Abstract

This draft describes the emulation of an Ethernet segment or broadcast domain over an IP network and the use of L2TPv3 to transport Ethernet frames.

1. Terminology

LCCE     L2TP Control Connection Endpoint (See [L2TPv3])
NSP      Native Service Processing
PSN      Packet Switched Network
PW       Pseudo-Wire
PWE3     Pseudo-Wire Emulation Edge to Edge (Working Group)
VPL      Virtual Private LAN (aka Ethernet Pseudo-Wire)

2. Overview

To emulate an Ethernet broadcast domain, tunnels are setup between sites (LCCE) of a VPL. At a site, Ethernet traffic of a VPL is encapsulated in L2TP by a LCCE and transported over the IP network
to another LCCE of the VPL. The receiving LCCE decapsulates the Ethernet frame and forward the frame to the destination node in the VPL.

[L2TP-ETH] specifies the transport of Ethernet frames from one point to another point over L2TPv3. This draft describes the transport of Ethernet traffic across multiple sites that belong to the same VPL, including point to point transport of Ethernet frames using [L2TP-ETH] and bridging at LCCEs. The scope of the application of this draft in this initial version is [CE-VPL].
The following two figures (adapted from [PWE3-frame]) describe the reference models to support VPL services.

Fig 1 Emulated Ethernet Segment/Ethernet Pseudo-Wire

Expires June 2003                                               [Page 3]
3. Establishing L2TPv3 control connection and session

An L2TP control connection (as described in [L2TPv3]) is set up first to each peer LCCE of a VPL (See "Tunnel Endpoints Information"). Ethernet PW type must be included in the Pseudo Wire Capabilities list as described in [L2TP-ETH].

A point to point Ethernet PW to each peer LCCE belonging to the same VPL, is established as an L2TP session. A new PW Type namely, "Ethernet VPL" is defined. This parameter indicates to an LCCE whether additional processing wrt multipoint service is required. Each LCCE signals its PW type in a AVP [L2TPv3] Attribute Type TBA. The PW ID is associated with an L2TP session as described in [L2TP-ETH].

In this version of the draft, each L2TP session is associated with one VPL only. Hence an LCCE does not need to add a globally unique
identifier (VLAN ID) to frames for the purpose of identifying a frame as belonging to the emulated broadcast domain, although the traffic from a LAN site may or may not be VLAN tagged.

A virtual interface is created for every L2TP session setup to a remote LCCE.

### 3.1 Tunnel Endpoint Authentication

If an LCCE authenticates the remote LCCE using L2TP, a Challenge AVP is included in the L2TP control connection setup message, as described in [L2TPv3]. If the expected response received from a LCCE does not match, the establishment of the control connection MUST be disallowed. A CHAP-like [RFC1994] authentication is used at each LCCE. To use L2TP tunnel authentication, a single shared secret MUST exist between the two LCCEs. [See section on "Tunnel Endpoint Information"].

L2TP (Layer Two Tunneling Protocol) may use IPsec for tunnel authentication as described in [L2TP-IPSEC] instead.

### 4. Bridging

An LCCE learns MAC addresses from the customer facing ports and the virtual interfaces (or the tunnels to remote LCCE sites of a VPL). When a new MAC address is learned, the MAC address is associated with the virtual interface or ports where the frame arrives. When a frame with the cached MAC address is received, the LCCE knows which virtual interface or port to forward the frame to. When a frame with a new MAC address is received, an LCCE floods the frame to all other ports or virtual interfaces, except the interface where the frame is received from. To optimize forwarding of traffic over a VPL see the next section.

The learning, bridging, filtering and forwarding procedures are as defined in [802.1d] and [802.1q], except that the ports on a switch in this case can be a virtual interface as well as a physical port.

### 5. Optimizing bridging over a VPL

To optimize the forwarding of traffic in a VPL, a full mesh of tunnels may be setup among LCCE sites. Since each LCCE has a direct tunnel to other LCCEs, bridging may be modified such that traffic arriving at an LCCE from another LCCE need not be forwarded to other LCCEs. Spanning Tree Protocol (STP) may be turned off if there are no additional connectivity among the LCCEs (e.g. "backdoor" connectivity), apart from the full meshed of tunnels; otherwise STP must be used to prevent forwarding loops.
The states in setting up a full meshed of tunnels (over an IP network) are only incurred at LCCEs.

6. Tunnel Endpoints Information

How the configurable tunnel parameters (e.g. IP addresses of remote LCCEs) are obtained is not within the scope of this draft. [VPLS-DNS] and [CE-AUTOCONFIG] are examples of mechanisms that may be used to auto discover and distribute VPL site information.

7. PW Monitoring

The procedures for PW monitoring and fault detection described in [L2TP-ETH] may be used to monitor the virtual interfaces or L2TP sessions.

8. Acknowledgment

This draft benefited from discussions with Alexis Berthillier, Sasha Cirkovic, Arnold Jansen, Jeremy DeClercq, Jeanne DeJaegher and related discussions with the Ethernet over L2TPv3 design team, as well as consultations with Mark Townsley and Danny McPherson.

Normative References


Informational References


[CE-VPL] CY Lee, M Higashiyama, "CE-based VPL", (draft-lee-ce-based-vpl-00.txt), work in progress, July 2002

Authors’ Information

Cheng-Yin Lee Cheng-Yin.Lee@alcatel.com

Mitsuru Higashiyama Mitsuru.Higashiyama@yy.anritsu.co.jp

Expires June 2003