE-facing customer ports, called "PE-Edges", and core provider edge devices, labeled as "PE-Core". Another objective of the logical PE approach besides scaling is to be able to fit nicely with all existing VPLS network technologies supported on the service provider network (VPLS/58), [VPLS-REQ], [VPLS-ROSEN].

3. Logical PE Architecture

This section describes the LPE architecture with its related building blocks and functions.

3.1 VPLS/L2VPN Reference Model

The VPLS network reference model follows the model described in [VPLS-REQ] and [VPLS-ROSEN]. A service provider may offer VPLS services where a customer edge device (CE), which can be a layer 2 Ethernet switch, a server, a router, a routing switch or an Ethernet bridge is attached to a service provider edge device. PEs are connected to internal provider devices (P) which are considered VPLS unaware. This reference model is similar to existing layer-3 and point-to-point reference models.

3.2 VPLS LPE Reference Model

The logical PE architecture addresses network scenarios when PEs facing customer devices is connected to some switched Ethernet transport networks or uplinks attached to other PEs which are attached to a core network infrastructure. In the example illustrated in figure 1, from a conceptual view PEs facing customer equipment (and not attached to the core network) combined with PE attached to the core network represent from a conceptual view a "logical PE" construct where many VPLS along with other layer-2 and layer-3 VPN services are attached to it.
To highlight the case described in Figure 1, we label each PE within the network as a PE-Edge or PE-Core depending if the PE is attached to the core network or not (and depending if there is a functional relationship between the PE-Edge and the PE-Core). PEs who do not participate in these schemes are not labeled. This model extends the previous L2VPN model described in the section 2.5.1. Using Figure 1, PE1, PE7, PE5, PE6 can be labeled PE-Edges while PE2, PE3, PE4, and PE8 are labeled PE-Cores.

Within the LPE reference model, a CE can be attached to one or more than one PE-Edges. However, connecting to more than one PE-Edge may require the PE-Edges to participate in customer spanning tree protocol.

PE-Edges can be connected through the Switched Ethernet transport network or direct links to one (or more) PE-Core(s).

Within the LPE reference model, the CE can be attached to PE-Edges and PE-Cores using Ethernet ports. Within a Switched Ethernet transport domain, all devices within the switch Ethernet transport domain will receive an Ethernet broadcast message sent onto the switch Ethernet transport domain. Within a carrier's metro Ethernet network, there can be multiple Switched Ethernet transport domains. PE-Cores like any other PEs can provide VPLS, layer-2, and layer-3 VPN services - PE-Cores are connected to each other over core network (e.g. MPLS) through P devices as usual VPN architectures (PPVPN-REQ).

Logical PE concept can be used in situations requiring high scalability in terms of number of VPLSs and port density while aiming towards reusing low-cost PE devices. LPE can be used in situations where the provider PEs don't have equal weight with respect to resource availability and full VPN functionality supported.

Logical PE also allows a provider to gracefully introduce MPLS functionality into their existing 802.1Q or stacked Q-tag Ethernet network. One migration path is that the existing customer facing devices will evolve into PE-Edges devices. These PE-Edge devices need not be MPLS aware and can remain simple from the control plane side. PE-Edge to PE-Edge communication can continue to be carried over the existing switch Ethernet transport network. PE-Core can then be added into the switch Ethernet transport network to provide connectivity to the IP/MPLS core. The grouping of PE-Core, PE-Edge, and Switched Ethernet transport devices can give the appearance of a PE from other PEs across the IP/MPLS core.

3.3 Logical PE

A logical PE (LPE) is a PE constructed by distributing VPLS functions across PE-Edges and PE-Cores interconnected by Switched Ethernet transport network(s) or one or more than one uplink.
PE-Edges interoperate with other PE-Edges between different Logical PEs and within the same Logical PE. PE-Edges interconnected through a switched Ethernet transport domain can inter-operate without involvement of PE-Cores. A network consists of only PE-Edges can also deliver low-scale VPLS services. The PE-Cores provide intermediary functions to enable PE-Edges to interoperate with PEs outside their local Switched Ethernet Transport domain. This may be with another PE or with PE-Edges in other Logical PEs, with PE-Edges in the same LPE but belonging to different switched Ethernet transport domain.

PE-Cores can also offer VPLS services for directly connected CE. Finally, when LPEs are used they can communicate with conventional PE devices that are not associated with any PE-Edges.

Inter-site connectivity between PE-Edges sharing the same switched Ethernet transport domain need not involve PE-Core. Inter-site connectivity between PE-Edges in different switched Ethernet transport domains within the logical PE need not involve any PEs outside of the logical PE. PE-Cores are connected in a fully mesh topology of transport tunnels across the core network.

PE-Edges see only PE-Cores and other PE-Edges in the same switched Ethernet transport domain, therefore there is no direct full meshing between PE-Edges across the core network, and any inter-site connectivity between PE-Edges across the core network will traverse the PE-Cores.

3.4 PE-Core and Source MAC Learning Implementation

The logical PE can be built with a PE-Core with or without source MAC learning capabilities. A PE-Core needs to perform source MAC learning in situations where VPLS customer sites are attached to the PE-Core. However, when no customer sites are attached to a PE-Core, the LPE will perform MAC learning function only at the PE-Edge level.

3.5 Network Connectivity within the Logical PE

Various network configurations can be implemented within the Logical PE. This section describes some of these configurations (the LPE scheme is flexible enough to support many other configurations).

3.5.1 PE-Edges connected directly to the PE-Core

In this configuration the PE-Edges are connected directly to the PE-Cores using single line Ethernet trunks. For enhanced reliability the PE-Edges can be connected to the PE-Core via two Ethernet trunks where the PE-Core which can be used for load sharing and for recovery from link and device failures.

3.5.2 Multiple Broadcast Domains in Logical PE

In this case, a single PE-Core can be connected to PE-Edges via multiple Switched Ethernet Transport domains. An implementation example of Switched Ethernet Transport domain is Resilient Packet Rings (RPR).

3.6 Functional Elements of the Logical PE

Following sections describe a list of PE functions that can be distributed in forming a LPE:

3.6.1 MAC learning

To provide VPLS service, the provider network is required to learn customer MAC addresses and their associated customer sites. MAC learning refers to the learning and aging the L2 forwarding tables based on MAC addresses received from customer packets.

3.6.2 Participation in customer Spanning Tree Protocol (OPTIONAL)

Provider VPLS network can participate in customer STP to avoid loops in the customer network for multi-homed customers or customers with backdoor connectivity. This is an OPTIONAL function.

3.6.3 Transport tunnel within the LPE

IP/VPLS based tunnels can be used in the core network. Since the PE-Edge and PE-Core devices are connected via switched Ethernet transport domains, Ethernet header can be used as a form of transport tunnel between PE-Edges and PE-Core devices.

3.6.4 Service label de-multiplexing within LPE

De-multiplexing header used to identify the service within a transport tunnel. Mechanism analogous to the "VC label" stated in [MARTINI-ENCAPS] can be used.

3.6.5 PE-Edge/PE-Core auto-discovery Mechanism (LPE-AD)

A lightweight protocol needs to be established between the PE-Edge and PE-Core for VPLS information exchange (e.g., membership, tunneling, etc). An example of functions provided by an LPE-AD:

- Notification of endpoint Addition, Deletion, Modification of VPLS.
- Service Label/Tunnel information exchange within the LPE.
- Addition/Deletion/Modification of PE-Edges.

3.6.6 Customer traffic prioritizing, policing, and shaping
Function includes ingress classification, metering, policing, and egress shaping of customer traffic at the provider boundary.

3.6.7 Customer VLAN processing
On customer facing interfaces where the provider recognizes and acts on customer 802.1Q tagged frames.

3.6.8 VPLS membership determination
A VPLS service visible at the LPE level can be created either at the PE-Edge or the PE-Core or both. A VPLS solution is a port-based VPN type architecture. Therefore, the VPN membership is accomplished by configuring customer facing ports and associating the port/endpoints to the VPLS VPN membership scheme.

3.6.9 Topology
Full mesh transport tunnels with other PE device across the core.

3.6.10 VPLS auto-discovery between PEs
On the core network, point-to-point circuits can be created using either [L2VPN-KOMP], or [Martini-TRANSP] with extensions to accomodate signaling/auto-discovery VPLS service information. For example, [Martini-TRANSP] type signaling can be used to create VC LSPs between virtual endpoints. In this scheme, the auto-discovery mechanism is decoupled from signaling. LDP-DU can be used where the VPEC will carry VPLS membership scheme (e.g., VPN-ID) and relevant information about VPLS endpoints (new VFEC parameter IDs can be defined for carrying such information).

BGP based auto-discovery mechanism can also be used in the core to inform each PE about VPLS membership information (e.g., described in [BGP-AD], and [L2VPN-KOMP]).

3.6.11 VPN Membership Mapping from within LPE domain to core domain (OPTIONAL)
Typically a VPLS is associated with a VPN-ID, which uniquely identifies the VPLS across the service provider network. An example of VPN-ID format can be found in [RFC-2685]. This draft doesn't preclude the use of other schemes for VPLS membership as those used in layer-3 and optical VPNs (e.g., route-target schemes).

It may happen that a VPLS has dual membership schemes within the LPE and inter-LPE on the core network. In this case, a VPN membership mapping function is needed at the LPE level.

3.6.12 Forwarding Plane Mechanism Translation
Mechanism in the forwarding plane within the LPE can be different than the forwarding plane mechanism in the core network. For example, with the existence of switched Ethernet transport networks within the LPE, a form of forwarding plane mechanism within the LPE can be Ethernet.

4. LPE Functional Distribution
Distribution of Logical PE functions is primarily determined upon the VPLS architecture model used. This section discusses one such possible distribution of these LPE functions.

In most cases, the PE-Edge provides such functions as managing the SLA including bandwidth policing, traffic classification and QoS, as well as customer Ethernet frame encapsulation, and MAC and VLAN learning. Also, in most cases, the PE-Core maintains membership information and performs VPN membership determination and advertisement to all the PE-Cores members of the same VPLS.

By using a signaling and/or an auto-discovery mechanism, the PE-Core distributes the VPN and/or endpoint related information to all PEs/LPEs across the core. Such distribution can be constrained to only the PEs/LPEs that have VPLS membership in common.

4.1 PE-Edge Functions
Typically a PE-Edge being a bridge, a routing switch, or a router will perform regular Ethernet based functions. Among these functions:
- MAC learning
- Participation in customer Spanning Tree Protocol (OPTIONAL)
- Transport tunneling within the LPE
- Service label de-multiplexing within LPE
- PE-Edge/PE-Core auto-discovery Mechanism (LPE-AD)
- Customer traffic prioritizing, policing, and shaping
- Customer VLAN processing
- VPLS membership determination
- VPLS configuration (depending on the configuration model)

4.2 PE-Core Functions
A PE-Core being attached to an IP/MPLS network and providing other VPN service than just VPLS should provide the following functions:
- Transport tunnel within the LPE
- Service label de-multiplexing within LPE
- PE-Edge/PE-Core auto-discovery Mechanism (LPE-AD)
5. LPE Configuration Models

A VPLS service can be configured on the PE-Edge or PE-Core or using a service provider network management system to configure both PE-Edge and PE-Core. The LPE-AD auto-discovery conveys configuration data between PE-Edge and PE-Core. The information needed on the PE-Edge/PE-Core relates to the VPLS membership scheme, the port/endpoint configuration. It may happen that a different membership scheme is used intra-LPE than the membership used inter-LPE, in this case a mapping function is used to maintain unique VPLS membership across the service provider network.

6. Quality of Service

Intra-LPE or inter PE-Core connectivity can be traffic engineered. RSVP-TE/CR-LDP can be used at the core and/or switched Ethernet transport. Customer traffic can be policed and shaped at the access port on the PE-Edge. The customer traffic is classified on the PE-Edge, and is mapped onto the endpoints VC-Labels. Most generally priority configured per access port (at the PE-Edge level) maps the customer 802.1p traffic to the network priority tunneling. This mapping is based on customer VPLS SLA.

7. LPE Resiliency

VPLS/L2VPN architecture resiliency is key to ensure service availability in presence of failures. Indeed, VPLS, like any layer-2 scheme is subject to failures like link, trunk, node failures.

Within the logical PE, failures can appear at the PE-Edge, PE-Core, the PE-Edge/PE-Core interconnecting link or switched Ethernet network. Dual PE-Cores can be used to protect the LPE failure and VPLS failures. Although using two dual PE-Cores, the LPE appears to the network as a single LPE.

8. Security Considerations

VPLS security needs to be considered within the LPE and inter-LPEs.

Within the LPE Customer traffic needs to be separated within the LPE. Ethernet Qtag, MPLS/IP based tunneling can be used. The level of data path security is same as ATM or FR networks. This document doesn’t preclude the use of encryption mechanisms within the LPE (although not recommended, particularly if Ethernet switched transport is used).

Inter-LPE security is provided within the layer-2 VPN architecture. A range of security parameters can be used, from using link layer type security to full encryption and authentication. An inter-domain solution usually requires some security mechanism across provider boundaries. For full inter-provider security (only when needed), IPSec tunneling mechanism is recommended.

9. References


progress.


10. Acknowledgments.

We would like to acknowledge the following individuals for their constructive comments: Marc Holness, Paul Valentine, Phil Edholm, San Sigarto, Bilal Jamoussi, Frank Neill, Liam Casey, Wai-Chai Chan, Weson El-Bakoury, Dinesh Mohan, Paul Knight and many other people who contributed to the concept of logical PE.

11. Intellectual Property Considerations

Nortel Networks may seek patent or other intellectual property protection for some or all of the technologies disclosed in this document. If any standards arising from this document are or become protected by one or more patents assigned to Nortel Networks, Nortel Networks intends to disclose those patents and license them on reasonable and non-discriminatory terms.

12. Author's Addresses

Hamid Ould-Brahim
Nortel Networks
P O Box 3511 Station C
Ottawa ON K1Y 4H7 Canada
Phone: +1 (613) 765 3418
Email: hbrahim@nortelnetworks.com

Vasile Radoaca
Nortel Networks
600 Technology Park
Billerica, MA 01821
vasile@nortelnetworks.com
978-288-6977

Michael Chen
Nortel Networks
4010 E Chapel Hill-Selma Iw
Research Triangle Park, NC 27709 USA
Phone: +1 (919) 997 3840
Email: mchen@nortelnetworks.com


Pascal Menezes
Terabeam Networks
2300 Seventh Ave
Seattle, WA, USA
98121
Access Line and Fax : 206 686-2001
email: pascal.menezes@terabeam.com