Network Working Group
Internet-Draft
Category: Standards Track
<draft-ietf-l2tpext-sesinfo-04.txt>

William Palter
Pipal Systems
W. Mark Townsley
cisco Systems
Ignacio Goyret
Lucent Technologies
Suhail Nanji
Redback Networks
February 2002

L2TP Session Information "sesinfo"

Status of this Memo

Copyright Notice

Abstract

This document defines additional L2TP AVPs that may be used during session or control connection establishment to provide additional node and port information for accounting and debugging use.

Contents

1. Introduction

By design, an L2TP LNS is insulated from many of the details of the interface on which the session arrives before being tunneled. This abstraction is further mitigated when an L2TP session is directed to an additional tunnel via an L2TP Tunnel Switching (a.k.a. "Multihop") node. While not necessary for the proper operation of the tunneled session itself, it may be desirable for L2TP node identity, LAC media, and port information to be provided in a descriptive format for accounting or debugging use.

It should be noted that the Framing Type and Bearer Type AVPs defined in [RFC2661] are designed simply to allow the LNS to tailor the PPP options it uses for the media the session is running over. They are not intended to fully describe the originating port type or LAC. Further, at the time this document is being written, there there is no standardized mechanism for keeping this information intact as a session traverses L2TP tunnel switching nodes. None of the AVPs described in this document should have any effect on either the functioning of the tunnel or the parameters used in negotiating PPP parameters. They should only be used for logging, session limiting, accounting, and/or debugging purposes.

2. AVPs

Each of the following AVPs are defined in a list format which is designed to allow propogation of information forward by receiving and appending values to each AVP list when passing through an L2TP tunnel switching node or LAC. Values in each list AVP are correlated based upon their actual position in the list, thus care must be taken that entries remain balanced properly for all lists propogated. In the event that a value is unknown for a given list, a suitable "default"

or "unknown" value (defined within the context of each AVP) MUST be inserted in any list AVPs before propogating.

Each list entry is appended such that the last entry corresponds to the most recent sending node, and all preceding values are for "downstream" L2TP nodes. It is possible that all L2TP nodes did not participate in the Session Information extensions, in which case the entire list of L2TP nodes may not be accurately reflected at the final location.

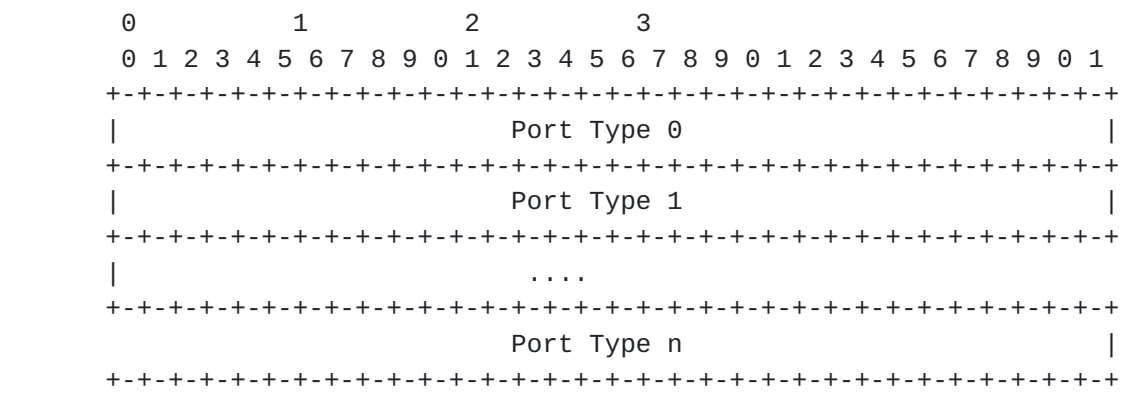
It is permissible, though not recommended, to implement only a portion of the AVP Lists defined in this document. However, if any of the AVPs defined in this document are implemented, the Port Type List MUST be among them. The Port Type List is the basis for correlating values in all other lists defined in this document.

For example, if the Port Type List AVP (section 2.1) contained a single entry, and no other AVPs defined in this document are sent, this would be valid for a typical LAC aiming to implement the minimum requirements of this document. A more sophisticated L2TP tunnel switching node may then use the information in the single Port Type List AVP and entry, together with information from other sources (such as other AVPs defined outside this document), to populate the remaining AVP lists defined here. More specific information on this is decribed in the individual AVP definitions throughout this document.

2.1 Port Type List (icrq, iccn)

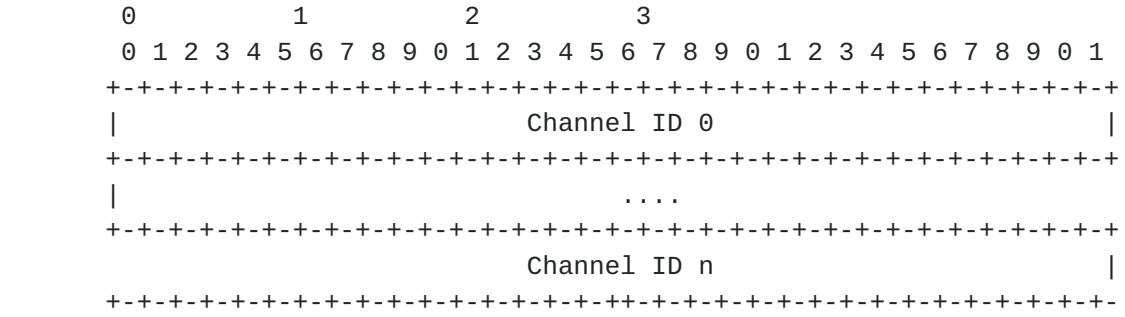
The Port Type List AVP is encoded as IETF Vendor ID 0, attribute TBD. The Value is a list of Port Types, using the same values that are used in RADIUS [RFC2058][RFC2059]. Each time an L2TP node forwards a session, a new value MUST be appended to this list before it is propogated.

Note that the last port type (or first if there is only one value in the list) always represents the port type of the sender of the control message containing this AVP.



2.2 Channel ID List (icrq, iccn)

The Channel ID List AVP is encoded as the IETF Vendor ID 0, Attribute TBD. The Value is a list of four octet values, representing the Channel ID of each node that the session has passed through. Each time an L2TP node forwards a session, a new value MUST be appended to this list before it is propogated. If there is no appropriate value, the reserved value 0 MUST be appended as a place holder.

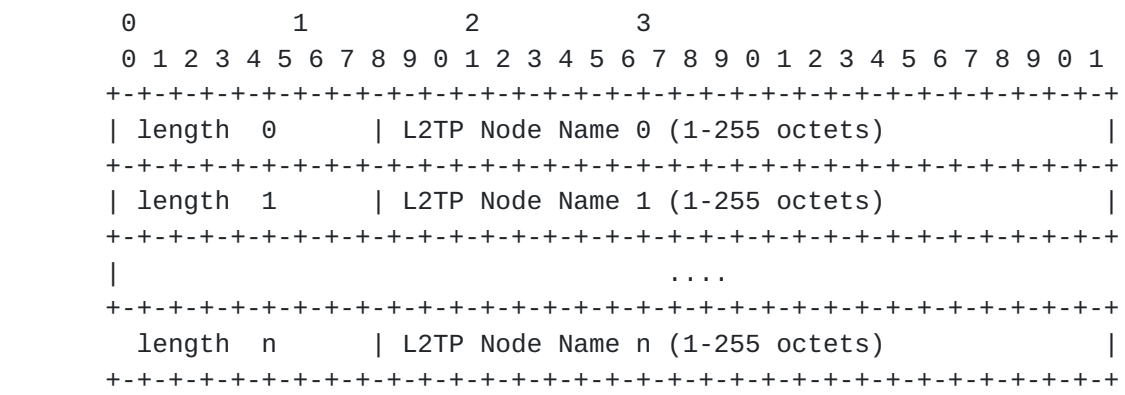


This AVP is analogous to the Physical Channel ID AVP defined in [RFC2661], except that it is allowed to grow as a list. As with the Port Type List, the last item in the list always represents the Channel ID of the sender of this AVP. Thus, the last value in the list should be identical to the Physical Channel ID AVP at any given node.

In the event a tunnel switching node has implemented the extensions defined in this document but does not receive a Channel ID List from its downstream node, it MUST first copy the value received in the Physical Channel ID AVP at Session establishment into the Channel ID List before adding its own Channel ID to the list.

2.3 L2TP Node Name List (sccrq, icrq, iccn)

The LAC Name List AVP is encoded as Vendor ID 0, Attribute TBD. The Value is a list of counted strings, with the octet prior to each string indicating the length of the string that follows it. Each time an L2TP node forwards a session, a new value MUST be appended to this list before it is propogated. If there is no appropriate value, then a length of 0 MUST be inserted for the L2TP Node Name Length as a place holder. The L2TP Node Name should be a human readable value, analogous or equivalent to the value sent the the L2TP Hostname AVP defined in [RFC2661]. Human readable text in all messages MUST be provided in the UTF-8 charset using the Default Language [RFC2277].



This AVP is analogous to the Hostname AVP defined in [RFC2661], except that it is allowed to grow as a list, and may be present at session as well as control connection startup. The last item in the list always represents the name of the sender of the message containing this AVP. Thus, the last value MAY be identical to that in the Hostname AVP.

In the event a tunnel switching node has implemented the extensions defined in this document but does not receive a LAC Node Name List from its downstream node, it MUST first copy the value received in the Hostname AVP at Control Connection establishment into the LAC Node Name List before adding its own LAC Node Name to the list.

4. IANA Considerations

This document requires three new "AVP Attributes" to be assigned through IETF Consensus [RFC2434] as indicated in Section 10.1 of [RFC2661]. These are:

Port Type List (section 2.1)

Channel ID List (section 2.2)

L2TP Node Name List (section 2.3)

This document defines no additional number spaces for IANA to manage.

5. Security Considerations

This document describes a method for propogating additional information about interfaces and equipment information by which a PPP session arrives before and after tunneling via L2TP. While it is not obvious how this information could be used for malicious purposes, if it somehow was used to comprimise security then implementation of the mechanisms described in this document increase the number of times this information is made available on the network. AVP hiding, described in [RFC2661] MAY be used to help mitigate this, though it is not widely regarded as cryptographically secure. [RFC3193] describes a more robust method for securing L2TP in general, and should be used to encrypt all L2TP messages if access to the information sent within the AVPs described in this document is of concern.

6. Contacts

Ignacio Goyret
Lucent Technologies
1701 Harbor Bay Parkway
Alameda, CA 94502
igoyret@lucent.com

William Palter
Pipal Systems
palter.ietf@zev.net

W. Mark Townsley
cisco Systems
7025 Kit Creek Road
PO Box 14987
Research Triangle Park, NC 27709
mark@townsley.net

Suhail Nanji
RedBack Networks
1389 Moffett Park Drive
Sunnyvale, CA 94089
suhail@redback.com

7. References

[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.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434,

[RFC2058] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)," RFC 2058, January 1997

[RFC2059] C. Rigney, RADIUS Accounting, RFC 2059, January 1997

[RFC3193] B. Patel, B. Aboba, W. Dixon, G. Zorn, S. Booth, "Securing L2TP Using IPsec," RFC 3193, November 2001