Service Requirements for Ethernet based L2VPNs

draft-ouldbrahim-ethernet-l2vpn-requirements-00.txt

Abstract

This document addresses service requirements for provider provisioned Ethernet layer 2 VPNs.

1. Sub-IP ID Summary

This document addresses service requirements for provider
provisioned Ethernet layer-2 virtual private networks.

RELATED DOCUMENTS

See also the reference section.

WHERE DOES IT FIT IN THE PICTURE OF THE SUB-IP WORK

Fits the PPVPN box.

WHY IS IT TARGETED AT THIS WG

This WG is looking at Layer-2 VPN using IP related building blocks. This work is in scope with such objective.

2. Introduction

This document addresses service requirements for provider provisioned Ethernet layer-2 virtual private networks.

3. 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].

4. Ethernet Layer-2 VPN Reference Model

A service provider may offer an Ethernet layer-2 VPN service (E-L2VPN) 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 network infrastructure. A CE can be attached to one or more than one provider edge devices (PE). PEs are attached to internal provider devices (P).

The Ethernet L2VPN network reference model follows the model described in [PPVPN-REQ]. It may happen that a PE providing the service is connected to some layer-2/3 networks attached to another PE/P and then to a core network infrastructure. For easy reference we call such networks as access networks to indicate access to the core network infrastructure. A PE attached to such networks and a core network may provide both PE and P functionalities. The access network(s) can be an Ethernet, an IP, MPLS, or a resilient packet ring (RPR) network or any layer-2 network (e.g., ATM, FR). In the example
illustrated in figure 1, from a conceptual view PEs at the access combined with PE providing also P functionality represents a "logical PE" construct where many E-L2VPN services are attached to it.

Figure 1: E-L2VPN Network Configuration with access networks

Figure 2 below describes examples of inter-site connectivity scenarios provided for network configuration described in figure 1. The E-L2VPN service can be built between site-1 and site-5 across a single transport tunnel. Other alternative is to connect site-1 and site-5 through a set of tunnels combining both access and core tunnels. On the other hand, an E-L2VPN service that connects site-1 and site-2 can be built without the need to cross the network core.
5. Service Requirements

A service provider may offer Ethernet L2VPN services over single or multiple network infrastructures where the E-L2VPN service topology can be point to point, point to multipoint, or multipoint to multipoint.

1) The E-L2VPN service MUST provide transparent transport of customer traffic across the service provider network including the transport of customer information such as "P" bit, spanning tree, VLAN type information when required by the service.

2) The E-L2VPN service SHOULD support the ability to transport customer traffic through multiple layer-2 technologies (e.g., Ethernet to ATM, or FR, etc). For this reason access networks can be built and interconnected using multiple layer-2 technologies [RFC-1483], [RFC-1490].

3) The E-L2VPN service MUST be independent of the Ethernet transfer rate. The service MUST support 10, 100, 1 GE, 10Ge etc. Therefore the E-L2VPN architecture MUST accommodates all these service rates.

4) The Ethernet over MPLS encapsulation SHOULD follow the rules defined in PWE3 working group for Ethernet (e.g., [ENCAPS]).

5) For scalability purposes, the tunneling/encapsulation technology used in the access and in the core networks SHOULD support demultiplexing capabilities.

6) The E-L2VPN service SHOULD provide the ability to police and/or shape customer Ethernet traffic.
7) The E-L2VPN service can be associated with one or many VLANs. Such association is at the discretion of the service provider and E-L2VPN customer.

8) The E-L2VPN service SHOULD provide priority handling of customer Ethernet frames when traversing the service provider network.

9) The E-L2VPN service SHOULD preserve priority levels of customer incoming Ethernet frames (e.g., [802.1P]).

10) The Tunneling used in the access may have no relation to the tunneling used in the core.

11) The E-L2VPN service SHOULD accommodate different types of tunneling (e.g., MPLS, IP, Ethernet, etc.) within the service provider network(s) (including at the access network level).

12) In the situation where a PE is attached to both a core network and access networks, it is desirable that this PE provides both PE and P functionalities.

13) The E-L2VPN service SHOULD be able to use VPN service label with another non MPLS tunneling mechanism in the access and in the core network.

14) The E-L2VPN service SHOULD be able to provide OAM management capabilities (e.g., using a label stack approach [OAM]).

15) When an access network is used it SHOULD support aggregation and switching in the transport layer-2 domain.

16) For the control and provisioning of the E-L2VPN service, both distributed control mechanisms and centralized control mechanisms SHOULD be supported.

17) To provide E-L2VPN service that scales to a large number of customers, no single component of the service provider networks should be required to maintain all the information about all the E-L2VPNs.

18) For scalability purposes, it SHOULD be desirable to minimize the amount of configuration changes when adding/deleting an Ethernet port to/from a given E-L2VPN. For the same reasons, it is also desirable that configuration/provisioning changes of a port to/from a given E-L2VPN SHOULD involve configuration/provisioning only on the device that this port is connected to.
19) The E-L2VPN service SHOULD support the case where E-L2VPN spans multiple (interconnected) service providers or multiple networks within a single service provider.

20) The E-L2VPN SHOULD be able to provide access to existing service provider VPN infrastructure (e.g., layer-3 VPNs, Optical VPNs) with minimal disruption to the service provider existing VPN infrastructure.

21) For the same reason, an E-L2VPN service SHOULD, when possible, maximize reusability of existing VPN service and technology building blocks already deployed (e.g., management tools, membership schemes, etc.) and being standardized in the IETF.

22) As value added E-L2VPN services, service provider MAY provide auto-provisioning tools to facilitate customer ordering. (e.g. web ordering, "point-and-click" solutions). Service provider MAY also provide its customer with customer specific report via web access or other means.

23) Operator should have the capability to display the E-L2VPN topology on a per E-L2VPN basis or multiple E-L2VPN basis.

24) The E-L2VPN service MUST allow layer-2 addressing used by the Service Provider network offering the service to be completely independent from the addressing used by the E-L2VPN services. Moreover, for the purpose of the E-L2VPN service, addressing used by one E-L2VPN service, need not be coordinated with any other E-L2VPNs.

25) The E-L2VPN service SHOULD provide the ability to test and do some operational and maintenance activities per E-L2VPN service basis.

26) The E-L2VPN service SHOULD collect statistics to allow the Service Provider to monitor and report on the performance of the service to the E-L2VPN customer.

27) The E-L2VPN service SHOULD provide as an added value the ability to constrain and enforce the set of E-L2VPN topologies that can be built across the service provider network infrastructure (e.g., hub and spoke, full mesh, arbitrary, etc.).

6. Security Considerations

[TBD]

7. References
8. Acknowledgments.

We would like to acknowledge the following individuals for their comments: Gary Southwell, John Beatty, Don Ellis, Wai-Chau, David Allen, Greg Wilbur, Greg Wright, Robert Eros, Bilel Jamoussi and Silvestro Taddio. Special thanks to the authors of [OVPN-REQ] as some of the above requirements have been inspired by the list of requirements listed in [OVPN-REQ].

9. 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.

10. 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
Francis E. Neil (Nortel)
600 Technology Park Drive
Billerica, MA, 01821
USA
fneil@nortelnetworks.com

Frank Palermo
Nortel Networks
8200 Dixie Road
Brampton, ON L6T 4B8
palermof@nortelnetworks.com

Vasile Radoaca
Nortel Networks
600 Technology Park
Billerica, MA 01821
vasile@nortelnetworks.com
978-288-6097

Juan Manuel Ramos-Gurrion
Bell Canada
700 de la Gauchetiere Ouest, bureau 18-02
Montreal, Quebec
Canada
514 870 3060
juan_manuel.ramos-gurrion@bellnexxia.com

Paul LeBel
Bell Canada
700 de la Gauchetiere Ouest, bureau 18-02
Montreal, Quebec
Canada
514 870 2807
paul.lebel@bellnexxia.com
Full Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.