L2TPEXT Working Group Vipin Rawat
INTERNET DRAFT Cisco Systems, Inc.
Category: Internet Draft Rene Tio
Title: draft-ietf-l2tpext-fr-00.txt Redback Networks, Inc.
Date: July 2000 Rohit Verma
Deloitte Consulting

Layer Two Tunneling Protocol (L2TP) over Frame Relay
<draft-ietf-l2tpext-fr-00.txt>

Status of this Memo

Abstract

Layer Two Tunneling Protocol describes a mechanism to tunnel PPP sessions. The protocol has been designed to be independent of the media it runs over. The base

specification describes how it should be implemented to run over UDP and IP. This document describes how the Layer Two Tunneling Protocol MUST be implemented over Frame Relay PVCs and SVCs.

Applicability

This specification is intended for those implementations which desire to use facilities which are defined for L2TP. These capabilities require a point-to-point relationship between peers, and are not designed for multi-point relationships which is available in Frame Relay and other NBMA environments.

1.0 Introduction

L2TP [1] defines a general purpose mechanism for tunneling PPP over various media. By design, it insulates L2TP operation from the details of the media over which it operates. The base protocol specification illustrates how L2TP may be used in IP environments. This draft specifies the encapsulation of L2TP over native Frame Relay and addresses relevant issues.

2.0 Conventions

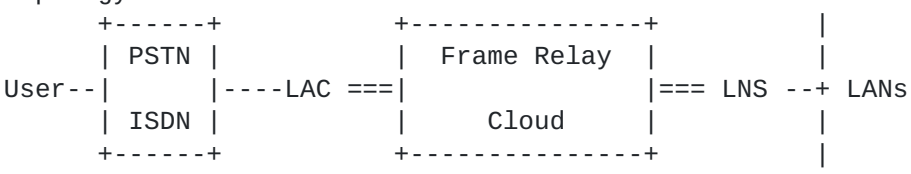
The following language conventions are used in the items of specification in this document:

- MUST, SHALL, or MANDATORY -- This item is an absolute requirement of the specification.
- SHOULD or RECOMMEND -- This item should generally be followed for all but exceptional circumstances.
- MAY or OPTIONAL -- This item is truly optional and may be followed or ignored according to the needs of the implementor.

3.0 Problem Space Overview

In this section we describe in high level terms the scope of the problem being addressed.

Topology:



L2TP Access Concentrator (LAC) is a device attached to the switched network fabric (e.g. PSTN or ISDN) or co-located with a PPP end system capable of handling the L2TP protocol. The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNS's. It may tunnel any protocol carried within PPP.

L2TP Network Server (LNS) operates on any platform capable of PPP termination. The LNS handles the server side of the L2TP protocol. L2TP is connection-oriented. The LNS and LAC maintain state for each user that is attached to an LAC. A session is created when an end-to-end PPP connection is attempted between a user and the LNS. The datagrams related to a session are sent over the tunnel between the LAC and LNS. A tunnel is defined by an LNS-LAC pair. The tunnel carries PPP datagrams between the LAC and the LNS.

L2TP protocol operates at a level above the particular media over which it is carried. However, some details of its connection to media are required to permit interoperable implementations. L2TP over IP/UDP is described in the base draft [1]. Issues related to L2TP over Frame Relay are addressed in later sections of this draft.

4.0 Encapsulation and Packet Format

L2TP MUST be able to share a Frame Relay virtual circuit (VC) with other protocols carried over the same VC. The Frame Relay header format for data packet needs to be defined to identify the protocol being carried in the packets. The Frame Relay network MAY NOT understand these formats.

All protocols over this circuit MUST encapsulate their packets within a Q.922 frame. Additionally, frames MUST contain information necessary to identify the protocol carried within the frame relay Protocol Data Unit (PDU), thus allowing the receiver to properly process the

incoming packet.

The frame format for L2TP is based on SNAP encapsulation as defined in RFC 1490 [5] and FRF3.1 [2] . SNAP format uses NLPID followed by Organizationally Unique Identifier and a PID.

NLPID

The single octet identifier provides a mechanism to allow easy protocol identification. For L2TP NLPID value 0x80 is used which indicates the presence of SNAP header.

OUI & PID

The three-octet Organizationally Unique Identifier (OUI) 0x00-00-5E identifies IANA who administers the meaning of the Protocol Identifier (PID) 0x0007. Together they identify a distinct protocol.

Format of L2TP frames encapsulated in Frame Relay is given in Figure 1.

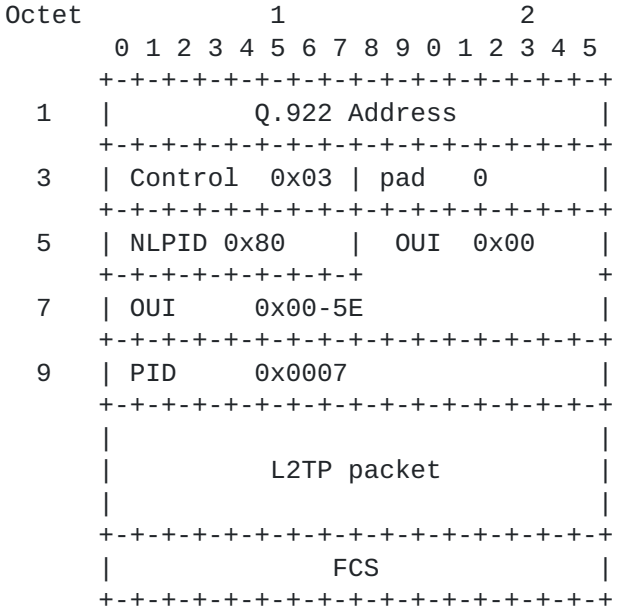


Figure 1 Format for L2TP frames encapsulated in Frame Relay

5.0 MTU Considerations

FRF.12 [4] is the Frame Relay Fragmentation Implementation Agreement. If fragmentation is not supported, the two Frame Relay endpoints MUST support an MTU size of at least PPP Max-Receive-Unit size + PPP header size + Max L2TP Header Size + Frame Relay header size (PPP header size is the protocol field size plus HDLC framing bytes, which is required by L2TP). To avoid packet discards on the Frame Relay interface, the RECOMMENDED default Frame Relay MTU is 1564 based on a PPP default MRU of 1500. The means to ensure these MTU settings are left to implementation.

6.0 QOS Issues

In general, QoS mechanisms can be roughly provided for with proprietary mechanisms localized within the LAC or LNS. Interworking issues with various QoS implementations is therefore at this time left as a topic for future study.

7.0 Frame Relay and L2TP Interaction

In case of Frame Relay SVCs, connection setup will be triggered when L2TP tries to create a tunnel. Details of triggering mechanism are left to implementation. There SHALL NOT be any change in Frame Relay SVC signaling due to L2TP. The endpoints of the L2TP tunnel MUST be identified by X.121/E.164 addresses in case of Frame Relay SVC. These addresses MAY be obtained as tunnel endpoints for a user as defined in [3]. In case of PVCs, the Virtual Circuit to carry L2TP traffic MAY be configured administratively. The endpoints of the tunnel MUST be identified by DLCI, assigned to the PVC at configuration time. This DLCI MAY be obtained as tunnel endpoints for a user as defined in [3].

There SHALL be no framing issues between PPP and Frame Relay. PPP frames received by LAC from remote user are stripped of CRC, link framing, and transparency bytes, encapsulated in L2TP, and forwarded over Frame Relay tunnel.

8.0 Security Considerations

Currently there is no standard specification for Frame Relay security although the Frame Relay Forum is working

on a Frame Relay Privacy Agreement. In light of this work, the issue of security will be re-examined at a later

date to see if L2TP over Frame Relay specific protection mechanisms are still required. Meanwhile, if stronger security mechanisms is required, the use of IP as an intermediate transport layer with IPsec [6] for security is RECOMMENDED.

9.0 Acknowledgments

Ken Pierce (3Com Corporation) and (Rick Dynarski 3Com Corporation) contributed to the editing of this document.

10.0 References

[1] Valencia et al., "Layer Two Tunneling Protocol 'L2TP'", RFC 2661, August 1999.

[2] Multiprotocol Encapsulation Implementation Agreement, FRF.3.1 , Frame Relay Forum Technical Committee, June 1995

[3] G. Zorn, D. Leifer, A. Rubens, J. Shriver. "RADIUS Attributes for Tunnel Protocol Support." Internet draft (work in progress).

[4] Frame Relay Fragmentation Implemenation Agreement, FRF.12, Frame Relay Forum Technical Committee, December 1997

[5] T. Bradley, C. Brown, A. Malis, "Multiprotocol Interconnect over Frame Relay", RFC 1490, July 1993

[6] B. Patel, B. Aboda. "Securing L2TP using IPSEC." Internet draft (work in progress).

11.0 Author's Addresses

Vipin Rawat
Cisco Systems, Inc.
170 West Tasman Drive
San Jose CA 95134-1706
vrawat@cisco.com

Rene Tio
Redback Networks, Inc.
1195 Borregas Avenue
Sunnyvale, CA 94089
tor@redback.com

Rohit Verma
Deloitte Consulting
180 N. Stetson Avenue
Chicago Illinois 60601
rverma@dc.com

Suhail Nanji
Redback Networks, Inc.
350 Holger Way
San Jose, CA 95134
suhail@redback.com

J. Senthilnathan
3Com Corporation
1800 West Central Road
Mount Prospect, IL 60056
janakiraman_senthilnathan@3com.com