Network Working Group
Request for Comments: 3437
Category: Standards Track

W. Palter
zev.net
W. Townsley
Cisco Systems

December 2002

Layer-Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation

Status of this Memo

Copyright Notice

Abstract

This document defines extensions to the Layer Two Tunneling Protocol (L2TP) for enhanced support of link-specific Point to Point Protocol (PPP) options. PPP endpoints typically have direct access to the common physical media connecting them and thus have detailed knowledge about the media that is in use. When the L2TP is used, the two PPP peers are no longer directly connected over the same physical media. Instead, L2TP inserts a virtual connection over some or all of the PPP connection by tunneling PPP frames over a packet switched network such as IP. Under some conditions, an L2TP endpoint may need to negotiate PPP Link Control Protocol (LCP) options at a location which may not have access to all of the media information necessary for proper participation in the LCP negotiation. This document provides a mechanism for communicating desired LCP options between L2TP endpoints in advance of PPP LCP negotiation at the far end of an L2TP tunnel, as well as a mechanism for communicating the negotiated LCP options back to where the native PPP link resides.

Table of Contents

1. Introduction..... 2
1.1 Specification of Requirements..... 3
2. LCP Options From LAC to LNS..... 3
2.1 LCP Want Options (iccn, occn)..... 4
2.2 LCP Allow Options (iccn, occn)..... 6
2.3 LCP Options From LNS to LAC..... 7
3. Security Considerations..... 8
4. IANA Considerations..... 8
5. Normative References..... 8
6. Author's Addresses..... 9
7. Full Copyright Statement..... 10

1. Introduction

L2TP [RFC2661] provides a very limited amount of guidance to the LNS as to what type of interface a tunneled PPP session arrived on at an LAC. Such information is limited to whether the interface was "synchronous" or "asynchronous", "digital" or "analog." These indications provide some guidance when negotiating PPP LCP at the LNS, but they are not as robust as they could be.

This document defines a more robust way to inform the LAC of LCP negotiated options, and provides guidance to the LNS on the limits and values that the LAC requires during LCP negotiation. Deep knowledge of PPP [RFC1661] and L2TP [RFC2661] are expected for the remainder of this document.

L2TP Proxy LCP allows options to be negotiated where the native PPP link resides, thus circumventing issues with ACCM, Alternate FCS, and other LCP Options that the LNS would not necessarily know how to properly negotiate without access to the physical media for the native PPP connection, interface type, or configuration. However, use of Proxy LCP introduces other problems as well as there are options within LCP PPP negotiation which should be set or adjusted by the LNS, such as the PPP Authentication Type and MRU. Finally, the PPP Client may reinitiate LCP negotiation at any time, and unless the LAC is sniffing every PPP data packet it forwards, it would not be aware that this is even occurring.

LCP options may be classified into roughly three different categories with respect to their affect on L2TP; (1) options which affect framing in a way that the LAC may need to know about or handle specifically (e.g., ALT-FCS, ACCM, MRU), (2) options that are mostly transparent to the LAC (e.g., AUTH-TYPE), and (3) options that the

LAC may wish to influence because they are dependent on the media type (ACFC, PFC). We are most concerned with options that fall into category (1) and (3).

This document defines new AVPs to allow the LAC and the LNS to communicate complete LCP information in order to react accordingly. LCP option information is structured in the same way as the Proxy LCP AVPs are in [RFC2661]. This essentially involves encapsulation of a PPP LCP Configure-Request or Configure-Ack packet within an L2TP AVP.

1.1 Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

2. LCP Options From LAC to LNS

The LAC may utilize the following AVPs within an ICCN or OCCN message in order to influence the LNS to negotiate LCP in a specific manner. If these AVPs are supported by the LNS, they should override any suggestions for LCP options implied by the Bearer Type or Framing Type AVPs.

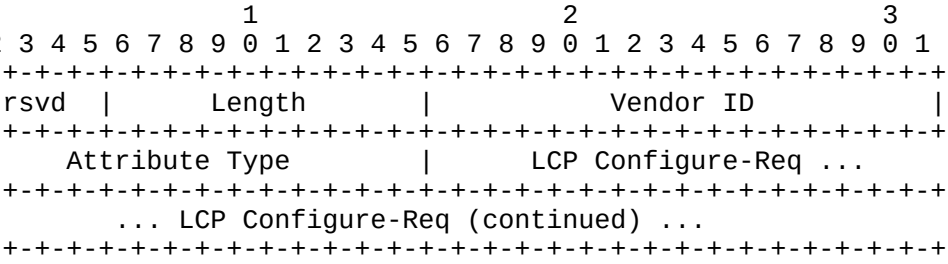
These AVPs may coexist with the Proxy LCP and Proxy Authentication AVPs (Proxy AVPs) defined in the base L2TP specification. If Proxy AVPs are received, the LNS may choose to accept these parameters, or renegotiate LCP with the options suggested by the AVPs defined in this document. If the LAC wishes to force negotiation of LCP by the LNS, it should simply omit all Proxy AVPs during call initialization.

By default, the AVPs defined in this document are not mandatory (M-bit is set to zero). However, if an implementation needs to strongly enforce adherence to the options defined within the AVPs, it MAY set the M-bit to 1, thus forcing the peer to discontinue the session if it does not support this AVP. This is NOT recommended unless it is known that the result of operating without these extensions is completely unacceptable.

If the AVPs in sections 2.1 and 2.2 are sent to the LNS, the LAC MUST be prepared to accept the AVPs as defined in section 2.3.

2.1 LCP Want Options (iccn, occn)

The LCP Allow Options AVP, Attribute Type 49, contains a list of options that the LAC wants to be negotiated by the LNS.



The Vendor ID is the IETF Vendor ID of 0.

This AVP MAY be hidden (the H bit MAY be 0 or 1).

The M bit for this AVP may be set to 0 or 1. If the sender of this AVP does not wish to establish a connection to a peer which does not understand this L2TP extension, it SHOULD set the M bit to 1, otherwise it MUST be set to 0.

The Length (before hiding) of this AVP is 6 plus the length of the LCP Configure Request.

The AVP SHOULD be present in the following messages: ICCN, OCCN

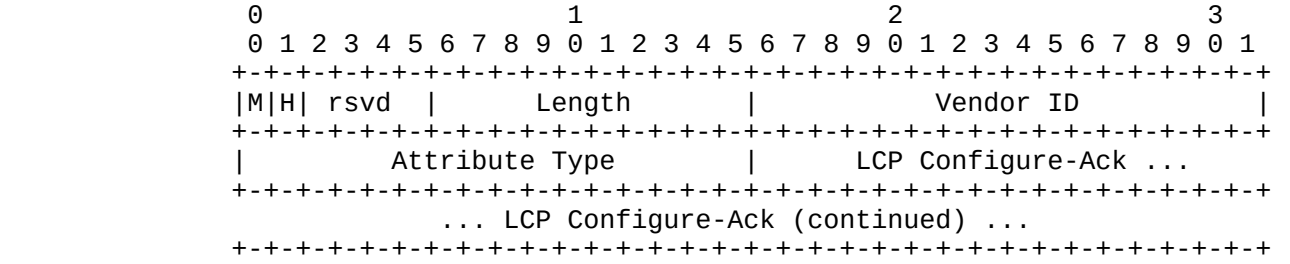
The LCP Configure-Req Value for this AVP is identical to the information field of a PPP LCP Configure-Req Packet (much like a Proxy LCP AVP in [RFC2661]). It is sent from the LAC to the LNS, and is intended to guide PPP LCP negotiations at an LNS. In some cases, each individual PPP LCP option carried in this AVP maps to a desired value (e.g., MRU) and in some cases it maps to a specific option that is desired to be enabled (e.g., ACFC). The LNS should use these suggestions when building its initial Configure-Request.

The following chart defines some of the more common LCP options that may be included in this AVP with guidance on how to handle them at the LAC and LNS. This table is provided for some of the more common or problematic LCP options. It is not intended to be an exhaustive representation of all LCP options available.

LCP Want Option	LAC Action	LNS Action
MRU	LAC provides a	LNS SHOULD begin LCP negotiation maximum value with this value. However, it MAY reduce MRU if necessary.
ACCM	LAC Provides a mask	LNS SHOULD begin LCP negotiation with this value. LNS may add bit(s) while negotiating.
PFC	LAC provides PFC on the link type the link type (e.g. AHDLC)	LNS SHOULD begin LCP negotiation if it is desired with this value.
ACFC	LAC provides ACCOMP if it is desired on the link type (e.g. AHDLC)	LNS SHOULD begin LCP negotiation with this value.
FCS-ALT	LAC indicates required values for the link type	LNS SHOULD begin negotiation with this value. Note that this value is of no consequence to the LNS as FCS is stripped at the LAC, however some PPP media types require this option.

2.2 LCP Allow Options (iccn, occn)

The LCP Allow Options AVP, Attribute Type 50 contains a list of options that the LAC will allow to be negotiated by the LNS.



The Vendor ID is the IETF Vendor ID of 0.

This AVP MAY be hidden (the H bit MAY be 0 or 1).

The M bit for this AVP may be set to 0 or 1. If the sender of this AVP does not wish to establish a connection to a peer which does not understand this L2TP extension, it SHOULD set the M bit to 1, otherwise it MUST be set to 0.

The Length (before hiding) of this AVP is 6 plus the length of the LCP Configure Request.

The AVP MAY be present in the following messages: ICCN, OCCN

The LCP Configure-Ack Value for this AVP is identical to the information field of a PPP LCP Configure-Req Packet (much like a Proxy LCP AVP in [RFC2661]). It is sent from the LAC to the LNS, and is intended to guide PPP LCP negotiations at an LNS. In some cases, each individual PPP LCP option carried in this AVP maps to a maximum value (e.g., MRU), while in others it maps to an option that is permitted by the LAC (e.g., ACFC). If the option is not included here, it can be assumed by the LNS that the LAC does not understand how to perform that particular option at the link layer (and would thus Configure-Reject that option). Information in this AVP should be utilized when building PPP Configure-Ack, Configure-Reject and Configure-Nak messages.

The following chart defines some of the more common LCP options that may be included in this AVP with guidance on how to handle them at the LAC and LNS. This table is provided for illustration purposes for some of the more common or problematic LCP options. It is not intended to be an exhaustive representation of all LCP options available.

LCP Allow Option	LAC Action	LNS Action
MRU	LAC provides a maximum value	LNS may accept reduction MRU as requested.
ACCM	LAC Provides a mask	LNS may accept bit(s) defined here. Note that if ACCM is missing it is assumed that it is not applicable to the link type.
PFC	LAC provides PFC if it is allowed on the link type (e.g. AHDLC)	LNS may accept PFC.
ACFC	LAC provides ACFC if it is allowed on the link type (e.g. AHDLC)	LNS may accept ACFC.
FCS-ALT	LAC indicates valid values for the link type	Negotiation this option is of no consequence to the LNS as the FCS is stripped at the LAC. However, the LNS SHOULD only accept FCS-ALT types listed here (more than one value may be present).

2.3 LCP Options From LNS to LAC

In order to communicate negotiated LCP parameters from the LNS to the LAC, the format of two existing messages in [RFC2661] are used. These are:

Last Sent LCP Confreq (IETF L2TP Attribute 27)
Last Received LCP Confreq (IETF L2TP Attribute 28)

These AVPs are sent from the LAC to the LNS to support Proxy LCP negotiation. In order to report negotiated LCP parameters from the LNS to the LAC, two messages of precisely the same format are defined:

LNS Last Sent LCP Confreq (IETF L2TP Attribute 51)
LNS Last Received LCP Confreq (IETF L2TP Attribute 52)

When LCP negotiation is completed by the LNS, a Set-Link-Info control message MUST be sent with these AVPs contained within. These AVPs MUST contain the last sent and last received (with respect to the LNS) LCP packets.

Rather than simply using the old Attribute values in the SLI Message, new AVP Attribute types are defined for these messages due to the fact that some existing L2TP implementations might check for what could seem like misplacement of known AVP types and generate a false error condition.

3. Security Considerations

There are no known additional significant threats incurred by the mechanisms described in this document.

This document defines additional L2TP AVPs that identify link characteristics and interface information of a tunneled PPP link. If these values were snooped, a rogue individual may have access to more information about a given network or topology. Given that these same values may be negotiated over the tunneled link in PPP LCP packets anyway, this is no more information than is potentially transmitted today, it is just in a different form.

4. IANA Considerations

This document requires four new L2TP "AVP Attribute" numbers to be assigned by IANA.

49, Section 2.1, LCP Want Options
50, Section 2.2, LCP Allow Options
51, Section 2.3, LNS Last Sent LCP Confreq
52, Section 2.3, LNS Last Received LCP Confreq

5. Normative References

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

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

[RFC 2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer Two Tunneling Layer Two Tunneling Protocol (L2TP)", RFC 2661, August 1999.

6. Author's Addresses

W. Mark Townsley
Cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709

EMail: mark@townsley.net

Bill Palter
EMail: palter.ietf@zev.net

7. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.