L2TPEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 11, 2009

C. Pignataro, Ed.
Cisco Systems, Inc.

July 10, 2008

PPP Tunneling Using Layer Two Tunneling Protocol Version 3 (L2TPv3) draft-ietf-l2tpext-l2tp-ppp-08

Status of this Memo

Abstract

This document describes the use of "version 3" of Layer Two Tunneling Protocol (L2TPv3) to tunnel Point-to-Point Protocol (PPP) packets. This document defines the control protocol and encapsulation specifics for tunneling PPP over L2TPv3, and is a companion document to the L2TPv3 base specification.

Table of Contents

1. Introduction 4
1.1. Terminology 4
1.2. Requirements Language 6
1.3. Contributing Authors 6

2. Topology 6

3. Control Channel Specifics for PPP 7
3.1. Control Connection Establishment 7
3.2. Session Establishment 7
3.3. Session Maintenance 8

4. Data Channel Specifics for PPP 9
4.1. L2-Specific Sublayer 10
4.2. Offset Padding 10
4.3. Forwarding PPP Frames 11

5. AVP Description 12
5.1. PPP-Specific AVPs 12
5.1.1. Control Connection Management AVPs 13
5.1.1.1. Framing Capabilities (SCCRP, SCCRQ) 13
5.1.1.2. Bearer Capabilities (SCCRP, SCCRQ) 13
5.1.1.3. Offset Capability (SCCRP, SCCRQ) 14
5.1.2. Session Management AVPs 15
5.1.2.1. Bearer Type (ICRQ, OCRQ) 15
5.1.2.2. Framing Type (ICCN, OCCN, OCRQ) 16
5.1.2.3. Called Number (ICRQ, OCRQ) 16
5.1.2.4. Calling Number (ICRQ) 17
5.1.2.5. Called Sub-Address (ICRQ, OCRQ) 18
5.1.2.6. Calling Sub-Address (ICRQ) 18
5.1.2.7. Q.931 Cause Code (CDN) 19
5.1.2.8. Private Group ID (ICCN) 19
5.1.2.9. Offset Size (ICRQ, ICRP, ORCQ, OCRP) 20
5.1.2.10. Tx Minimum Speed (OCRQ) 21
5.1.2.11. Tx Maximum Speed (OCRQ) 22
5.1.2.12. Rx Minimum Speed (OCRQ) 23
5.1.2.13. Rx Maximum Speed (OCRQ) 23
5.1.3. Proxy LCP and Authentication AVPs 24
5.1.3.1. Initial Received LCP CONFREQ (ICCN) 24
5.1.3.2. Last Sent LCP CONFREQ (ICCN) 25
5.1.3.3. Last Received LCP CONFREQ (ICCN) 25
5.1.3.4. Proxy Authen Type (ICCN) 26
5.1.3.5. Proxy Authen Name (ICCN) 27
5.1.3.6. Proxy Authen Challenge (ICCN) 27
5.1.3.7. Proxy Authen ID (ICCN) 28
5.1.3.8. Proxy Authen Response (ICCN) 28

5.1.4. Session Status AVPs 29
5.1.4.1. PPP Circuit Errors (WEN) 29
5.1.4.2. ACCM (SLI) 30
5.2. Service Type Independent AVPs 30
5.2.1. Session Management AVPs 31
5.2.1.1. Data Sequencing (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN) 31
5.2.1.2. Circuit Status (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN, SLI) 31
5.2.1.3. Tx Connect Speed (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN) 32
5.2.1.4. Rx Connect Speed (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN) 32

6. Data Channel Sequencing 33
6.1. Sequence Numbers 33
6.2. Data Channel Sequencing over Specific Media 34

7. Acknowledgements 35

8. IANA Considerations 35
8.1. AVP Attributes 36
8.2. Pseudowire Type 36
8.3. Result Code AVP Values 37
8.4. Bearer Capabilities and Bearer Type 37
8.5. Framing Capabilities and Framing Type 37
8.6. Proxy Authen Type AVP Values 37

9. Security Considerations 37
9.1. Proxy PPP Authentication 38

10. References 38
10.1. Normative References 38
10.2. Informative References 39

Appendix A. Revision History 40

Author's Address 43
Intellectual Property and Copyright Statements 44

1. Introduction

The Point-to-Point Protocol (PPP) [RFC1661] is a data link layer protocol that provides a standard method for carrying multiprotocol packets across point-to-point links. It is the most commonly used protocol to provide remote access over various access media such as dial-up POTS, ISDN, ADSL, ATM SVC (Switched Virtual Circuit) or PVC (Permanent Virtual Circuit) based access [RFC3301], etc.

Typically, a user obtains a Layer 2 (L2) connection to a Network Access Server (NAS) using one of a number of access techniques (e.g., dial-up POTS, ISDN, ADSL, ATM access, 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).

Tunneling protocols, such as the Layer Two Tunneling Protocol - Version 3 (L2TPv3) defined in [RFC3931], provide a dynamic mechanism for extending PPP by allowing the L2 and PPP endpoints to reside on different devices that are interconnected by a packet switched network (PSN), for example over IP. This separation allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit.

L2TPv3 can also be used as the control protocol and for data encapsulation in the creation of Pseudowires (PWs) to transport PPP frames over an IP or other packet-based network. A PPP Pseudowire (PPPPW) emulates a single PPP link between exactly two endpoints.

This document defines the specific mechanisms for the tunneling of PPP using L2TPv3.

This is a companion document to be read in conjunction with [RFC3931]. A large part of this document is derived from [RFC2661], which describes the L2TP protocol signaling as well as the encapsulation method to tunnel PPP sessions. This document is a result of the rewriting of [RFC2661] to separate the base L2TP protocol from the PPP tunneling details.

1.1. Terminology

This document uses terminology defined in Section 1.3 of [RFC3931]. Additional terminology is defined here.

Called Number

The telephone number dialed by a caller to reach the receiver of the call.

Calling Number

The telephone number of the caller.

CHAP

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

DSLAM

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

ISDN

Integrated Services Digital Network.

Network Access Server (NAS)

A device providing local network access to users across a remote access network, such as the PSTN.

Packet Switched Network (PSN)

A network that uses packet switching technology for data delivery. For L2TPv3, this layer is principally IP. Other examples include MPLS, Frame Relay, and ATM. See also [RFC3985].

POTS

Plain Old Telephone Service.

Pseudowire (PW)

An emulated circuit as it traverses a PSN. See also [RFC3985]. There is one Pseudowire per L2TP Session.

PPPPW

PPP Pseudowire.

1.2. Requirements Language

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].

1.3. Contributing Authors

This document is a result of the combined effort of several individuals. The following are the authors that contributed to this document:

Ignacio Goyret
Jed Lau
Gurdeep Singh Pall
Bill Palter
Allan Rubens
W. Mark Townsley
Andrew J. Valencia
Madhvi Verma
Glen Zorn
Carlos Pignataro

2. Topology

PPP tunneling can be deployed in all of the different tunneling models specified in Section 2 of [RFC3931]. Traditionally, it is most commonly deployed for access applications in the LAC-LNS reference model. The LAC physically terminates the L2 connection and tunnels the PPP packets across a packet-based network (i.e., IP network) to the LNS. The LNS then terminates the logical PPP connection. The L2 service extends between Remote System and LNS, and the emulated service extends between LAC and LNS (see Section 2 of [RFC3931]). The session establishment can be driven by the LAC (an incoming call) or the LNS (an outgoing call).

In the LNS-LNS reference model, both the emulated service and L2 service extend between the two LNS devices. A software package on a host which runs L2TP natively and acts as an LNS is often referred to as a "LAC Client" [RFC2661].

More recently, in the symmetric LAC-LAC reference model, the emulated service extends between LACs while the L2 service extends between remote systems. In the most basic form, the LAC acts as a cross-connect between a PPP interface to a remote system and an L2TP session, and forwards PPP traffic from the remote system to the peer LAC using L2TP and vice versa. This model typically involves

symmetric establishment: Either side of the connection may initiate a session at any time, or simultaneously (utilizing the tie breaking mechanism defined in Section 5.4.4. of [RFC3931]).

3. Control Channel Specifics for PPP

The following sections highlight Control Connection and Session management details in the context of PPP over L2TPv3. This includes AVPs that need special attention for PPP over L2TPv3 or that differ from [RFC2661].

3.1. Control Connection Establishment

In order to tunnel PPP over L2TPv3, an L2TPv3 Control Connection MUST first be established as described in Section 3.3 of [RFC3931].

The L2TPv3 SCCRQ Control Message and corresponding SCCRP Control Message MUST include the "PPP Pseudowire Type" of 0x0007 (See Section 8.2), in the Pseudowire Capabilities List AVP, Attribute Type 62, as defined in Section 5.4.3 of [RFC3931]. This identifies the Control Connection as being able to establish PPP L2TPv3 sessions.

During Control Connection Establishment, LCCEs are identified either by the Host Name AVP, Attribute Type 7, the Router ID AVP, Attribute Type 60, or a combination of the two. See Section 3.3 of [RFC3931] that describes the LCCE identity.

The Assigned Control Connection ID defined in Section 5.4.3 of [RFC3931], Attribute Type 61, is the L2TPv3 analogous to the Assigned Tunnel ID in L2TPv2. The Control Connection Tie Breaker AVP defined in Section 5.4.3 of [RFC3931], Attribute Type 5, is used to choose a single Control Connection when two LCCEs request a Control Connection simultaneously.

3.2. Session Establishment

The following signaling elements are needed for session establishment:

The Pseudowire Type AVP defined in Section 5.4.4 of [RFC3931], Attribute Type 68, MUST be present in the ICRQ and OCRQ messages and MUST include the PPP PW Type of 0x0007.

The Remote End ID AVP, Attribute Type 66, binds the L2TP session to a given PPP circuit, and MUST be present in ICRQ messages in the LAC-LAC cross-connect application (see Section 2(b) of [RFC3931]). In this case, an implementation MUST support a Remote End ID of an

unstructured four-octet value that is known to both LCCEs (either by manual configuration of some other means outside of the scope of this document).

The Circuit Status AVP, Attribute Type 71, MUST be included in ICRQ, ICRP, OCRQ and OCRP messages. The N (New) bit of the Circuit Status AVP MUST be set to 1 in these messages indicating a new circuit, and the A (Active) bit is set to 0 (INACTIVE) or 1 (ACTIVE) reflecting the operational circuit status underneath PPP. This AVP is further described in the context of PPP over L2TPv3 in Section 5.2.1.2.

The Local Session ID AVP, Attribute Type 63, is analogous to the Assigned Session ID in L2TPv2. The Remote Session ID AVP, Attribute Type 64, echoes the value of the Local Session ID AVP received, and MUST be present in all session-level control messages. Additionally, when using the Remote End ID AVP, the Session Tie Breaker AVP, Attribute Type 5, is used to break session-level ties (detected by comparing both the peer's identity as described in Section 3.1 and the value of the Remote End ID AVP).

3.3. Session Maintenance

When PPP is tunneled through L2TP, a session control message, Set-Link-Info (SLI), is used to send PPP-specific link level information between LCCEs.

The SLI is sent by the LNS to the LAC to set any PPP-negotiated options. It is sent after the last LCP CONFACK is received in case of PPP LCP renegotiations, or after the ICCN message with PPP Last CONFREQ AVPs is received when proxy LCP is accepted. This AVP contains any relevant link level parameters of which the LAC may need to be aware (e.g., ACCM info). If there is no relevant information to be sent in the SLI, then the sending of this message MAY be omitted. Since LCP may be renegotiated at any time, an SLI may be sent at any time during the life of the call. For this reason, the LAC MUST be able to update its internal call information and behavior on an active session. Furthermore, if there are packets in queue at the LAC when an SLI is received, these must be flushed before applying the SLI information to the link.

If the PPP session at the LNS renegotiates LCP during the call, an SLI MUST be sent to the LAC to return link level information to the initial default values while the negotiation occurs. However, if the last SLI sent was already set to default values or no SLI was sent at all, this step MAY be omitted.

The SLI MAY be sent from a LAC to indicate a change in the circuit status underneath PPP.

The following AVPs MUST be present in the SLI:

Message Type

This AVP is described in [RFC3931]. In the SLI, the value of this attribute is 16.

The following AVP MAY be present in the SLI:

ACCM

This AVP is described in Section 5.1.4.2.

Circuit Status

In SLI messages, the N (New) bit of the Circuit Status AVP MUST be set to 0 indicating that the status is for an existing circuit. This AVP is described in Section 5.2.1.2.

4. Data Channel Specifics for PPP

This section describes the encapsulation mechanism for forwarding PPP frames over the L2TPv3 data channel.

The general format for tunneling PPP frames over L2TPv3 is as follows:

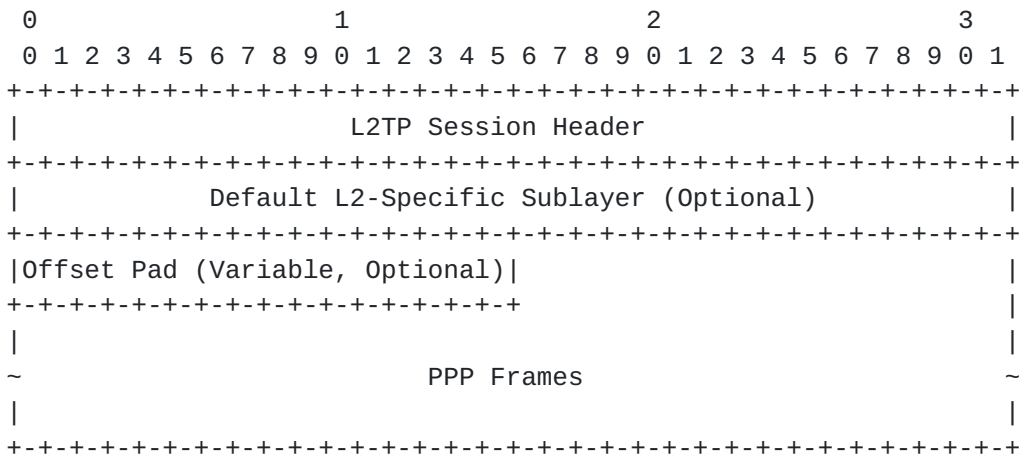


Figure 1: PPP over L2TPv3 encapsulation

The header format for the PPP over L2TPv3 data messages consists of an L2TP Session Header (see Section 4.1 of [RFC3931]) followed by the optional Default L2-specific Sublayer, an optional variable-length Offset Padding and then the Tunnel Payload (PPP Frames).

This document decouples the L2-Specific Sublayer intermediary function (see Section 4.1) from the Offset padding function (see Section 4.2), making them independent from each other. Because those two fields perform orthogonal functions, separating them enables their independent request and existence (i.e., only the Offset Padding field can be requested and present when no functions of the L2-Specific Sublayer such as sequencing are needed). It also simplifies moving the request of the Offset Size downstream to the LCCE receiver of the data packet (see Section 4.2 and Offset Size AVP in Section 5.1.2.9), in a similar fashion as requesting the presence and format of the L2-Specific Sublayer (with the L2-Specific Sublayer AVP) or the size and value of the Cookie (with the Assigned Cookie AVP). The Offset Size request is conditioned by the upstream's LCCE capability (see Section 4.2).

4.1. L2-Specific Sublayer

This section defines the usage and specifics of an L2-Specific Sublayer for PPP over L2TPv3. When an intermediary L2-Specific Sublayer is needed or desired to support features such as sequencing, PPP over L2TPv3 uses the Default L2-Specific Sublayer defined in Section 4.6 of [RFC3931].

The usage of the Default L2-Specific Sublayer is OPTIONAL. However if an L2-Specific Sublayer is requested, it MUST be the Default one. Its presence is requested by a peer during session negotiation using the L2-Specific Sublayer Type AVP, Attribute Type 69, with a value of 1. If the AVP is not received, it is assumed that there is no sublayer present.

4.2. Offset Padding

The optional Offset Padding field MAY be included containing offset padding before the tunneled PPP frame. This field can be used to provide alignment of the data carried in PPP to longword size boundaries for performance reasons, but increases the size of the L2TPv3 packet. The Offset Padding field follows the Default L2-Specific Sublayer if present or the L2TPv3 Session Header otherwise. For a given L2TPv3 Session and direction, all Data Messages have the same Offset Padding Size.

During Control Connection establishment, an LCCE advertises the maximum Offset Padding size that it is willing to insert, if requested at Session establishment, for all the associated Sessions within that Control Connection. This capability advertisement is performed using the Offset Capability AVP (see Section 5.1.1.3), and allows the sender of L2TP data messages (i.e., the upstream LCCE) to have control over the offset size.

The number of octets past the L2TPv3 Session Header or optional L2-Specific Sublayer if present at which the payload data is expected to start (i.e., the size of the Offset Padding field) is signaled during Session establishment using the Offset Size AVP (see Section 5.1.2.9). When an LCCE agrees to support a requested Offset Size during session establishment, it MUST send all data packets including an Offset Padding of that agreed size. The size of the Offset Padding field MAY be different in both directions of the session. An Offset Size of zero signaled during session establishment indicates no offset. The maximum offset value that may be requested by a peer during session negotiation is limited by the offset capability value advertised during control connection establishment. An offset capability of zero advertised during control connection establishment indicates that no offset padding can be requested on sessions within the control connection.

Actual data within the Offset Padding field is undefined, and MUST be ignored on receipt.

4.3. Forwarding PPP Frames

PPP tunneling via L2TPv3 utilizes both the Control Connection for session management and the base L2TPv3 encapsulation for demultiplexing to tunnel the PPP frames. Both of these mechanisms are defined in [RFC3931].

After L2TP control channel establishment (see [RFC3931], and Section 3.1 and Section 3.2 of this document for details on Control Connection and Session establishment), PPP frames are tunneled.

The PPP frames from the remote system are received at the LAC, stripped of CRC, link framing, and transparency bytes, encapsulated with the L2TPv3 data header (see [RFC3931]) followed by the optional Default L2-Specific Sublayer (see Section 4.1) and optional Offset Padding (see Section 4.2) fields, and forwarded over the session. When using PPP in HDLC framing (See [RFC1662]) the PPP frame is stripped of HDLC header (HDLC Address and Control Fields or ACF), flags and trailing FCS. The remaining data, including the protocol field, is transported over the L2TPv3 session. The LNS then receives the L2TPv3 packet and processes the encapsulated PPP frame as if it were received on a local PPP interface. The LNS receives the PPP frame over the L2TP session without the HDLC Address and Control Fields. All framing operations (e.g., CRC, character escaping, etc.) are handled by the LAC. If the LNS wishes to support Address-and-Control-Field-Compression (ACFC) [RFC1661], it MUST support the "LCP Options From LNS to LAC" extensions defined in Section 2.3 of [RFC3437]. The LAC needs to learn the negotiated ACFC settings to know whether the ACF needs to be re-inserted on output towards the

remote system.

When encapsulating the PPP frame in L2TPv3, both the LAC and the LNS MUST always include the PPP Protocol ID field along with the PPP frame. They SHOULD NOT include the HDLC Address and Control Fields (ACF). An LCCE SHOULD strip off the ACF before encapsulating the PPP frames in L2TP and forwarding them over the PPPPW session. The reception and transmission of the HDLC header on a PPP Attachment Circuit (AC) is media specific. If the LAC is providing L2TPv3 transport for a PPP AC that requires HDLC Address and Control Fields, then this information SHOULD be stripped before transmitting the packet into the L2TPv3 session. Similarly, for a PPP AC that requires the HDLC header, the LAC MUST check the presence of the ACF and, if ACF is not present, prepend it to packets received from the L2TPv3 session before transmitting them out of the AC. While the sender SHOULD omit and not send the HDLC Address and Control Fields, a receiver MUST allow the HDLC Address and Control Fields to be present in a received packet, for robustness reasons.

It is worth noting that if an implementation wishes to receive the space equivalent to the HDLC Address and Control Fields in the tunneled PPP frame, it can request a two-octet offset padding with the Offset Size AVP if it received the Offset Capability of at least two from the peer during control connection establishment.

5. AVP Description

The base L2TPv3 specification [RFC3931] describes the use of service type specific Attribute Value Pairs (AVPs). These AVPs are specific to the L2 payload carried by the L2TPv3 sessions. This section provides a description of all PPP-specific AVPs. It also provides additional PPP-specific information about certain other service-independent AVPs when PPP is tunneled by L2TPv3.

Following the name of each AVP is a list indicating the message types that utilize each AVP. These message types are described in the base L2TPv3 specification [RFC3931]. After each AVP title follows a short description of the purpose of the AVP, a detail (including a graphic) of the format for the Attribute Value, and any additional information needed for proper use of the AVP.

5.1. PPP-Specific AVPs

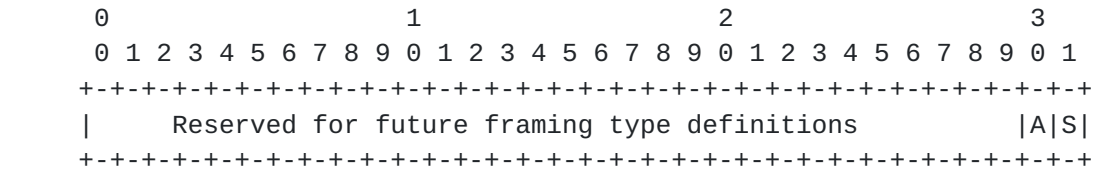
5.1.1. Control Connection Management AVPs

The AVPs described in this section are included in the Control Connection messages.

5.1.1.1. Framing Capabilities (SCCRP, SCCRQ)

The Framing Capabilities AVP, Attribute Type 3, provides the peer with an indication of the types of PPP framing that will be supported for outgoing call requests.

The Attribute Value field for this AVP has the following format:



The Attribute Value field is a 32-bit mask, with two bits defined. If bit A is set, asynchronous framing is supported. If bit S is set, synchronous framing is supported.

The framing capabilities defined in this AVP refer only to the physical interfaces available for dialout usage on an LAC. An LNS MUST NOT send an OCRQ with a Framing Type AVP specifying a value not advertised in this AVP. Presence of this message is not a guarantee that a given outgoing call will be placed by the sender if requested, just that the physical capability exists.

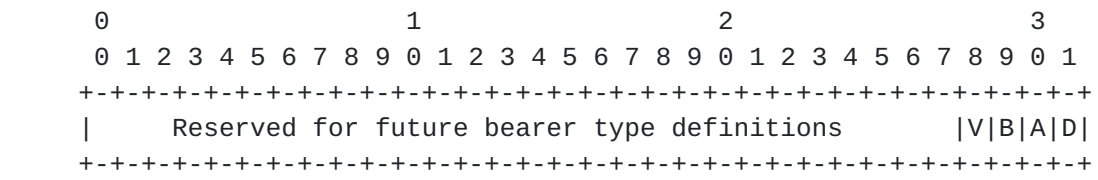
It is RECOMMENDED that an implementation includes all the Framing Capabilities that its software module supports rather than conveying its physical interface capabilities at the time of Control Connection establishment. This way, a shut down and re-establishment of the Control Connection is prevented if new physical interface capabilities are added to the LCCE. This step pushes the capability check to the Session establishment phase. The same recommendation applies to the Bearer Capabilities.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) is 10.

5.1.1.2. Bearer Capabilities (SCCRP, SCCRQ)

The Bearer Capabilities AVP, Attribute Type 4, provides the peer with an indication of the bearer device types supported by the hardware interfaces of the sender for outgoing calls.

The Attribute Value field for this AVP has the following format:



This is a 32-bit mask, with four bits defined. If bit A is set, analog access is supported. If bit D is set, digital access is supported. If bit B is set, broadband access is supported (ATM). If bit V is set, virtual access is supported. (Virtual access refers to access in which there is no physical point-to-point link.)

The bearer capabilities defined in this AVP refer only to the physical interfaces available for dialout usage on an LAC. An LNS MUST NOT send an OCRQ with a Bearer Type AVP specifying a value not advertised in this AVP.

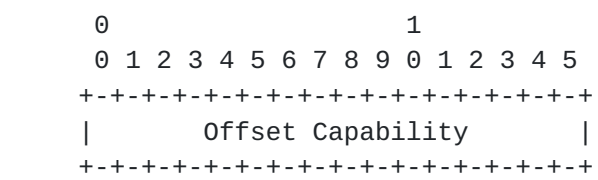
This AVP MUST be present if the sender can place outgoing calls when requested. Presence of this message is not a guarantee that a given outgoing call will be placed by the sender if requested, just that the physical capability exists.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) is 10.

5.1.1.3. Offset Capability (SCCRP, SCCRQ)

The Offset Capability AVP, Attribute Type AVP-TBD-1, indicates the size in octets of the Offset Padding field the sender of this AVP is willing and capable to insert, if requested at Session establishment. The Offset Capability AVP sets the maximum value that an LCCE peer can request in the Offset Size AVP for a session within this control connection (see Section 4.2), allowing the sender of L2TP data messages (i.e., the upstream LCCE) to have control over the offset size.

The Attribute Value field for this AVP has the following format:



The Offset Capability is a 2-octet unsigned integer. If absent, the peer MUST assume a value of zero, which implies that the peer MUST

NOT request Offset Padding (i.e., MUST NOT send the Offset Size AVP for sessions within this control connection).

A missing Offset Capability AVP or an Offset Capability AVP with a value of zero indicates that the Offset Size AVP cannot be sent by the peer LCCE. If this AVP is received and has a value other than zero, the receiving LCCE can request an Offset Padding using the Offset Size AVP up to the value indicated in this AVP.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 8.

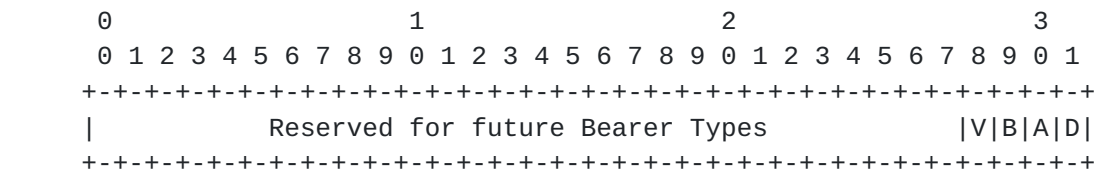
5.1.2. Session Management AVPs

This section describes Session (i.e., Call) Management AVPs.

5.1.2.1. Bearer Type (ICRQ, OCRQ)

The Bearer Type AVP, Attribute Type 18, encodes the bearer type for the incoming or outgoing call.

The Attribute Value field for this AVP has the following format:



The Bearer Type is a 32-bit bit mask indicating the bearer capability of the call (ICRQ) or required for the call (OCRQ). Bit A refers to an analog channel. Bit D refers to a digital channel. Bit B refers to broadband access. Bit V (virtual) refers to a channel for which there is no physical point-to-point link.

Bits set in the Bearer Type AVP in an OCRQ message indicate the bearer type(s) on which an outgoing call may be placed. If more than one bit is set, the LAC may choose the bearer type with which to place the call. If no bits are set, any type of available channel may be used.

Bits in the Value field of this AVP MUST only be set by the LNS for an OCRQ if the same bit was set in the Bearer Capabilities AVP received from the LAC during Control Connection establishment.

Bits set in the Bearer Type AVP in an ICRQ message indicate the bearer type on which an incoming call was received at the LAC. If no bits are set in an ICRQ, then it is assumed that the bearer type was

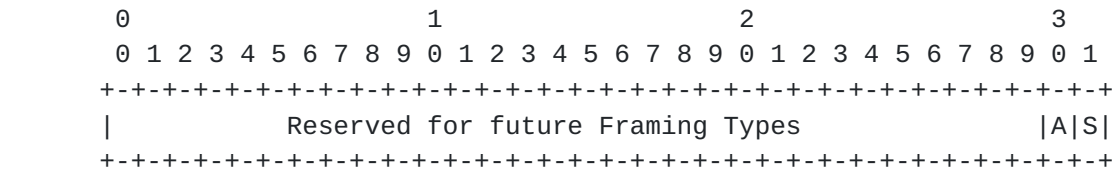
indeterminable.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 10.

5.1.2.2. Framing Type (ICCN, OCCN, OCRQ)

The Framing Type AVP, Attribute Type 19, encodes the framing type for the incoming or outgoing call.

The Attribute Value field for this AVP has the following format:



The Framing Type is a 32-bit mask, which indicates the type of PPP framing requested for an OCRQ, or the type of PPP framing negotiated for an OCCN or ICCN.

Bit A indicates asynchronous framing. Bit S indicates synchronous framing. For an OCRQ, both may be set, indicating that the LAC may decide the type of framing to be used.

For an ICCN, only one framing type bit may be set. The framing type SHOULD be used as an indication to PPP on the LNS as to what link options to use for LCP negotiation [RFC1662]. For example, if the A bit is not set in the Framing Type AVP in an ICCN message and an ACCM LCP option is requested by the PPP client, then the LNS should try to respond with no bits set in the ACCM mask, since the LAC will not likely perform async mapping on a non-async interface.

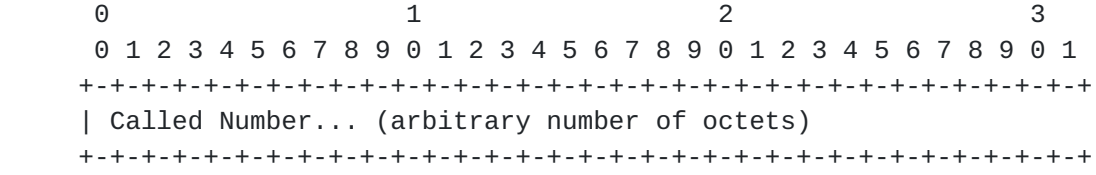
Bits in the Value field of this AVP MUST only be set by the LNS for an OCRQ if it was set in the Framing Capabilities AVP received from the LAC during Control Connection establishment.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 10.

5.1.2.3. Called Number (ICRQ, OCRQ)

The Called Number AVP, Attribute Type 21, encodes the telephone number to be called for an OCRQ, and the called number for an ICRQ.

The Attribute Value field for this AVP has the following format:



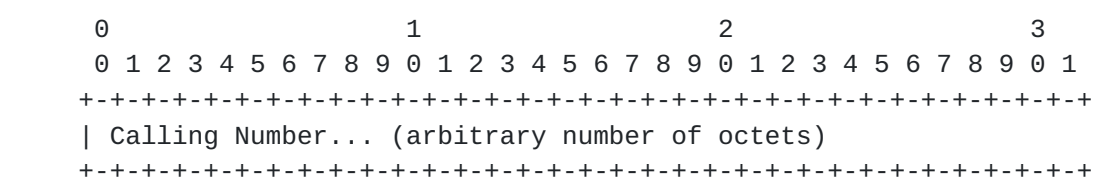
The Called Number is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value needed in this AVP. Additionally, other Called Number encodings MAY be defined to be interpreted in the context of the Bearer Type in use for the specific call. An example of alternate encoding is defined in [RFC3301]. Newly defined alternate encodings qualified by the Bearer Type SHOULD use ASCII encoding of the value, although the value of this AVP is binary encoded when the B bit is set in the Bearer Type AVP [RFC3301].

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 6 plus the length of the Called Number.

5.1.2.4. Calling Number (ICRQ)

The Calling Number AVP, Attribute Type 22, encodes the originating number for the incoming call.

The Attribute Value field for this AVP has the following format:



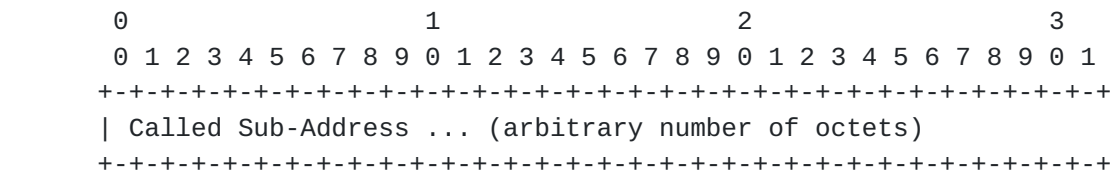
The Calling Number is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value in this AVP. Additionally, other Calling Number encodings MAY be defined to be interpreted in the context of the Bearer Type in use for the specific call. An example of alternate encoding is defined in [RFC3301]. Newly defined alternate encodings qualified by the Bearer Type SHOULD use ASCII encoding of the value, although the value of this AVP is binary encoded when the B bit is set in the Bearer Type AVP [RFC3301].

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 6 plus the length of the Calling Number.

5.1.2.5. Called Sub-Address (ICRQ, OCRQ)

The Called Sub-Address AVP, Attribute Type 23, encodes additional called party dialing information. For instance, it can be used by the LNS to encode the ISDN sub-address information for an outgoing call request.

The Attribute Value field for this AVP has the following format:



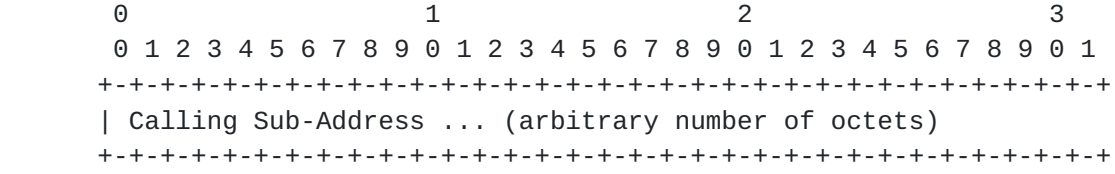
The Called Sub-Address is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value in this AVP. Additionally, other Called Sub-Address encodings MAY be defined to be interpreted in the context of the Bearer Type in use for the specific call. An example of alternate encoding is defined in [RFC3301]. Newly defined alternate encodings qualified by the Bearer Type SHOULD use ASCII encoding of the value, although the value of this AVP is binary encoded when the B bit is set in the Bearer Type AVP [RFC3301].

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 6 plus the length of the Called Sub-Address.

5.1.2.6. Calling Sub-Address (ICRQ)

The Calling Sub-Address AVP, Attribute Type 44, encodes additional calling party information. For instance, it can be used by the LAC to encode the ISDN sub-address information for an incoming call request.

The Attribute Value field for this AVP has the following format:



The Calling Sub-Address is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value in this AVP. Additionally, other Calling Sub-Address encodings MAY be defined to be interpreted in the context

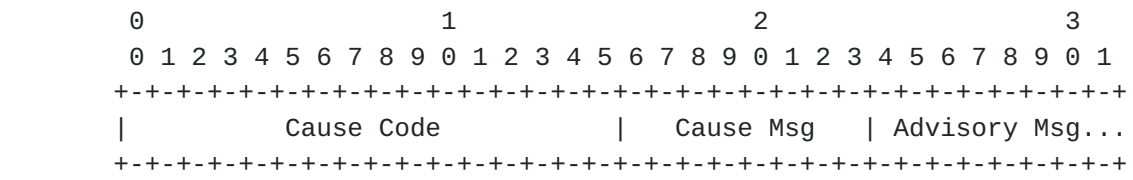
of the Bearer Type in use for the specific call. An example of alternate encoding is defined in [RFC3301]. Newly defined alternate encodings qualified by the Bearer Type SHOULD use ASCII encoding of the value, although the value of this AVP is binary encoded when the B bit is set in the Bearer Type AVP [RFC3301].

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 6 plus the length of the Calling Sub-Address.

5.1.2.7. Q.931 Cause Code (CDN)

The Q.931 Cause Code AVP, Attribute Type 12, is used to give additional information in case of unsolicited call disconnection.

The Attribute Value field for this AVP has the following format:



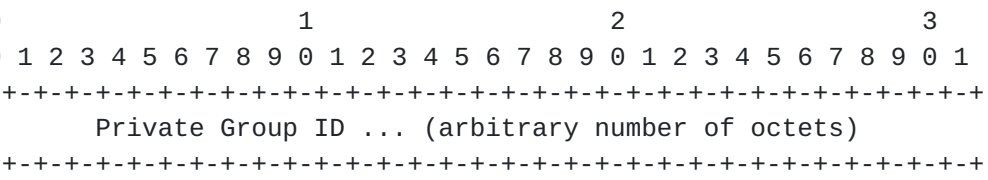
The Cause Code field is the returned Q.931 cause code, and the Cause Msg field is the returned Q.931 message code (e.g., DISCONNECT) associated with the cause code. Both values are returned in their native ITU encodings [ITU.Q931.1998]. Additionally, the Cause Code field can carry Cause Codes specific to ATM signaling messages as described in [RFC3301]. The Cause code should be interpreted relative to the Bearer Type in use for the specific call. An additional ASCII text Advisory Message may also be included (presence indicated by the AVP Length) to further explain the reason for disconnecting.

This AVP MUST NOT be hidden (the H bit MUST be 0). The M bit for this AVP MUST be set to 1. The Length of this AVP is 9, plus the size of the Advisory Message.

5.1.2.8. Private Group ID (ICCN)

The Private Group ID AVP, Attribute Type 37, is used by the LAC to indicate that this call is to be associated with a particular customer group.

The Attribute Value field for this AVP has the following format:



The Private Group ID is a string of octets of arbitrary length.

The LNS MAY treat the PPP session as well as network traffic through this session in a special manner determined by the peer. For example, if the LNS is individually connected to several private networks using unregistered addresses, this AVP may be included by the LAC to indicate that a given call should be associated with one of the private networks.

The Private Group ID is an ASCII string. Contact between the administrator of the LAC and the LNS may be necessary to coordinate interpretation of the value of this AVP.

The LNS MAY treat the PPP session as well as network traffic through this session in a special manner determined by the Private Group ID value. The Private Group ID defines the particular characteristics of the selected group. For example, the LNS could interpret this AVP to route traffic from this session to a particular interface or private network.

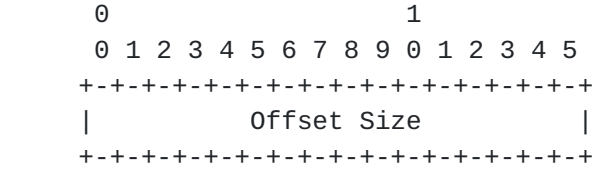
A LAC MAY determine the Private Group ID from an AAA (Authentication, Authorization and Accounting) protocol response response, local configuration, or some other source.

This AVP may be hidden (the H-bit MAY be 1 or 0). The M-bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6 plus the length of the Private Group ID.

5.1.2.9. Offset Size (ICRQ, ICRP, ORCQ, OCRP)

The Offset Size AVP, Attribute Type AVP-TBD-2, indicates the size in octets of the Offset Padding field the sender of this AVP requires on all incoming data packets for this L2TP session. It allows an LCCE to request the peer includes an Offset Padding in all data messages (see Section 4.2), and is conditioned to the value received in the Offset Capability AVP.

The Attribute Value field for this AVP has the following format:



The Offset Size is a 2-octet unsigned integer. The maximum value for the Offset Size is the value that the peer LCCE advertised in the Offset Capability AVP during control connection establishment. If this AVP is absent, the peer MUST assume a value of zero.

A missing Offset Size AVP or an Offset Size AVP with a value of zero indicates that the Offset Padding field should not be present in any data packets sent to the LCCE sending this AVP. If this AVP is received and has a value other than zero (and less than or equal to the received Offset Capability AVP for the control connection), the receiving LCCE MUST include an Offset Padding of the requested size in its outgoing data messages.

If the LCCE receiving this AVP has not advertised an Offset Capability AVP, if the requested size is greater than the value advertised in the Offset Capability AVP, or if the LCCE receiving this AVP is not capable, configured or willing to include an Offset Padding field of the requested size, the LCCE MUST reject the session via a CDN message with the following General Result Code:

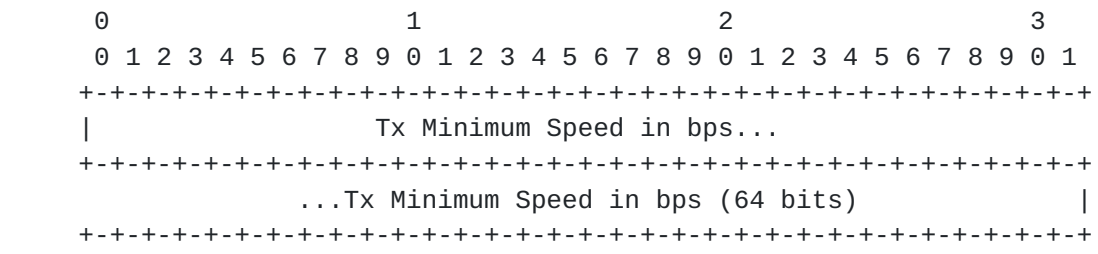
RC-TBD1: Session not established due to unsupported Offset Size

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 8.

5.1.2.10. Tx Minimum Speed (OCRQ)

The Tx Minimum Speed AVP, Attribute Type AVP-TBD-3, encodes the lowest acceptable line speed for this call over a dial-up or ATM access network. This is the lowest acceptable line speed in the transmit direction (i.e. the direction from the LAC to the user).

The Attribute Value field for this AVP has the following format:



The Tx Minimum Speed BPS is an 8-octet value indicating the speed in bits per second. This speed is the minimum line speed (for example, modem connect speed) in the transmit direction. When the optional Rx Minimum Speed AVP is NOT present, then symmetric transmission is implied, with both minimum receive and transmit bit-rates equal to the Tx Minimum Speed BPS.

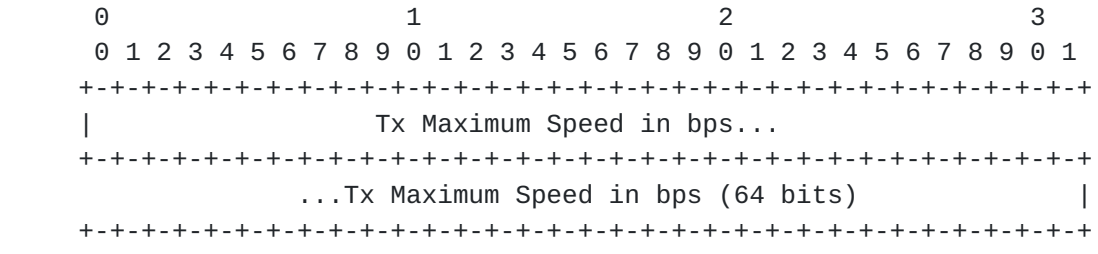
The Minimum BPS AVP, Attribute Type 16, MUST NOT be used in PPP over L2TPv3 signaling.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 14.

5.1.2.11. Tx Maximum Speed (OCRQ)

The Tx Maximum Speed AVP, Attribute Type AVP-TBD-4, encodes the highest acceptable line speed for this call in the transmit direction (i.e. from LAC to the user).

The Attribute Value field for this AVP has the following format:



The Tx Maximum Speed BPS is an 8-octet value indicating the speed in bits per second. This speed is the maximum line speed (for example, modem connect speed) in the transmit direction. When the optional Rx Maximum Speed AVP is NOT present, then symmetric transmission is implied, with both maximum receive and transmit bit-rates equal to the Tx Maximum Speed BPS.

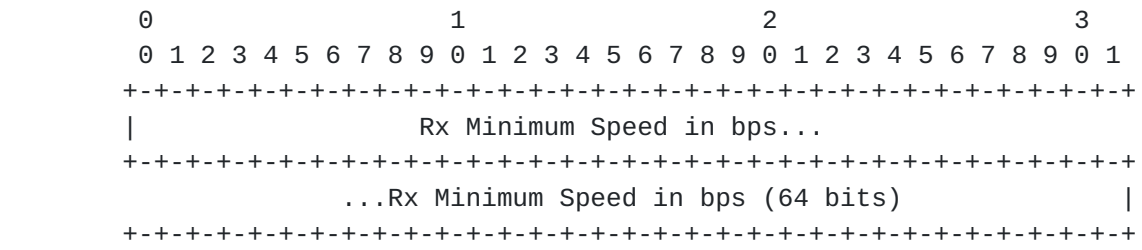
The Maximum BPS AVP, Attribute Type 17, MUST NOT be used in PPP over L2TPv3 signaling.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 1. The Length (before hiding) of this AVP is 14.

5.1.2.12. Rx Minimum Speed (OCRQ)

The Rx Minimum Speed AVP, Attribute Type AVP-TBD-5, encodes the lowest acceptable line speed for this call in the receive direction (i.e., data flowing from the remote system to the LAC), for cases where asymmetric transmission may be required.

The Attribute Value field for this AVP has the following format:



The Rx Minimum Speed BPS is an 8-octet value indicating the speed in bits per second. This speed is the minimum line speed (for example, modem connect speed) in the receive direction. Presence of this AVP implies that the connection speed may be asymmetric with respect to the Tx Minimum Speed BPS.

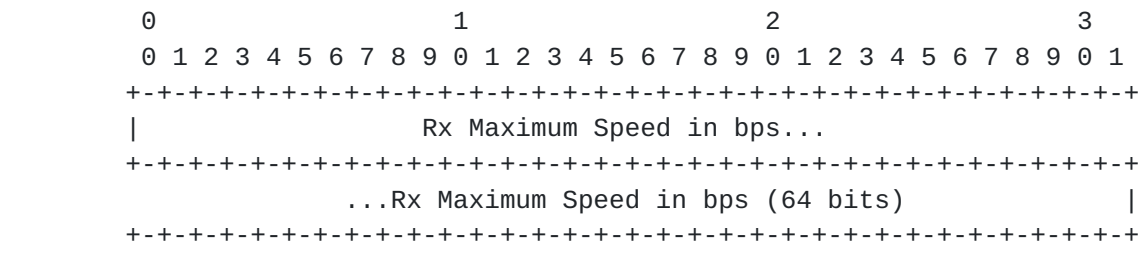
The Rx Minimum BPS AVP, Attribute Type 40, MUST NOT be used in PPP over L2TPv3 signaling.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 14.

5.1.2.13. Rx Maximum Speed (OCRQ)

The Rx Maximum Speed AVP, Attribute Type AVP-TBD-6, encodes the highest acceptable line speed for this call in the receive direction (i.e., data flowing from the remote system to the LAC), for cases where asymmetric transmission may be required.

The Attribute Value field for this AVP has the following format:



The Rx Maximum Speed BPS is an 8-octet value indicating the speed in bits per second. This speed is the maximum line speed (for example, modem connect speed) in the receive direction. Presence of this AVP implies that the connection speed may be asymmetric with respect to the Tx Maximum Speed BPS.

The Rx Maximum BPS AVP, Attribute Type 41, MUST NOT be used in PPP over L2TPv3 signaling.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 14.

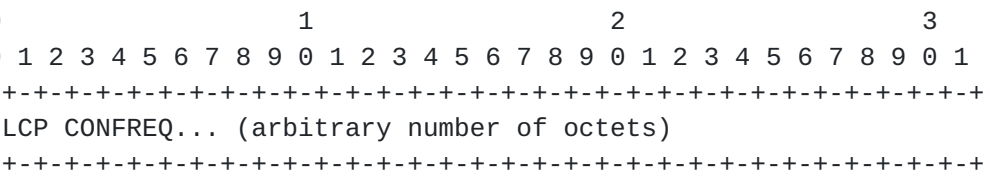
5.1.3. Proxy LCP and Authentication AVPs

The LAC may have answered the call and negotiated LCP with the remote system, perhaps in order to establish the system's apparent identity. In this case, these AVPs may be included to indicate, first, the link properties the remote system initially requested, and second, the properties the remote system and LAC ultimately negotiated. In addition, the authentication information can be sent by the LAC by including the proxy authentication AVPs. This information may be used to initiate the PPP LCP and authentication states on the LNS, allowing PPP to continue without renegotiation of LCP. Note that the LNS policy may be to enter an additional round of LCP negotiation and/or authentication if the LAC is not trusted.

5.1.3.1. Initial Received LCP CONFREQ (ICCN)

In the Initial Received LCP CONFREQ AVP, Attribute Type 26, the LAC provides the LNS with the Initial CONFREQ received by the LAC from the PPP Peer.

The Attribute Value field for this AVP has the following format:



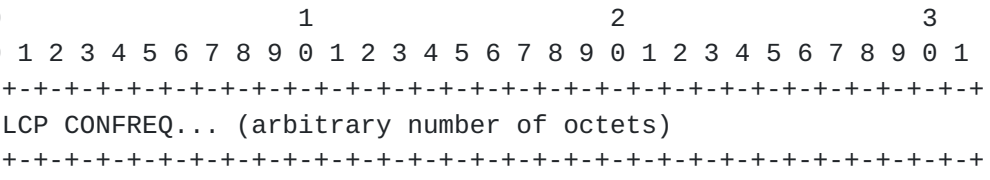
The LCP CONFREQ is a copy of the body of the initial CONFREQ received, starting at the first option within the body of the LCP message.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6 plus the length of the CONFREQ.

5.1.3.2. Last Sent LCP CONFREQ (ICCN)

The Last Sent LCP CONFREQ AVP, Attribute Type 27, provides the LNS with the Last CONFREQ sent by the LAC to the PPP Peer.

The Attribute Value field for this AVP has the following format:



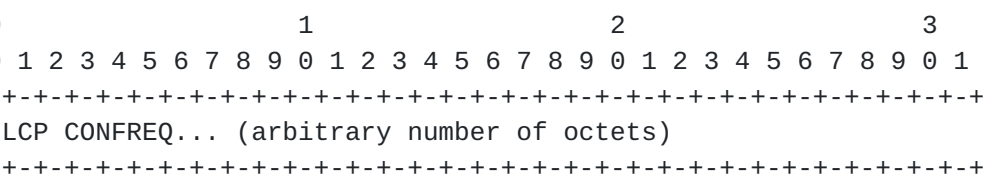
The LCP CONFREQ is a copy of the body of the final CONFREQ sent to the client to complete LCP negotiation, starting at the first option within the body of the LCP message.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6 plus the length of the CONFREQ.

5.1.3.3. Last Received LCP CONFREQ (ICCN)

The Last Received LCP CONFREQ AVP, Attribute Type 28, provides the LNS with the Last CONFREQ received by the LAC from the PPP Peer.

The Attribute Value field for this AVP has the following format:



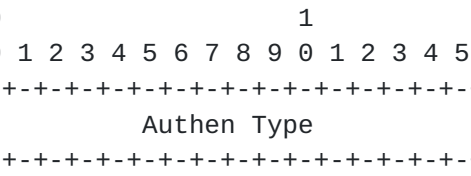
The LCP CONFREQ is a copy of the body of the final CONFREQ received from the client to complete LCP negotiation, starting at the first option within the body of the LCP message.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6 plus the length of the CONFREQ.

5.1.3.4. Proxy Authen Type (ICCN)

The Proxy Authen Type AVP, Attribute Type 29, indicates the type of authentication that was performed for this call by the LAC, if any.

The Attribute Value field for this AVP has the following format:



Authen Type is a 2-octet unsigned integer.

Defined Authen Type values are maintained by IANA. Currently defined values, which are referenced in upcoming AVP definitions, are:

0 - Reserved

1 - Textual username/password exchange

2 - PPP CHAP

3 - PPP PAP

4 - No authentication

5 - Microsoft CHAP Version 1 (MSCHAPv1)

This AVP MUST be present if proxy authentication is to be utilized. If it is not present, then it is assumed that this peer cannot

perform proxy authentication. In this case, a restart of the authentication phase at the LNS is required if the client has already entered this phase with the LAC (which may be determined by the presence of the Proxy LCP AVP).

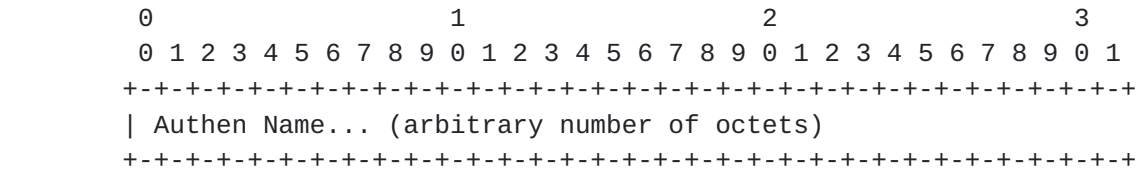
This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 8.

Associated AVPs for each type of authentication follow.

5.1.3.5. Proxy Authen Name (ICCN)

The Proxy Authen Name AVP, Attribute Type 30, specifies the name of the authenticating client when using proxy authentication.

The Attribute Value field for this AVP has the following format:



Authen Name is a string of octets of arbitrary length. It contains the name specified in the client's authentication response.

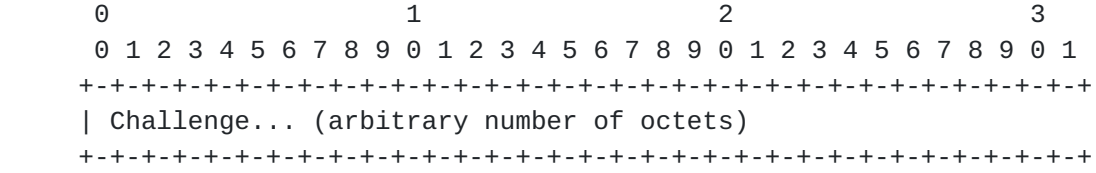
This AVP MUST be present in messages containing a Proxy Authen Type AVP with an Authen Type of 1, 2, 3 or 5. It may be desirable to employ AVP hiding for obscuring the cleartext name.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) is 6 plus the length of the cleartext name.

5.1.3.6. Proxy Authen Challenge (ICCN)

The Proxy Authen Challenge AVP, Attribute Type 31, specifies the challenge sent by the LAC to the PPP Peer when using proxy authentication.

The Attribute Value field for this AVP has the following format:



The Challenge is a string of one or more octets.

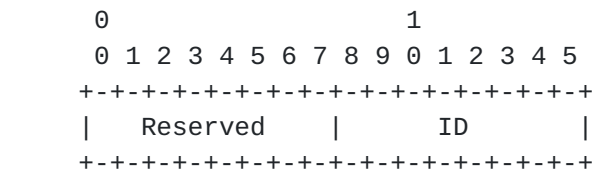
This AVP MUST be present for Proxy Authen Types 2 and 5. The Challenge field contains the CHAP challenge presented to the client by the LAC.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6, plus the length of the Challenge.

5.1.3.7. Proxy Authen ID (ICCN)

The Proxy Authen ID AVP, Attribute Type 32, specifies the ID value of the PPP Authentication that was started between the LAC and the PPP Peer when proxy authentication is being used.

The Attribute Value field for this AVP has the following format:



ID is a 2-octet unsigned integer. The most significant octet MUST be 0.

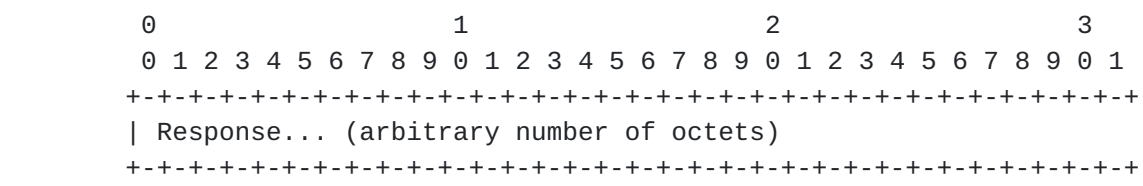
The Proxy Authen ID AVP MUST be present for Proxy Authen Types 2, 3 and 5. For 2 and 5, the ID field contains the byte ID value presented to the client by the LAC in its Challenge. For 3, it is the Identifier value of the Authenticate-Request.

This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 8.

5.1.3.8. Proxy Authen Response (ICCN)

The Proxy Authen Response AVP, Attribute Type 33, specifies the PPP Authentication response received by the LAC from the PPP Peer, when proxy authentication is used.

The Attribute Value field for this AVP has the following format:



The Response is a string of octets.

This AVP MUST be present for Proxy Authen Types 1, 2, 3 and 5. The Response field contains the client's response to the challenge. For Proxy Authen Types 2 and 5, this field contains the response value received by the LAC. For 1 and 3, it contains the cleartext password received from the client by the LAC. In the case of cleartext passwords, AVP hiding is recommended.

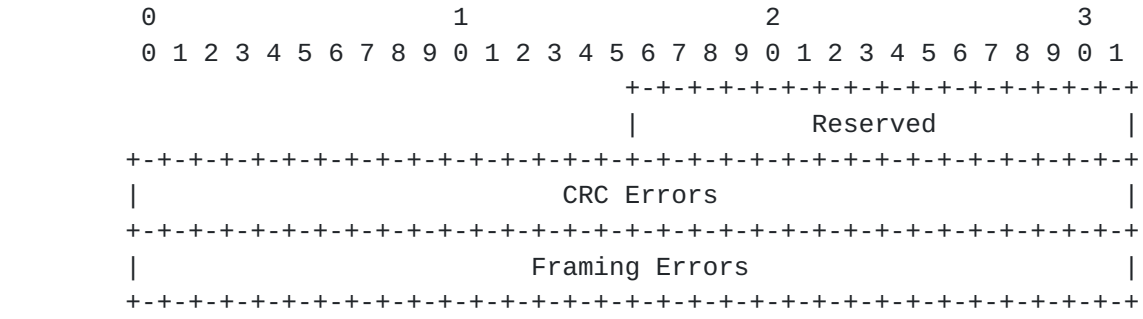
This AVP may be hidden (the H bit may be 0 or 1). The M bit for this AVP MUST be set to 0. The Length (before hiding) of this AVP is 6 plus the length of the Response.

5.1.4. Session Status AVPs

5.1.4.1. PPP Circuit Errors (WEN)

The PPP Circuit Errors AVP, Attribute Type AVP-TBD-7, conveys PPP specific circuit error information to the peer, and complements the Circuit Errors AVP, Attribute Type 34.

The Attribute Value field for this AVP has the following format:



The following fields are defined:

Reserved:
Two octets of Reserved data is present (providing longword alignment within the AVP of the following values). Reserved data MUST be zero on sending and ignored upon receipt.

CRC Errors:
Number of PPP frames received with CRC errors since the session was established.

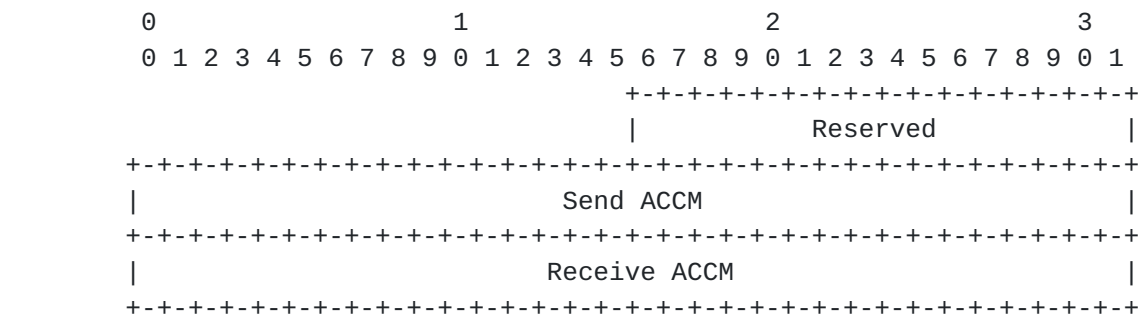
Framing Errors:
Number of improperly framed PPP packets received.

This AVP may be hidden (the H bit MAY be 1 or 0). The M bit for this AVP SHOULD be set to 0. The Length of (before hiding) this AVP is 16.

5.1.4.2. ACCM (SLI)

The ACCM AVP, Attribute Type 35, is used by the LNS to inform the LAC of the ACCM negotiated with the PPP Peer by the LNS.

The Attribute Value field for this AVP has the following format:



The Send ACCM and Receive ACCM fields are 4-octet values preceded by a 2-octet reserved quantity. The Reserved field provides longword alignment within the AVP of the Send and Receive ACCM values, and MUST be zero on sending and ignored upon receipt. The Send ACCM value should be used by the LAC to process packets it sends on the connection. The Receive ACCM value should be used by the LAC to process incoming packets on the connection. The default values used by the LAC for both these fields are 0xFFFFFFFF. The LAC should honor these fields unless it has specific configuration information to indicate that the requested mask must be modified to permit operation.

This AVP may be hidden (the H bit MAY be 1 or 0). The M bit for this AVP MUST be set to 1. The Length of this AVP is 16.

5.2. Service Type Independent AVPs

The base L2TPv3 specification [RFC3931] gives a detailed description of these AVPs. However, the AVP values described in [RFC3931] should be interpreted differently for different service type payloads

carried by L2TPv3. This section describes the AVP values in the context of the PPP Pseudowire Type. This section should be read in conjunction with the relevant sections from [RFC3931].

5.2.1. Session Management AVPs

This section describes Session (i.e., Call) Management service type independent AVPs.

5.2.1.1. Data Sequencing (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN)

The Data Sequencing AVP, Attribute Type 70, indicates that the sender requires some or all of the data packets that it receives to be sequenced.

The Data Sequencing AVP contains a 2-octet unsigned integer value, Data Sequencing Level, that indicates the degree of incoming data traffic that the sender of this AVP wishes to be marked with sequence numbers.

For PPP over L2TPv3 session establishment, Data sequencing may only be requested when the Default L2-Specific Sublayer is present to provide sequence numbers. If sequencing is requested without requesting the Default L2-Specific Sublayer in the L2-Specific Sublayer AVP, the session MUST be disconnected with a Result Code of 15 (see Section 5.4.2) of [RFC3931].

The Data Sequencing AVP is defined in Section 5.4.4 of [RFC3931]. The Sequencing Required AVP, Attribute Type 39, MUST NOT be used in PPP over L2TPv3 signaling.

5.2.1.2. Circuit Status (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN, SLI)

The Circuit Status AVP, Attribute Type 71, indicates the initial status of or a status change in the call to which the session is bound.

The Circuit Status AVP contains a 2-octet bitmask with two bits currently defined: The A (Active) bit and the N (New) bit.

For PPP over L2TPv3 session establishment, this AVP MUST be included in ICRQ, ICRP, OCRQ and OCRP messages, and MAY be included in ICCN, OCCN and SLI messages. In ICRQ, ICRP, OCRQ and OCRP messages, the N (New) bit MUST be set to 1 to indicate a new circuit.

In SLI messages, the Circuit Status AVP MAY be sent to advertise a change to Inactive to indicate that the call is down without tearing down the entire session. In this case, all data traffic for that

session MUST cease (or not begin) in the direction towards the sender of the Circuit Status AVP and data traffic from the sender of the SLI message with Inactive Circuit Status MUST be ignored. If the receiver of the SLI message with the Inactive indication is unable to stop data traffic, it MUST tear down the session with a CDN message. When the call comes back up, a new SLI message is used to re-advertise the subsequent Active state, the LNS MUST renegotiate PPP, and data traffic MUST continue (or start) upon successful renegotiation.

If a session is started with an initial status of Inactive, the Circuit Status AVP MUST be sent in an SLI when the circuit becomes Active.

The Circuit Status AVP is defined in Section 5.4.5 of [RFC3931].

5.2.1.3. Tx Connect Speed (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN)

The Tx Connect Speed AVP, Attribute Type 74, contains the speed of the facility chosen for the connection attempt.

The Tx Connect Speed AVP contains an 8-octet value, Tx Connect Speed BPS, that indicates the speed in bits per second. A value of zero indicates that the speed is indeterminable or that there is no physical point-to-point link.

When the optional Rx Connect Speed AVP is present, the value in this AVP represents the transmit connect speed from the perspective of the LAC (i.e., data flowing from the LAC to the remote system). When the optional Rx Connect Speed AVP is NOT present, the connection speed between the remote system and LAC is assumed to be symmetric and is represented by the single value in this AVP.

The Tx Connect Speed AVP is defined in Section 5.4.4 of [RFC3931]. The (Tx) Connect Speed BPS AVP, Attribute Type 24, MUST NOT be used in PPP over L2TPv3 signaling.

5.2.1.4. Rx Connect Speed (ICRQ, ICRP, ICCN, OCRQ, OCRP, OCCN)

The Rx Connect Speed AVP, Attribute Type 75, represents the receive connect speed of the connection from the perspective of the LAC (i.e., data flowing from the remote system to the LAC).

The Rx Connect Speed AVP contains an 8-octet value, Rx Connect Speed BPS, that indicates the speed in bits per second. A value of zero indicates that the speed is indeterminable or that there is no physical point-to-point link.

Presence of this AVP implies that the connection speed may be asymmetric with respect to the transmit connect speed given in the Tx Connect Speed AVP.

The Rx Connect Speed AVP is defined in Section 5.4.4 of [RFC3931]. The Rx Connect Speed BPS AVP, Attribute Type 38, MUST NOT be used in PPP over L2TPv3 signaling.

6. Data Channel Sequencing

The general procedures for sequencing data packets are defined in Section 4.6.1 of the base L2TPv3 specification [RFC3931]. Additionally, Appendix C of [RFC3931] provides sequence number processing considerations.

This section describes the method for using sequence numbers on the L2TPv3 data plane carrying PPP frames. It also provides guidelines on when to use these sequence numbers.

6.1. Sequence Numbers

The Sequence Number field defined in the Default L2-Specific Sublayer header allows an LCCE to convey sequence information to a peer. Unlike the L2TPv3 control plane, the L2TPv3 data plane carrying PPP frames does not use sequencing to retransmit lost data messages. Rather, sequencing may be used to detect lost packets and/or restore the original sequence of packets that may have been reordered during traversal of the packet network.

The sequence number begins at 0, which is a valid sequence number. Each subsequent message is sent with the next increment of the sequence number. The sequence number is thus a free-running counter represented modulo 2^24. The sequence number in the header of a received message is considered less than or equal to the last received number if its value lies in the range of the last received number and the preceding (2^23 - 1) values, inclusive. For example, if the last received sequence number was 15, then messages with sequence numbers 0 through 15, as well as 8388624 through 16777215, would be considered less than or equal.

When desired, sequencing may be enabled on some or all packets by using the S bit and Sequence Number field defined in the L2-Specific Sublayer (see Section 4.1). For a given L2TPv3 session, each LCCE is responsible for communicating to its peer the level of sequencing support that it requires of data packets that it receives using the Data Sequencing AVP in Section 5.2.1.1. Mechanisms to advertise this information during session negotiation are provided (see Data

Sequencing AVP in Section 5.4.4).

6.2. Data Channel Sequencing over Specific Media

When PPP frames are carried over an L2TP-over-IP or L2TP-over-UDP/IP data channel to the PPP client, this link has the characteristic of being able to reorder or silently drop packets. Reordering may break non-IP protocols being carried by PPP, especially LAN-centric ones such as bridging. Silent dropping of packets may break protocols that assume per-packet indication of error, such as TCP header compression.

If any protocol being transported by PPP over these L2TP data channels cannot tolerate reordering, sequencing may be turned on by using the sequence number field in the L2-Specific Sublayer header. The sequence dependency characteristics of individual protocols are outside the scope of this document.

Allowing packets to be dropped silently is perhaps more problematic with some protocols. If PPP reliable delivery [RFC1663] is enabled, no upper PPP protocol will encounter lost packets. If sequence numbers are enabled, L2TP can detect the packet loss. In the case of an LNS, the PPP and L2TP stacks are both present within the LNS, and packet loss signaling may occur precisely as if a packet was received with a CRC error. Where the LAC and PPP stack are co-resident, this technique also applies. Where the LAC and PPP client are physically distinct, the analogous signaling MAY be accomplished by sending a packet with a CRC error to the PPP client. Note that this would greatly increase the complexity of debugging client line problems, since the client statistics could not distinguish between true media errors and LAC-initiated ones. Further, this technique is not possible on all hardware.

If VJ compression is used, and neither PPP reliable delivery nor sequence numbers are enabled, each lost packet results in a 1 in 2^16 chance of a TCP segment being forwarded with incorrect contents [RFC1144]. Where the combination of the packet loss rate with this statistical exposure is unacceptable, TCP header compression SHOULD NOT be used.

In general, it is wise to remember that the L2TP-over-IP as well as the L2TP-over-UDP/IP transports are unreliable transport media. As with any PPP medium that is subject to loss, care should be taken when using protocols that are particularly loss-sensitive. Such protocols include compression and encryption protocols that employ history.

7. Acknowledgements

The L2TP rewrite team for splitting RFC2661 into the base and companion PPP specifications consisted of Ignacio Goyret, Jed Lau, Bill Palter, Mark Townsley, and Madhvi Verma.

This document was based upon RFC2661, for which a number of people provided valuable input and effort:

The basic concept for L2TP and many of its protocol constructs were adopted from L2F [RFC2341] and PPTP [RFC2637]. Authors of these are A. Valencia, M. Littlewood, T. Kolar, K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn.

Dory Leifer made valuable refinements to the protocol definition of L2TP and contributed to the editing of early drafts leading to [RFC2661].

Steve Cobb and Evan Caves redesigned the state machine tables.

Barney Wolff provided a great deal of design input on the endpoint authentication mechanism.

John Bray, Greg Burns, Rich Garrett, Don Grosser, Matt Holdrege, Terry Johnson, Dory Leifer, and Rich Shea provided valuable input and review at the 43rd IETF in Orlando, FL., which led to improvement of the overall readability and clarity of [RFC2661].

Thomas Narten provided a great deal of critical review, formatting, and wrote the initial IANA Considerations section.

Bill Storer, Madhvi Verma, Skip Booth and Maria Alice Dos Santos provided thorough reviews, most helpful input and many valuable comments and suggestions for the newer versions of the document.

Later, Mahesh Kelkar provided a healthy review of this document. Y Prasad provided input and comments on the handling of the offset padding. Alfred Hoenes provided many editorial suggestions that improved the text.

8. IANA Considerations

This document defines "magic" numbers to be maintained by the IANA. The Layer Two Tunneling Protocol "L2TP" Name Spaces are reachable from [IANA.l2tp-parameters].

Section 8.1 through Section 8.6 are registrations of new L2TP values

for registries already managed by IANA, and in some cases, description of the assignment policy for those registries.

8.1. AVP Attributes

As defined in [RFC3931], AVPs contain Vendor ID, Attribute, and Value fields. For a Vendor ID value of 0, IANA will maintain a registry of assigned Attributes for the PPP-specific AVPs described in Section 5, and in some cases, values for those attributes. Seven new AVPs need assignment by IANA as described in Section 2.2 of [RFC3438].

A summary of the new AVPs follows:

Control Message Attribute Value Pairs

Attribute Type	Description
AVP-TBD-1	Offset Capability AVP
AVP-TBD-2	Offset Size AVP
AVP-TBD-3	Tx Minimum Speed AVP
AVP-TBD-4	Tx Maximum Speed AVP
AVP-TBD-5	Rx Minimum Speed AVP
AVP-TBD-6	Rx Maximum Speed AVP
AVP-TBD-7	PPP Circuit Errors

Additionally, IANA is requested to rename the Sub-Address AVP, Attribute Type 23, to "Called Sub-Address AVP".

8.2. Pseudowire Type

The signaling mechanisms defined in this document rely upon the allocation of the following Pseudowire Type (see Pseudowire Capabilities List as defined in Section 5.4.3 of [RFC3931], and L2TPv3 Pseudowire Types in Section 10.6 of [RFC3931]) by the IANA. The number space is already created as part of the publication of [RFC3931]. The PPP Pseudowire Type is defined in Section 3.1 of this specification:

L2TPv3 Pseudowire Types	
0x0007	PPP Pseudowire Type

8.3. Result Code AVP Values

A new L2TP Result Code for the CDN message appears in Section 5.1.2.9 which need assignment by IANA as described in Section 2.3 of [RFC3438].

Result Code AVP (Attribute Type 1) Values

Defined Result Code values for the CDN message are:

RC-TBD1: Session not established due to unsupported Offset Size

8.4. Bearer Capabilities and Bearer Type

The Bearer Capabilities AVP and Bearer Type AVP (defined in Section 5.1.1.2 and Section 5.1.2.1 respectively) both contain a 32-bit bitmask called Bearer Field, which is maintained by IANA.

There is one new bitfield value allocated for this specification:

Value	Meaning
0x00000008	V-bit (Virtual access)

Additional bits should only be assigned via Standards Action [RFC5226].

8.5. Framing Capabilities and Framing Type

The Framing Capabilities AVP and Framing Type AVP (defined in Section 5.1.1.1 and Section 5.1.2.2 respectively) both contain a 32-bit bitmask, Framing Field, maintained by IANA. Additional bits should only be assigned via Standards Action [RFC5226].

8.6. Proxy Authen Type AVP Values

The Proxy Authen Type AVP (Attribute Type 29) has an associated value maintained by IANA. Values 0-5 are currently defined, the remaining values are available for assignment upon Expert Review [RFC5226].

9. Security Considerations

PPP over L2TPv3 is subject to the security considerations defined in

[RFC3931]. Specifically, Control Connection Endpoint and Message Security mechanisms are provided in Section 4.3 and Section 5.4.1 of [RFC3931]. Data Packet Level Security is described in Section 8.2 of [RFC3931]. When running over L2TP-over-IP or L2TP-over-UDP/IP, IPsec can provide packet-level security via ESP and/or AH, as described in Section 4.1.3 of [RFC3931]. Additional security considerations specific to carrying PPP frames over L2TPv3 are described in the following section.

9.1. Proxy PPP Authentication

L2TP defines Proxy LCP and Authentication AVPs that MAY be exchanged during session establishment to provide forwarding of PPP LCP and authentication information obtained at the LAC to the LNS for validation (see Section 5.1.3). This authentication information may be used to initiate the PPP authentication states on the LNS, allowing PPP to continue without renegotiation. This implies a direct trust relationship of the LAC on behalf of the LNS. If the LAC is not trusted, the LNS policy may mandate to enter an additional round of LCP negotiation and/or authentication. Therefore, if the LNS chooses to implement proxy authentication, it MUST be able to be turned off by configuration, requiring a new round of PPP authentication initiated by the LNS (which may or may not include a new round of LCP negotiation).

10. References

10.1. Normative References

[ITU.Q931.1998] "Digital Subscriber Signalling System No. 1 (DSS 1) - ISDN User - Network Interface Layer 3 Specification for Basic Call Control", ISO Standard 9594-1, May 1998.

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

[RFC1662] Simpson, W., "PPP in HDLC-like Framing", STD 51, RFC 1662, July 1994.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

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

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn,

G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC3301] T'Joens, Y., Crivellari, P., and B. Sales, "Layer Two Tunnelling Protocol (L2TP): ATM access network extensions", RFC 3301, June 2002.

[RFC3437] Palter, W. and W. Townsley, "Layer-Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation", RFC 3437, December 2002.

[RFC3931] Lau, J., Townsley, M., and I. Goyret, "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, March 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

10.2. Informative References

[IANA.l2tp-parameters]
Internet Assigned Numbers Authority, "Layer Two Tunneling Protocol "L2TP"", April 2007, <http://www.iana.org/assignments/l2tp-parameters>.

[RFC1144] Jacobson, V., "Compressing TCP/IP headers for low-speed serial links", RFC 1144, February 1990.

[RFC1663] Rand, D., "PPP Reliable Transmission", RFC 1663, July 1994.

[RFC2341] Valencia, A., Littlewood, M., and T. Kolar, "Cisco Layer Two Forwarding (Protocol) "L2F"", RFC 2341, May 1998.

[RFC2637] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol", RFC 2637, July 1999.

[RFC3438] Townsley, W., "Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers Authority (IANA) Considerations Update", BCP 68, RFC 3438, December 2002.

[RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

Appendix A. Revision History

[Note to RFC Editor: please remove this entire appendix, and the corresponding entries in the table of contents, prior to publication.]

Changes between -07 and -08:

- Added section elements to all the AVPs in Section 5, and include them in the TOC. Updated citations to all these subsections.
- Multiple editorial fixes and enhancements from Alfred Hoenes.
- Miscelaneous updates in the Called/Calling Number/Sub-Address and Private Group ID from Ignacio Goyret.
- IANA instructions to rename the Sub-Address AVP to "Called Sub-Address AVP".
- Updated reference from RFC2434 to [RFC5226].

Changes between -06 and -07:

- Refresh document about to expire, no content changes.

Changes between -05 and -06:

- Added an Offset Capability AVP at tunnel establishment, to allow an LCCE advertise the maximum Offset Padding size that it is willing to insert if requested. This is described in Section 4.2 and Section 5.1.1.3.
- Small clarifications regarding the Offset Size on Section 4 and Section 5.1.2.9.
- Clarified handing of the ACF in Section 4.3, which resulted in normatively referencing [RFC3437].
- Added reference and corresponding citation to IANA's l2tp-parameters.

Changes between -04 and -05:

- Refresh revision, only rev++, date and boiler changes from new xml2rfc.tcl version.

Changes between -03 and -04:

- Fixed assorted editorial and typographical errors.
- Moved Section 1.2 and Section 1.3, new acronym in Section 1.1.
- Added a final sentence in Section 2.
- Added clarification regarding the presence of the Rx Minimum| Maximum|Connect Speed AVPs.
- Change in Section 8.2 and Section 8.2 to match IANA's page format.
- Source changes for strict XML.

Changes between -02 and -03:

- Fixed PPP acronym in the Abstract.
- Added PPP Circuit Errors AVP in Section 5.1.4.1 with the two PPP-specific fields removed from the Circuit Errors AVP 34 in [RFC3931].
- Redraw ACCM AVP figure in Section 5.1.4.2 and added Reserved field explanation.

Changes between -01 and -02:

- Updated title and title abbrev to reflect L2TPv3.
- Updated abstract, introduction and topology sections.
- Added contributing authors and editors.
- Added Section 3.1 and Section 3.2, turned Section 3 into Section 3.3. Added the "PPP PW Type" in Section 3.1.
- Added Figure 1 in Section 4.
- Decoupled the L2-Specific Sublayer from the Offset Padding in Section 4.1, and added new Offset Padding in Section 4.2.
- Removed the HDLC Address and Control fields from the encapsulation in Section 4.3.
- Changed Section 5.1.2 and Section 5.1.4 title, substituting Call for Session.
- Updated Bearer Capabilities AVP in Section 5.1.1.2 and Bearer Type AVP in Section 5.1.2.1 with the existing bit B (broadband access)

in bit 30 and moved bit V (virtual access) to bit 29.

- Substituted ICRQ for ICCN in the Framing Type AVP description in Section 5.1.2.2.

- Added a note for Called Number AVP, Calling Number AVP and Sub-Address AVP to interpret the encoding in the context of the Bearer Type in use for the specific call in Section 5.1.2.

- Added Calling Sub-Address AVP (ICRQ) Type 44 in Section 5.1.2.6.

- Added a note to the Q.931 Cause Code AVP to interpret the Cause Code relative to the Bearer Type in Section 5.1.2.7.

- Replaced Sequencing Required AVP Type 39 in Section 5.2.1.1 with the Data Sequencing AVP Type 70 defined in [RFC3931], and moved it to Section 5.2.1.1.

- Added Private Group ID AVP existing in [RFC2661] to Section 5.1.2.8.

- Added new Offset Size AVP in Section 5.1.2.9.

- Listed only currently assigned enumerations of "Defined Authen Type values" for Proxy Authen Type AVP in Section 5.1.3.4 and Section 8.6, and pointed to Section 8.6.

- Added Circuit Status AVP usage in Section 5.2.1.2, Section 3.2 and Section 3.3.

- Added short reference in Section 5.2.1.3 and Section 5.2.1.4 to 8-octet Tx/Rx Connect Speed AVPs, Type 74 and 75 defined in [RFC3931], instead of 4-octet Types 24 and 38.

- Moved Minimum BPS and Maximum BPS from Section 5.2 to Section 5.1.2 because not defined in [RFC3931], and changed them to new 8-octet value AVPs renaming them to Tx Minimum Speed and Tx Maximum Speed respectively in Section 5.1.2 and Section 8.1.

- Added 8-octet Rx Minimum Speed and Rx Maximum Speed in Section 5.1.2 and Section 8.1.

- Added general sequencing procedures note from [RFC3931] in Section 6 as well as updated Section 6.1 with 24-bit Sequence Number and usage of Data Sequencing AVP.

- Added small paragraph to the IANA Considerations generic section about existing vs. new registries.

- Added Section 8.2 and Section 8.3 with IANA Considerations for Pseudowire Type and Result Code AVP Values.

- Regrouped, updated and added the new value from -01 in IANA Considerations Section 8.4 (Bearer Capabilities and Bearer Type) and Section 8.5 (Framing Capabilities and Framing Type).

- Added Security Considerations Section.

- Updated References and split them into Normative and Informative.

Author's Address

Carlos Pignataro (editor)
Cisco Systems, Inc.
7200 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709
USA

Email: cpignata@cisco.com

Full Copyright Statement

Intellectual Property