Provider Provisioned VPN WG
Internet Draft

Elwin Eliazer (Corona)
Brijesh Kumar (Corona)
Benson Schliesser (SAVVIS)

Category: Informational
Expiration Date: August 2002

February 2002

PPVPN Architecture using L2TP

draft-elwin-ppvpn-l2tp-arch-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 [RFC-2026].

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."
The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html.

Abstract

This document discusses the use of L2TP for establishing PPVPNs. It proposes to use L2TP for VPN membership, topology discovery, and as a tunneling mechanism. The basic idea is based on leveraging the inherent strengths of L2TP for tunneling traffic, and extend the same advantages to PPVPNS. The mechanism is applicable for both Layer2 and Layer3 PPVPNs.

ID Summary

RELATED DOCUMENTS

See References section below.

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

This ID fits the PPVPN box.

WHY IS IT TARGETED AT THIS WG

This ID describes a tunneling and discovery mechanism for PPVPNs, which comes under the charter of this WG.

JUSTIFICATION

This ID describes a tunneling and discovery mechanism for PPVPNs, which comes under the charter of this WG.

Table of Contents

1.0 Introduction

The establishment of a PPVPN require three basic mechanisms: VPN membership and topology discovery, tunnel signaling and establishment, and route distribution [PPVPN-FW]. Currently, three different approaches have been proposed for distributing VPN discovery information:

(a) manual or SNMP based configurations at each PE
(b) centralized directory or database servers
(c) piggybacking onto a routing protocol such as BGP.

In this document, we make two new proposals. The first proposal is to use L2TP as a PPVPN tunneling protocol so that the benefits of L2TP as a tunneling mechanism for a variety of traffic classes are available to PPVPNs too. Secondly, we propose the use of L2TP to carry VPN discovery information as with simple extensions to L2TP, it can fulfill this role very effectively. Unlike extending a complex routing protocol such as BGP, L2TP extensions add no complexity to routing protocols, and carriers aren't forced to use BGP based discovery mechanisms for all their VPNs.

L2TP, a protocol originally meant to tunnel PPP, has decoupled itself from PPP, and currently can tunnel a variety of payload. The rich set of tunnel managment functions offered by L2TP is a valid candidate for PPVPN tunneling.

The use of L2TP for VPN discovery and tunneling has a second benefit that any IGP can be used for VPN related route distribution between two

PEs. One is not forced to use BGP for route distribution as is the case with some proposals such as BGP/MPLS VPNs in [RFC-2547].

2.0 L2TP for PPVPN Tunneling

PPVPNs inherently need a tunneling mechanism to tunnel over the public backbone. Signaling these tunnels reduces the amount of configuration needed in setting up and tearing down these tunnels. L2TP, a protocol originally meant to tunnel PPP, has decoupled itself from PPP, and currently can tunnel a variety of payload. The rich set of tunnel management functions offered by L2TP is a valid candidate for PPVPN tunneling.

Here we discuss the merits and demerits in using L2TP, to provide both Layer2 and Layer3 VPNs. We also suggest some simple extensions that can be made to L2TP which can help in PPVPN solutions.

Note:
VFI = Virtual Forwarding Instance. Refers to Layer-3 Virtual Router.
VSI = Virtual Switching Instance. Refers to a Layer-2 Virtual Bridge.
This terminology is used in the PPVPN requirement and framework docs.

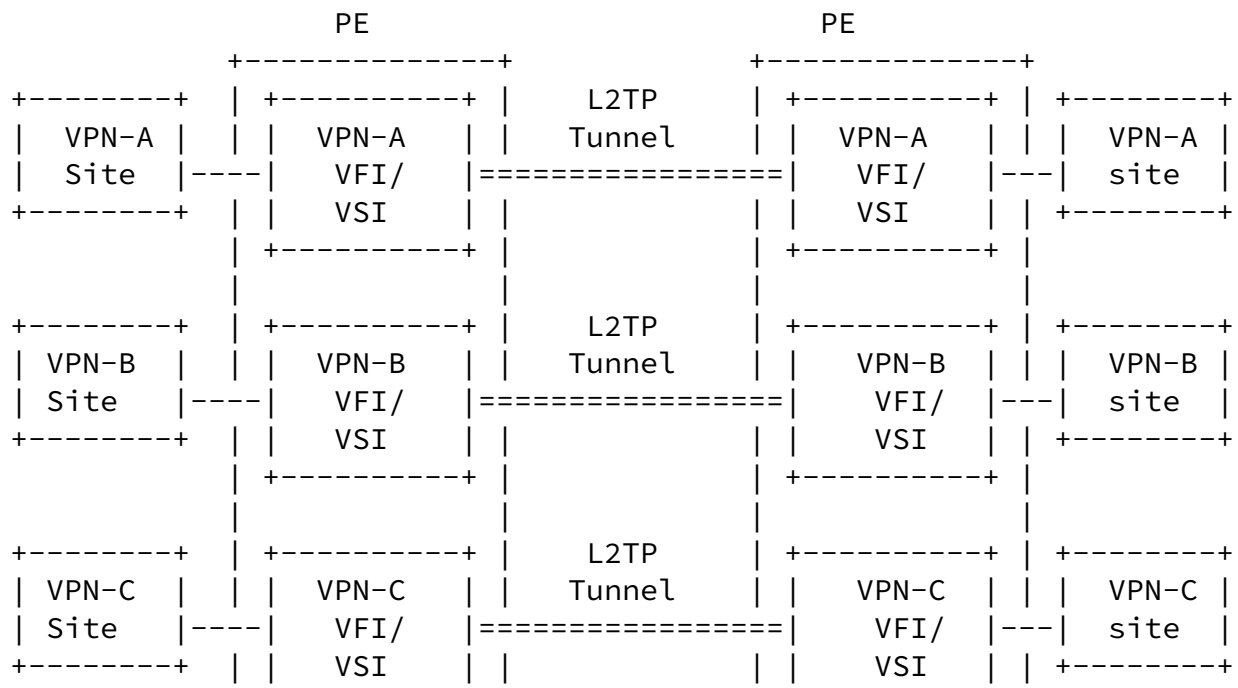

Figure 1: Reference Model

3.0 Merits and demerits with this approach

3.1 Merits

+ L2TP provides a good tunneling mechanism with an associated signaling protocol. The payload can carry IPv4 or IPv6 for L3 VPNs, or any L2 for L2 VPNs.

+ The tunnel encapsulation header has a hierarchical demultiplexing capability.

+ Keepalive for the tunnels are available.

+ Tunnel authentication is also available.

+ Tunneling is over IP and hence can work in both IP and MPLS networks.

+ Can work with IPSec in transport mode when security is needed. Thus IPSec can be made optional, based on the need.

+ Tunnel virtual interfaces can emulate real interfaces. If needed, any routing protocol can be run over this dynamic interface.

+ Decouples tunneling and VPN discovery, from learning of VPN routes.

+ L2TP Tunnel Switching can help in arriving at complex topologies.

+ VPN discovery and setup of tunnels can be automatically signaled with simple extensions.

+ Because keepalives are available, remote tunnel endpoint liveness can be easily detected. This could be of significant benefit, for VFIs and VSIs that are configured with static routes/forward entries.

3.2 Demerits

- L2TP, as it is widely deployed today is over UDP. This increases the PE processing, and also increases the encapsulation header size. There are means to bypass the UDP in L2TP, which is recommended for PPVPNs.

- L2TP tunnels, are inherently point-to-point tunnels. There is a proposal in L2TPext WG to support multicast tunnels. This will have to be explored for multipoint tunnels. Refer [L2TP-MLT].

4.0 PPVPN Services Using L2TP

4.1 VPN Membership Discovery

The VPN-ID format as defined in [RFC-2685] is used to identify a VPN. All VFIs/VSIs that are members of a specific VPN share the same VPN-ID.

L2TP control connection is made across each PE devices, in the case of fully mesh topology for control connections. Refer Section 3.6 for other control connection topologies.

VPN AVP in the L2TP Hello messages are used to determine any new VFI or VSI for a VPN coming up. Thus each PE gets to know the other PEs that have VFIs or VSIs corresponding to the VPNs it supports.

[L2TP-EXT] describe the L2TP extensions needed in detail.

4.2 VPN Topology

The desired VPN topology information for each PPVPN VFI/VSI can be specified as part of the VFI/VSI configuration.

Following topology values are defined:

```
     "Hub" -- Connects (tunnel) to all the spoke VFIs/VSIs
     "Spoke"  -- connects only to the hub VFI/VSI
     "Mesh" -- connects to all the other member VFIs/VSIs
```

Other topologies are to be handled in a similar way.

The tunnel switching capability in L2TP also help in defining the topology.

4.3 Tunnel Setup

Per VPN L2TP tunnel setup across each VFI (or VSI) pair is initiated by L2TP when it receives the membership and topology information.

If the PEs decide to use the same tunnel IP address for multiple VFIs or VSIs, the tunnel/session ID in L2TP can be used for multiplexing.

The tunnel endpoint IP addresses is learnt as part of the VPN membership discovery.

If security is needed on these tunnels, IPSec in transport mode is used on these L2TP encapsulated packets. Refer [RFC-3193].

4.4 Keepalive

The Hello messages in L2TP can be used to determine the control connection as well as the per VPN tunnel status.

4.5 Tunnel Authentication

The per VPN tunnels and the control connections can be authenticated with the L2TP tunnel authentication methods, when the tunnels are setup.

4.6 Control Connection Topology

The control connection tunnels are different from the per VPN tunnels, and they can have different tunnel endpoints.

To have control connections in a hub and spoke topology, a designated Tunnel Manager is chosen as the hub. This can be a PE or any device that is reachable to the PEs. All the spoke PEs are configured with the Tunnel Manager's IP address, as the control connection peer. The tunnel manager then resolves the perVPN tunnel endpoints, and lets the PEs setup the per VPN tunnels directly.

This can be extended with L2TP tunnel switching [L2TP-TSW]to achieve more complex topologies.

5.0 Applications

This approach is useful, but is not limited to, the applications listed in the following subsections.

5.1 OSPF/L2TP VPNs

OSPF running at the individual VPN sites, are connected together by the per-VPN tunnels provided by L2TP.

5.2 Ethernet/L2TP VPNs and other L2 VPNs.

Ethernet coming from the CEs of the VPN sites, are connected together by the per-VPN tunnels provided by L2TP. Similar approach is used for other L2s: Frame-relay, ATM, etc.

5.3 Remote Access L2TP/IPSec VPNs

Roaming or mobile remote access VPN clients, can access VPN nodes, by reaching a PE VFI using L2TP/IPSec tunnels. This can be directly handled in this model.

5.4 IPv6/L2TP VPNs

Islands of IPv6 networks, can be transported over a L2TP tunnel transparently so as to have a connected IPv6 network.

6.0 Comparison with other approaches

6.1 Other tunneling methods

IPIP tunnels:

This provides a simple tunnel encapsulation method. The disadvantages are:
- It has no associated signaling protocol.
- It has no demultiplexing field.
- There is no mechanism to determine the liveness of the tunnel enpoint, since there is no keepalive.

GRE tunnels:
Though this provides a demultiplexing field, this has no associated signaling protocol, and hence relies on external means to setup the tunnels. And no way to determine the liveness of a tunnel.

IPSec tunnels: [PPVPN-SEC]
With IPSec tunnels, either AH or ESP needs to be done and can not be made optional due to security reasons. These are operations involving scanning of the complete payload and hence expensive.
The other disadvantage is with the associated signaling protocol, IKE. IKE is not flexible for new additions and is not a protocol meant for setting up generic tunnels.

MPLS tunnels: [RFC-2547]
The problem with using MPLS tunnels is that it needs MPLS networks. Another disadvantage is that there is no means to determine the liveness of a tunnel, due to lack of keepalive mechanism.

6.2 Other VPN discovery methods

BGP-based Discovery: [BGP-AUTO]
This method suggests extensions to BGP to enable VPN discovery. For cases where BGP is not involved, this is an unnecessary involvement of BGP. For example, a Ethernet L2 VPN, do not need BGP to do VPN discovery.

Multicast-based Discovery: [RFC-2917]
This discovery method is based on multicasting, and hence assumes multicast enabled backbone, which is most of the times inappropriate.

7.0 Scalability Considerations

Both the Control Connection tunnels and Per VPN tunnels should be scalable to have a scalable PPVPN solution. The main scalability issue arises when a mesh topology is mandated for both the cases. The following sections describe how a mesh can be avoided.

7.1 Control Connection -- Scalability

As described in Section 4.6, mesh topology can be avoided by having a Tunnel Manager.

<More details to be done>

7.2 Per VPN Tunnels -- Scalability

L2TP Tunnel Switching [L2TP-TSW], helps in avoiding the need for a tunnel mesh.

<More details to be done>

8.0 Security Considerations

This approach suggests the use of L2TP alone for the cases where security is implicitly addressed for the cases like private backbones. For the cases where security is needed, we recommend the use of L2TP over IPSec, as described in [RFC-3193].

9.0 References

[BGP-AUTO] Ould-Brahim H., et al., "Using BGP as an Auto-Discovery Mechanism for Network Based VPNs", Work in progress, draft-ietf-ppvpn-bgpvpn-auto-02.txt

[L2TP-BASE] Lau J., et al., "Layer Two Tunneling Protocol, L2TP", Work in progress, draft-ietf-l2tpext-l2tp-base-01.txt

[L2TP-EXT] Stelzer E., Gowda N., "L2TP Extensions for PPVPN", Work in progress, draft-elwin-l2tpext-ppvpn-00.txt

[L2TP-MLT] Bourdon G., "L2TP Multicast Extension", Work in progress, draft-ietf-l2tpext-mcast-01.txt

[L2TP-TSW] Jain V., et al., "L2TP Tunnel Switching", Work in progress, draft-ietf-l2tpext-tunnel-switching-01.txt

[PPVPN-FW] Callon R., et al., "A Framework for Provider Provisioned Virtual Private Networks", Work in progress, draft-ietf-ppvpn-framework-03.txt

[PPVPN-L2] Rosen E., et al., "An Architecture for L2VPNs", Work in progress, draft-ietf-ppvpn-l2vpn-00.txt

[PPVPN-RQ] Carugi M., et al., "Service Requirements for Provider Provisioned Virtual Private Networks", Work in progress, draft-ietf-ppvpn-requirements-03.txt

[PPVPN-SEC] Gleeson B., "Uses of IPSec with Provider Provisioned VPNs", Work in progress, draft-gleeson-ipsec-ppvpn-01.txt

[PPVPN-VR] Ould-Brahim H., et al., "Network based IP VPN Architecture using Virtual Routers", draft-ietf-ppvpn-vpn-vr-01.txt

[RFC-2401] Kent S., Atkinson R., "Security Architecture for the Internet Protocol", RFC2401, November 1998.

[RFC-2547] Rosen E., Rekhter Y., "BGP/MPLS VPNs", RFC2547, March 1999.

[RFC-2685] Fox B., et al, "Virtual Private Networks Identifier", RFC 2685, September 1999.

[RFC-2917] Muthukrishnan K., Malis A., "A Core MPLS IP VPN Architecture", RFC2917, September 2000.

[RFC-3193] Patel B., et al., "Securing L2TP using IPSec", RFC3193, November 2001.

10.0 Acknowledgments

To be added.

11.0 Author's Addresses

Elwin Stelzer Eliazer
Corona Networks, Inc.
630 Alder Drive
Milpitas, CA 95035
Email: elwinietf@yahoo.com

Brijesh Kumar
Corona Networks, Inc.
630 Alder Drive
Milpitas, CA 95035
Email: brijesh@coronanetworks.com

Benson Schliesser
SAVVIS Communications
717 Office Parkway
St. Louis, MO 63141
Email: bensons@savvis.net