Network Working Group
INTERNET DRAFT
Category: Standards Track
Title: draft-ietf-l2tpext-eth-00.txt
Date: November 2000

Suhail Nanji
Redback Networks, Inc.

Ethernet Service Type for Layer Two Tunneling Protocol
<draft-ietf-l2tpext-eth-00.txt>

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

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html.

The distribution of this memo is unlimited. It is filed as <draft-ietf-l2tpext-eth-00.txt>, and expires May, 2001. Please send comments to the authors.

Abstract

The Layer Two Tunneling Protocol (L2TP) [RFC2661] provides a standard method for tunneling PPP [RFC1661] packets. In accordance with the Layer Two Tunneling Protocol (L2TP) Service Type draft [L2TP_svctype], this document describes the details for transporting Ethernet frames over a session in an L2TP tunnel. That is, the details of an Ethernet service type for L2TP sessions.

1. Introduction

With L2TP it is possible to divorce the location of the initial dial-up server from the location at which the dial-up protocol connection is terminated and access to the network provided. However, this is only possible if PPP is used to access the network. The L2TP Service Type draft describes how other payload types may be tunneled on a session by session basis over L2TP. This document describes how Ethernet frames may be tunneled over an L2TP session as a new service type as described by the L2TP Service Type draft.

It is possible to use PPP Bridging Control Protocol (BCP) as specified in [RFC2878] to transport the Ethernet frame over L2TP without employing a new service type. However, using BCP might not be feasible since the Ethernet client may not support BCP. Furthermore, the service type approach has less protocol overhead than using BCP.

2. Conventions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

Ethernet in this document refers to both DIX Ethernet and IEEE 802.3. It is assumed the receipient of an Ethernet frame has the capabilities to distinguish between the two different Ethernet encapsulations. Both Ethernet types MAY be used on the same L2TP session.

3. Ethernet Service Type

A Ethernet srvice type value of 3 MUST be used for the L2TP Service Type draft to identify an Ethernet payload.

4. Tunnel Establishment

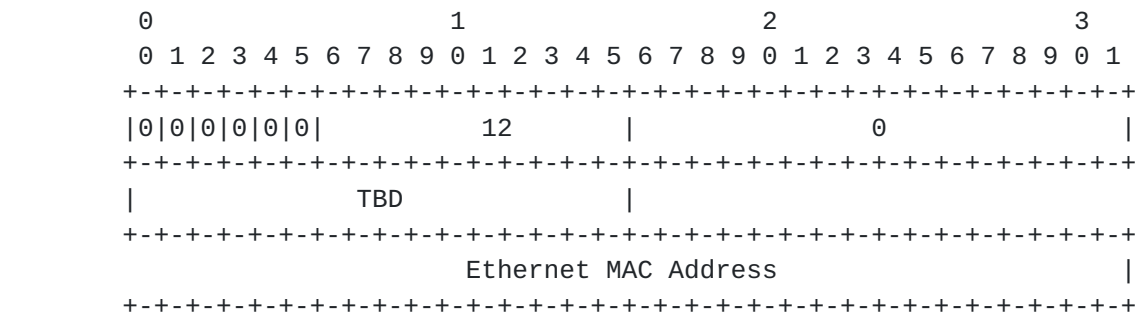
The basic tunnel establishment procedures defined in [RFC2661] and [L2TP_svctype] draft are unchanged. The Ethernet service type value MUST be included in the Service Capabilities List AVP.

5. Session Establishment

The basic call establishment procedures defined in [RFC2661] and [L2TP_svctype] are unchanged. Currently, Ethernet framing is only supported for incoming call requests (ICRQ). The Ethernet service type value MUST be used in the Service Type AVP of an ICRQ. The Ethernet service type value MUST NOT be used in the Service Type AVP of an OCRQ. Also, a new AVP MUST be included in the ICRQ which contains an Ethernet MAC address from the LAC.

5.1 Ethernet MAC Address AVP

Ethernet MAC Address

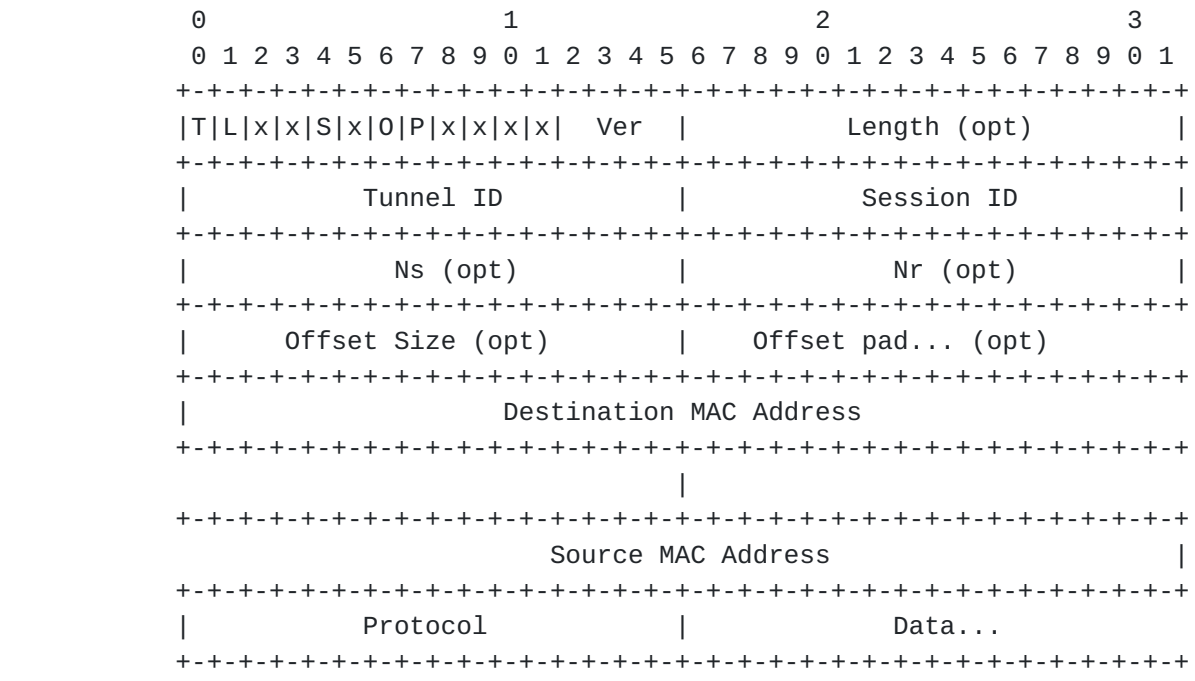


The Ethernet MAC Address AVP contains an Ethernet MAC address from the LAC in canonical form as specified in [RFC2469]. This value MUST be used as the source address for Ethernet frames sent to tunneled end stations from the LNS. The vendor code is 0 and the Attribute value is TBD. This AVP MUST NOT have the manditory bit set. The Value is a 48-bit Ethernet MAC address.

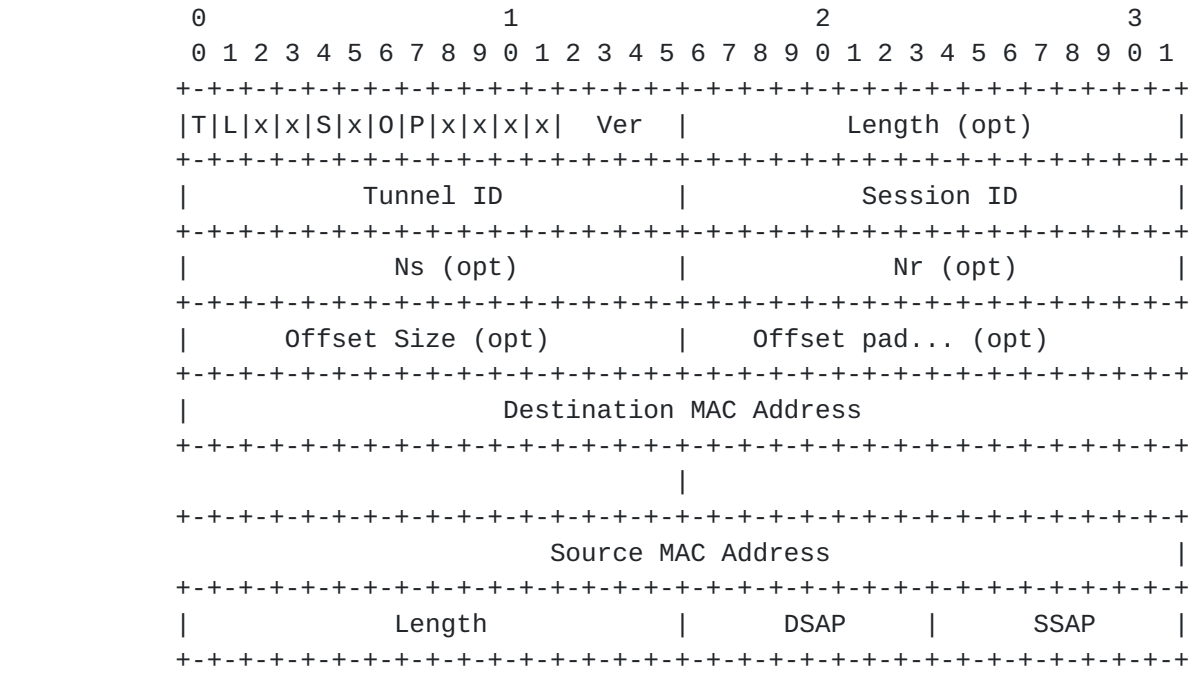
6. Ethernet Payload Message Format

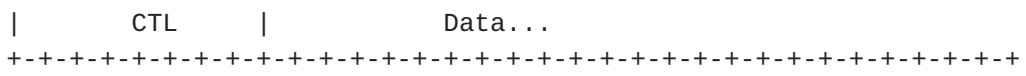
The L2TP payload header will be unchanged and as described in [RFC2661]. However, instead of carrying a PPP packet, the payload will carry an Ethernet frame starting from the MAC addresses, which MUST be in canonical form as specified in [RFC2469]. In both types of Ethernet frames, the CRC is preserved end-to-end.

DIX Ethernet



IEEE 802.3





7. Effects on Standard AVPs

If Ethernet frames are being tunneled in accordance with this document, then the following Call Management AVPs MAY be ignored:

- Bearer Type
- Framing Type
- Called Number
- Calling Number
- 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

8. Authentication Considerations

All issues dealing with authenticating the incoming Ethernet client are beyond the scope of this document.

9. Security Considerations

All security considerations with tunneling Ethernet frames over L2TP are beyond the scope of this document.

10. Acknowledgments

Thanks to Bill Palter, Danny McPherson, Mark Townsley and Wei Luo for their help in reviewing this draft. Copious amounts of text were stolen from [RFC2661].

11. 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.

[RFC2119] Bradner S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[L2TP_svctype] McPherson D., Nanji S., "L2TP Service Type", August 2000.

[RFC2469] T. Narten, C. Burton, "A Caution On The Canonical Ordering Of Link-Layer Addresses", RFC 2469, December 1998.

[RFC2878] M. Higashiyama, F. Baker, "PPP Bridging Control Protocol (BCP)", RFC 2878, July 2000.

Authors' Addresses:

Suhail Nanji <suhail@redback.com>
Redback Networks, Inc.
350 Holger Way
San Jose, CA 95134-1362
United States of America