

PPP Working Group
Request for Comments: DRAFT
Category: Internet Draft
Title: [draft-ietf-l2tpext-adc-00.txt](#)
Date: October 1999

William Palter
RedBack Networks

L2TP Alternate Data Channel (``ADC'')

Status of this Memo

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

This document is an Internet-Draft. 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. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a ``working draft'' or ``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>.

To learn the current status of any Internet-Draft, please check the 1id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net, nic.nordu.net, ftp.nisc.sri.com, or munnari.oz.au.

Abstract

The Layer 2 Tunneling Protocol (``L2TP'') defines a mechanism for tunneling PPP sessions over arbitrary media. There exists a class of services for which different types of data packets should be segregated from each other, over the lower layer transport. This document describes the solution space addressed, its underlying motivations, and the protocol modifications required. This enhancement to the L2TP protocol is called L2TP Alternate Data Channel, or ``L2TPADC''.

1. 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. There are conditions where it may be desirable to send the data portion or some subset of

the data portion of an L2TP tunnel over a different media, or using different options of the lower layer medium than is used for the control portion of the tunnel.

2. Tunnel Establishment

2.1 Negotiation

L2TPADC is negotiated by an optional AVP ``L2TPADC'' which is placed in the SCCRQ/SCCRP tunnel establishment messages. The effect of this AVP on a given session will never occur until L2TP reaches a state where payload data may be forwarded for a session in the tunnel. Additionally, each side intending to use L2TPADC MUST NOT do so until it both sends and receives this AVP. Unless an L2TPADC AVP exists in both the SCCRQ and SCCRP packets, L2TP will operate in its regular mode

2.2 AVP Format

The AVP L2TPADC is encoded as Vendor ID 9, Attribute is the 16-bit quantity 2 (the ID 9 reflects Cisco Systems, the initial developer of this specification, and it SHOULD be changed to 0 and an official Attribute value chosen if this specification advances on a standards track). The Value is divided into two fields one indicating the channel type and usage of this alternate data channel and one for media specific information about the channel. This AVP itself is optional. The only type that is currently defined is the Degraded IPSEC Channel (see [section 2.3.1](#)).

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|0|0|0|0|      8 + data length      |          9          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|          2          |      Channel Type      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Media Specific Data .....
+---+---+---+---+---+---+---+---+---+---+---+---+

```

2.3 Channel Types

2.3.1 Degraded IPSEC Channel

The Degraded IPSEC Channel, Channel Type 0, is for use when the data flow on a tunnel may require strong security on some sessions (or packets within a session) and less secure security for other data packets and/or sessions. The control channel (which is also the primary data channel) should be setup with the highest level of security that is required. The media specific data should be set to a 16 bit value indicating another UDP port to which data packets can be sent that have less security associated with them. For example, a tunnel is created with IPSEC encryption on the control channel, and a

client establishes a PPP session over the tunnel in which ECP is also enabled and doing encryption. In this case the ECP PPP frames can be sent over the Degraded IPSEC Channel, and non ECP protected frames can be sent over the primary data channel. The policy for which packets can be sent over the degraded channel

is beyond the scope of this document. An implementation MUST send traffic over the strongest channel, unless it has specific policies permitting it to send a packet over the degraded channel.

2.4 Data Packet Flow

When data packets for a single session are sent over more than one, data channel the sequence number space is shared among both flows, L2TP SHOULD process all packets for a tunnel without regard for which channel the packet is received upon.

2.5 Control Packet Flow

Control packets MUST be sent over the primary channel. If a control packet is received on the alternate channel, it MUST be discarded.

3. Security Considerations

Security can be compromised by using this option. It is assumed that implementation policies with regard to determining which packets can go over a degraded channel will be sufficient to protect security. In addition since the security policies may not be symmetrical, an implementation should have the ability to be configured not to allow this option to be used.

4. Acknowledgments

Thanks to Andrew J. Valencia, W. Mark Townsley, and Robert Adams of Cisco Systems for help in creating, and reviewing this draft.

5. Contacts

William Palter
RedBack Networks
1389 Moffett Park Drive
Sunnyvale, CA 94089
palter.ietf@zev.net

6. References

- [1] A. Valencia, ``Layer 2 Tunnel Protocol (L2TP)'', Internet Draft, October 1997

INTERNET DRAFT

October 1999

Palter

expires March 2000

[Page 4]