Network Working Group
INTERNET DRAFT

Nishit Vasavada
Amber Networks, Inc.

July 2001

Encapsulation Services Protocol Service Type for L2TP
<draft-vasavada-l2tpext-es-svctype-00.txt>

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of 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.

2. Abstract

The Layer Two Tunneling Protocol (L2TP) [RFC2661] provides a standard method for tunneling PPP [RFC1661] packets. In accordance with the L2TP Service Type specification [L2TPST], this document provides a solution for transporting Encapsulation Services Protocol (ESP) [ESP] over L2TP. It uses [L2TPDS] for providing DS support to the L2TP control and ESP packets.

3. 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 RFC 2119 [RFC2119].

4. Introduction

The Layer Two Tunneling Protocol (L2TP) [RFC2661] provides a standard

method for tunneling PPP [RFC1661] packets. The L2TP Service Type [L2TPST] allows layer 1 and layer 2 traffic to be tunneled through an L2TP tunnel.

This document presents a solution to carry the ESP traffic over the IP network through the features offered by L2TP and the Service Type attribute.

It talks about the use of [RFC2661] and [L2TPST] for setting up an L2TP tunnel and session containing ESP traffic, and use of [L2TPDS] for signaling DS values for the L2TP control and payload traffic. It also introduces a new AVP - End-Identifier - to convey the end identifiers to the peer.

5. ESP Service Type

An ESP Service Type value of [TBD] MUST be used. The encoding of the Service Type AVP remains as specified in [L2TPST].

6. Tunnel Establishment

The basic tunnel establishment procedures defined in [RFC2661] and [L2TPST] are followed. Following are additional requirements:

6.1. Service Capabilities

For supporting ESP in a tunnel, the ESP Service Type value [TBD] MUST be included in the Service Capabilities List AVP.

[L2TPST] allows multiple services to be carried in different sessions inside a single L2TP tunnel. However, ESP requires that if a tunnel were to carry ESP traffic, all sessions within the tunnel be carrying ESP sessions. To accommodate this requirement, if ESP is present in the Service Capabilities AVP, the sender MUST NOT put any other service type in the Service Capabilities AVP. If a service other than ESP is also present in the Service Capabilities AVP carrying ESP service type, and if the receiving L2TP peer supports ESP, it MUST tear down the tunnel.

Since ESP is the exclusive service on ESP such a tunnel (i.e., PPP is not supported on this tunnel), the M-bit of Service Capabilities AVP MUST be set.

6.2 Control Connection DS (CCDS) AVP

If a DS value is made available to L2TP for the tunnel, L2TP MUST use this AVP.

7. Session Establishment

The basic call establishment procedures defined in [RFC2661] and [L2TPST] remain unchanged.

7.1. Service Type AVP

The ESP Service Type value [TBD] MUST be used in the Service Type AVP of an ICRQ or OCRQ of each session within the tunnel.

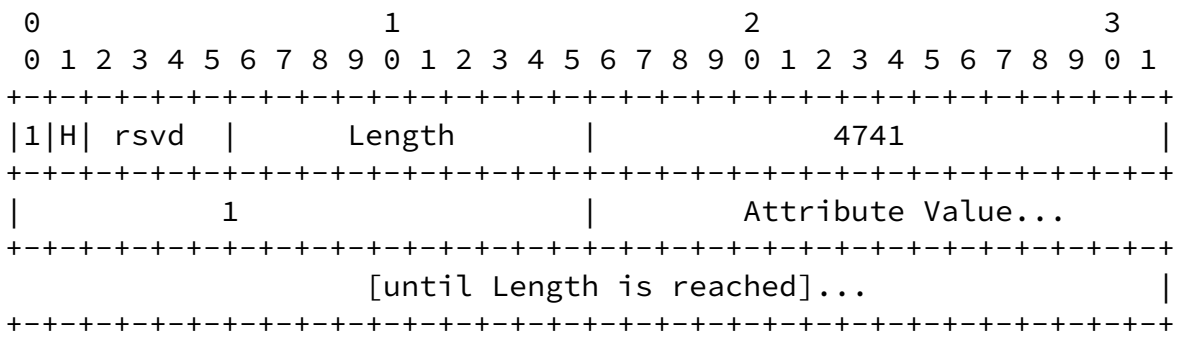
7.2. Session DS (SDS) AVP

If a DS value is made available to L2TP for the tunnel, L2TP MUST use this AVP and use the same value as that for the CCDS AVP while setting up the tunnel.

7.3. End-Identifier AVP (ICRQ, OCRQ)

ES needs to convey the end-identifiers on both sides to the remote side while setting up a session. We introduce a new AVP - End-Identifier AVP - for this purpose.

The End-Identifier AVP is encoded as follows:



Vendor ID = 4741 for Amber Networks
Attribute = 1

The attribute value contains interface and other optional information depending on the access link type that ESP is encapsulating. For

example, if the ESP is carrying FR payload, the additional information would DLCI numbers on both ends. No additional information is present for TDM circuits.

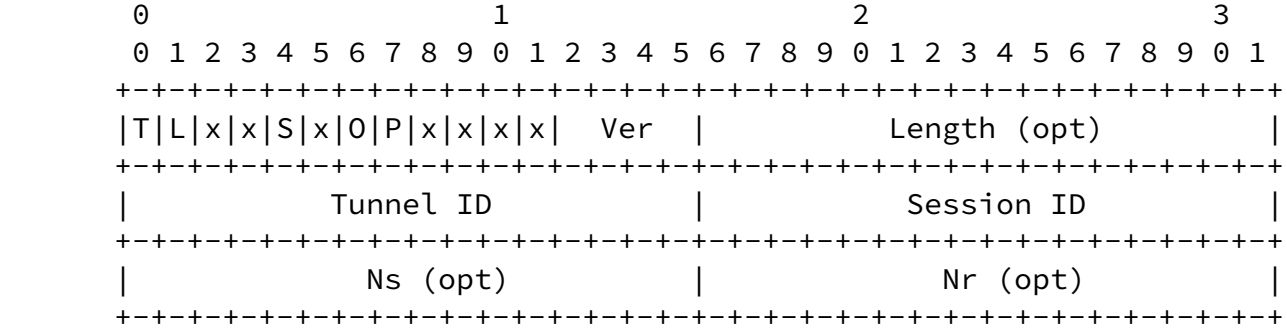
The attribute value may be a simple ASCII string. For example, a source interface serial 1/1 and DLCI 100, and a destination interface serial 1/1 with DLCI 200 could be represented as "serial 1/1 DLCI 100, serial 1/1 DLCI 200". The format of the information contained in this AVP should be agreed on by the administrators at the two L2TP peers.

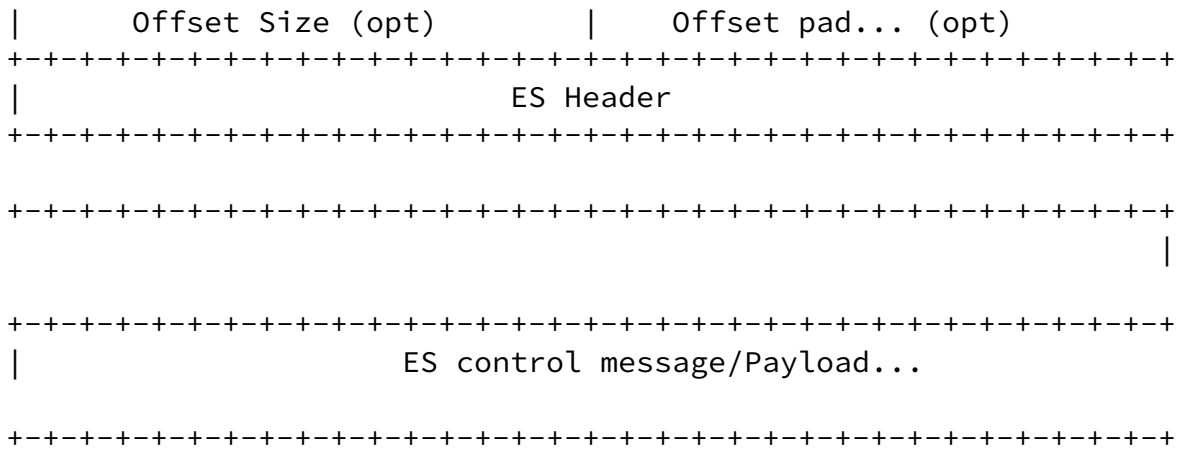
When employing the End-Identifier AVP for this purpose, the AVP is mandatory (the M-bit MUST be set to 1). The AVP MAY be hidden (the H-bit set to 0 or 1).

7.2. ESP Payload Message Format

The L2TP payload header format defined in [RFC2661] remains unchanged while carrying data for an ESP session. Entire ESP PDU will be carried.

The encapsulated ESP PDU looks like this:





As is true for the PPP traffic carried by L2TP, the frame size should consider the MTU and the additional headers to avoid IP fragmentation.

8. Effects on Standard AVPs

If ESP PDUs are being tunneled in accordance with this document, the following Call Management AVPs MAY be ignored:

- Bearer Type
- Framing Type
- Called Number
- Calling Number
- Sub-Address
- Initial Received LCP CONFREQ
- Last Sent LCP CONFREQ
- Last Received LCP CONFREQ
- Proxy Authen Type
- Proxy Authen Name
- Proxy Authen Challenge
- Proxy Authen ID
- Proxy Authen Response
- ACCM

9. Security Considerations

All the underlying L2TP Security considerations remain, though no 'new' ones are introduced?

10. IANA Considerations

Need to obtain a value for ES Service Type from IANA.

11. Acknowledgments

Many thanks to Harisankar Mallath for helping in reviewing this draft.

12. References

[RFC2661] Townsley, et. al., "Layer Two Tunneling Protocol L2TP", RFC 2661, February 1999.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[L2TPST] McPherson D., Nanji S., "L2TP Service Type", Work in Progress, April 2001.

[ESP] Vasavada, N., "ESP: Encapsulation Services Protocol", Work in Progress, July 2001.

[L2TPDS] Calhoun, P., et. al., "L2TP Differentiated Services Extension", Work in Progress, March 2001.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

14. Author's Address

Nishit Vasavada
Amber Networks, Inc.
48664 Milmont Drive
Fremont, CA 94538
Phone: +1 510.687.5200
Email: nishit@ambernetworks.com