

Network Working Group
Request for Comments: 2661
Category: Standards Track

W. Townsley
A. Valencia
cisco Systems
A. Rubens
Ascend Communications
G. Pall
G. Zorn
Microsoft Corporation
B. Palter
Redback Networks
August 1999

Layer Two Tunneling Protocol "L2TP"

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This document describes the Layer Two Tunneling Protocol (L2TP). STD 51, RFC 1661 specifies multi-protocol access via PPP [RFC1661]. L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications.

Table of Contents

1.0 Introduction.....	3
1.1 Specification of Requirements.....	4
1.2 Terminology.....	4
2.0 Topology.....	8
3.0 Protocol Overview.....	9
3.1 L2TP Header Format.....	9
3.2 Control Message Types.....	11
4.0 Control Message Attribute Value Pairs.....	12
4.1 AVP Format.....	13
4.2 Mandatory AVPs.....	14
4.3 Hiding of AVP Attribute Values.....	14

4.4 AVP Summary.....	17
4.4.1 AVPs Applicable To All Control Messages.....	17
4.4.2 Result and Error Codes.....	18
4.4.3 Control Connection Management AVPs.....	20
4.4.4 Call Management AVPs.....	27
4.4.5 Proxy LCP and Authentication AVPs.....	34
4.4.6 Call Status AVPs.....	39
5.0 Protocol Operation.....	41
5.1 Control Connection Establishment.....	41
5.1.1 Tunnel Authentication.....	42
5.2 Session Establishment.....	42
5.2.1 Incoming Call Establishment.....	42
5.2.2 Outgoing Call Establishment.....	43
5.3 Forwarding PPP Frames.....	43
5.4 Using Sequence Numbers on the Data Channel.....	44
5.5 Keepalive (Hello).....	44
5.6 Session Teardown.....	45
5.7 Control Connection Teardown.....	45
5.8 Reliable Delivery of Control Messages.....	46
6.0 Control Connection Protocol Specification.....	48
6.1 Start-Control-Connection-Request (SCCRQ).....	48
6.2 Start-Control-Connection-Reply (SCCRP).....	48
6.3 Start-Control-Connection-Connected (SCCCN).....	49
6.4 Stop-Control-Connection-Notification (StopCCN).....	49
6.5 Hello (HELLO).....	49
6.6 Incoming-Call-Request (ICRQ).....	50
6.7 Incoming-Call-Reply (ICRP).....	51
6.8 Incoming-Call-Connected (ICCN).....	51
6.9 Outgoing-Call-Request (OCRQ).....	52
6.10 Outgoing-Call-Reply (OCRP).....	53
6.11 Outgoing-Call-Connected (OCCN).....	53
6.12 Call-Disconnect-Notify (CDN).....	53
6.13 WAN-Error-Notify (WEN).....	54
6.14 Set-Link-Info (SLI).....	54
7.0 Control Connection State Machines.....	54
7.1 Control Connection Protocol Operation.....	55
7.2 Control Connection States.....	56
7.2.1 Control Connection Establishment.....	56
7.3 Timing considerations.....	58
7.4 Incoming calls.....	58
7.4.1 LAC Incoming Call States.....	60
7.4.2 LNS Incoming Call States.....	62
7.5 Outgoing calls.....	63
7.5.1 LAC Outgoing Call States.....	64
7.5.2 LNS Outgoing Call States.....	66
7.6 Tunnel Disconnection.....	67
8.0 L2TP Over Specific Media.....	67
8.1 L2TP over UDP/IP.....	68

8.2 IP.....	69
9.0 Security Considerations.....	69
9.1 Tunnel Endpoint Security.....	70
9.2 Packet Level Security.....	70
9.3 End to End Security.....	70
9.4 L2TP and IPsec.....	71
9.5 Proxy PPP Authentication.....	71
10.0 IANA Considerations.....	71
10.1 AVP Attributes.....	71
10.2 Message Type AVP Values.....	72
10.3 Result Code AVP Values.....	72
10.3.1 Result Code Field Values.....	72
10.3.2 Error Code Field Values.....	72
10.4 Framing Capabilities & Bearer Capabilities.....	72
10.5 Proxy Authen Type AVP Values.....	72
10.6 AVP Header Bits.....	73
11.0 References.....	73
12.0 Acknowledgments.....	74
13.0 Authors' Addresses.....	75
Appendix A: Control Channel Slow Start and Congestion Avoidance.....	76
Appendix B: Control Message Examples.....	77
Appendix C: Intellectual Property Notice.....	79
Full Copyright Statement.....	80

1.0 Introduction

PPP [RFC1661] defines an encapsulation mechanism for transporting multiprotocol packets across layer 2 (L2) point-to-point links. Typically, a user obtains a L2 connection to a Network Access Server (NAS) using one of a number of techniques (e.g., dialup POTS, ISDN, ADSL, etc.) and then runs PPP over that connection. In such a configuration, the L2 termination point and PPP session endpoint reside on the same physical device (i.e., the NAS).

L2TP extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. With L2TP, a user has an L2 connection to an access concentrator (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit.

One obvious benefit of such a separation is that instead of requiring the L2 connection terminate at the NAS (which may require a long-distance toll charge), the connection may terminate at a (local) circuit concentrator, which then extends the logical PPP session over

a shared infrastructure such as frame relay circuit or the Internet. From the user's perspective, there is no functional difference between having the L2 circuit terminate in a NAS directly or using L2TP.

L2TP may also solve the multilink hunt-group splitting problem. Multilink PPP [RFC1990] requires that all channels composing a multilink bundle be grouped at a single Network Access Server (NAS). Due to its ability to project a PPP session to a location other than the point at which it was physically received, L2TP can be used to make all channels terminate at a single NAS. This allows multilink operation even when the calls are spread across distinct physical NASs.

This document defines the necessary control protocol for on-demand creation of tunnels between two nodes and the accompanying encapsulation for multiplexing multiple, tunneled PPP sessions.

1.1 Specification of Requirements

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 [RFC2119].

1.2 Terminology

Analog Channel

A circuit-switched communication path which is intended to carry 3.1 kHz audio in each direction.

Attribute Value Pair (AVP)

The variable length concatenation of a unique Attribute (represented by an integer) and a Value containing the actual value identified by the attribute. Multiple AVPs make up Control Messages which are used in the establishment, maintenance, and teardown of tunnels.

Call

A connection (or attempted connection) between a Remote System and LAC. For example, a telephone call through the PSTN. A Call (Incoming or Outgoing) which is successfully established between a Remote System and LAC results in a corresponding L2TP Session within a previously established Tunnel between the LAC and LNS. (See also: Session, Incoming Call, Outgoing Call).

Called Number

An indication to the receiver of a call as to what telephone number the caller used to reach it.

Calling Number

An indication to the receiver of a call as to the telephone number of the caller.

CHAP

Challenge Handshake Authentication Protocol [RFC1994], a PPP cryptographic challenge/response authentication protocol in which the cleartext password is not passed over the line.

Control Connection

A control connection operates in-band over a tunnel to control the establishment, release, and maintenance of sessions and of the tunnel itself.

Control Messages

Control messages are exchanged between LAC and LNS pairs, operating in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.

Digital Channel

A circuit-switched communication path which is intended to carry digital information in each direction.

DSLAM

Digital Subscriber Line (DSL) Access Module. A network device used in the deployment of DSL service. This is typically a concentrator of individual DSL lines located in a central office (CO) or local exchange.

Incoming Call

A Call received at an LAC to be tunneled to an LNS (see Call, Outgoing Call).

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.