Network Working Group
Request for Comments: 3145
Category: Standards Track

R. Verma
Deloitte Consulting
M. Verma
3Com Corporation
J. Carlson
Sun Microsystems

July 2001

L2TP Disconnect Cause Information

Status of this Memo

Copyright Notice

Abstract

This document provides an extension to the Layer 2 Tunneling Protocol ("L2TP"), a mechanism for tunneling Point-to-Point Protocol (PPP) sessions. L2TP lacks a mechanism for a host to provide PPP-related disconnect cause information to another host. This information, provided by the extension described in this document, can be useful for accounting and debugging purposes.

1. Introduction

L2TP [1] defines a general-purpose mechanism for tunneling PPP over various media. By design, it insulates L2TP operation from the details of the PPP session that is being encapsulated by L2TP. There are, however, cases where it may be desirable for PPP-specific disconnect information to be provided to an L2TP host (L2TP Access Concentrator [LAC] or L2TP Network Server [LNS]) in a descriptive format. The lack of this information is especially a problem when the LAC and LNS are not owned or managed by the same entities.

The Result and Error Codes defined for L2TP specify only L2TP-specific disconnect information. This document provides an additional Attribute Value Pair (AVP), called PPP Disconnect Cause Code, that MAY be used by an L2TP host to provide PPP-specific

disconnect information to its peer. This AVP should be used in conjunction with, and not as a replacement for, the L2TP Result and Error Code AVPs.

The PPP Disconnect Cause Code AVP can also be used to provide a human-readable disconnect reason to the user. This AVP should not have any effect on either the functioning of the tunnel or the functioning of the PPP session; it is for informational and logging purposes only.

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 BCP 14 [2].

2. PPP Disconnect Cause Code AVP

The AVP is valid in the L2TP Call-Disconnect-Notify (CDN) message only, and it MUST NOT be marked Mandatory.

The PPP Disconnect Cause Code AVP is encoded with Vendor ID 0 and an Attribute Type of PPP Disconnect Cause Code (46). The length of the Value field MUST be at least 11 octets. If the length is more than 11 octets, the additional octets MUST contain a descriptive text in UTF-8 [3] format that can be displayed to the user or in a log file. The format of the AVP is shown below.

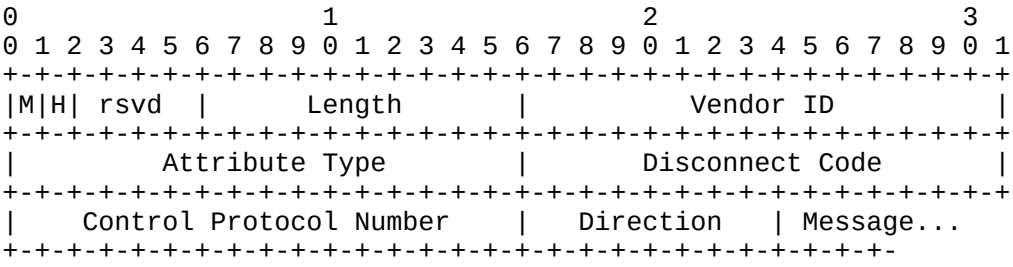

Figure 1: PPP Disconnect Cause Code AVP

Mandatory (M) bit: MUST be 0.

Hidden (H) bit: MAY be 1 if the attribute is hidden.

Length: The length of the entire attribute in octets, expressed as a single octet. The length MUST be at least 11.

Vendor ID: A two octet value in network byte order; set to 0 to indicate that this is an IETF-assigned attribute.

Attribute Type: A two octet value in network byte order; set to 46 (PPP Disconnect Cause Code).

Disconnect Code: A two octet value in network byte order. (Described in section 3 of this document.)

Control Protocol Number: The PPP Control Protocol number of the primary protocol known to have caused the error, if any. This field may be 0 unless mentioned otherwise in the description of the Disconnect Codes in section 3.

Direction: A single octet value; specifies the direction in which the Disconnect Code applies.

The valid values of this field are:

0: global error
1: at peer
2: at local
3-255: Reserved

This field SHOULD be 0 unless documented otherwise in the description of the specific Disconnect Code.

3. Disconnect Codes

This section contains the list of well-known values of the Disconnect Code field in the PPP Disconnect Cause Code AVP. The IANA will maintain a registry of the up-to-date values (see section 5 of this document). These values should be used in conjunction with the Direction value and the Control Protocol Number field to interpret the specific error condition.

Unless documented otherwise for a specific Disconnect Code, the Direction value SHOULD be 0.

3.1. Global Errors

The global error codes, given in the list below, are Disconnect Codes that do not relate to one particular PPP Control Protocol. The Control Protocol Number for these errors thus MUST be set to 0.

0 No information available.

1 Administrative disconnect.

2 Link Control Protocol (LCP) renegotiation at LNS disabled; LNS expects proxy LCP information, LAC did not send it.

3 Normal Disconnection, LCP Terminate-Request sent.

Valid Direction values are:

1: LCP Terminate-Request sent by peer
2: LCP Terminate-Request sent by local

4 Compulsory encryption required by a PPP peer was refused by the other.

Valid Direction values are:

1: Required by local; refused by peer
2: Required by peer; refused by local

3.2. LCP Errors

The LCP error codes, listed below, are disconnect reasons that are directly related to the failure of PPP peers to negotiate mutually agreeable link parameters. The Control Protocol Number for these errors MUST be set to C021 hexadecimal (LCP).

5 FSM (Finite State Machine) Timeout error. (PPP event "TO-".)

6 No recognizable LCP packets were received.

7 LCP failure: Magic Number error; link possibly looped back.

8 LCP link failure: Echo Request timeout.

9 Peer has unexpected Endpoint-Discriminator for existing Multilink PPP (MP) bundle.

10 Peer has unexpected MRRU for existing MP bundle.

11 Peer has unexpected Short-Sequence-Number option for existing MP bundle.

12 Compulsory call-back required by a PPP peer was refused by the other.

Valid Direction values are:

1: Required by local; refused by peer
2: Required by peer; refused by local

3.3. Authentication Errors

The authentication error codes, listed below, are disconnect reasons that are directly related to authentication failures between the PPP peers. The Control Protocol Number for such errors MUST correspond to the PPP Control Protocol number for the authentication protocol in use.

13 FSM Timeout error.

14 Peer has unexpected authenticated name for existing MP bundle.

15 PPP authentication failure: Authentication protocol unacceptable.

Valid Direction values are:

1: All local authentication protocols were rejected by the peer.

2: All authentication protocols requested by peer were unacceptable or unimplemented locally.

16 PPP authentication failure: Authentication failed (bad name, password, or secret).

Valid Direction values are:

1: Authentication of peer identity by local system.
2: Authentication of local identity by peer system.

3.4. Network Control Protocol (NCP) Errors

NCP Errors are disconnect reasons that are directly related to the failure of PPP peers to negotiate a mutually agreeable set of parameters for the network protocols. The Control Protocol Number for such errors SHOULD correspond to the PPP Network Control Protocol number in use. Where multiple network protocols are in use, multiple copies of this AVP MAY be given to indicate failure reasons for each NCP. Otherwise, if only one copy of the AVP is given, the Control Protocol Number SHOULD correspond to the last (most recent) failing NCP.

17 FSM Timeout error.

18 No NCPs available (all disabled or rejected); no NCPs went to Opened state. (Control Protocol Number may be zero only if neither peer has enabled NCPs.)

19 NCP failure: failed to converge on acceptable addresses.

Valid Direction values are:

1: Too many Configure-Naks received from peer.
2: Too many Configure-Naks sent to peer.

20 NCP failure: user not permitted to use any addresses.

Valid Direction values are:

1: Local link address not acceptable to peer.
2: Remote link address not acceptable to local system.

4. Notes

This AVP MAY may be sent by either the LNS or LAC. It is generally expected that this AVP will be most useful in sending notification from the LNS to LAC in the compulsory tunneling case, although it is not precluded from use in any other case.

A draft form of this AVP used Vendor ID 43 (3Com Corporation) and vendor-specific Attribute Type 46. Implementations MAY accept AVPs with these values as equivalent to the message described in this document, but SHOULD NOT transmit an AVP using these values.

5. Security Considerations

The integrity and confidentiality of this AVP relies on the underlying L2TP security mechanisms. It is intended for logging and diagnostic purposes in the event of PPP link failure and should not pose a threat to system security, but the AVP MAY be hidden as described in section 4.3 of RFC 2661.

The defined extension does not provide information that would be useful to an attacker. Future extensions should not be defined to lessen security. For instance, it is inappropriate to provide distinguishing information that would inform the peer that a given authentication name is correct, but the password/secret is incorrect.

6. IANA Considerations

IANA has assigned an L2TP Attribute Type value of 46 for the PPP Disconnect Cause Code defined in Section 2.

This AVP includes an enumerated cause code value, called the "Disconnect Code." Values 0 through 20 are described in this document. Values 21 through 32767 (inclusive) are assigned by the IANA subject to IESG Approval. Values 32768 through 65279 (inclusive) are assigned by the IANA on a First Come First Served basis, and are intended for vendor-specific features. Values 65280 through 65535 (inclusive) are allocated for Private or Experimental Use, and no assignment through the IANA is expected.

7. References

[1] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer 2 Tunnel Protocol (L2TP)", RFC 2661, August 1999.

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

[3] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

8. Acknowledgments

The authors thank W. Mark Townsley and Thomas Narten for their comments and help.

9. Contacts

9.1. L2TP Working Group Chair

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

EMail: townsley@cisco.com

9.2. Authors' Addresses

Rohit Verma
180 N. Stetson Avenue
Chicago IL 60601

Phone: +1 312 374 2475
Fax: +1 312 870 2475
EMail: rverma@dc.com

Madhvi Verma
3800 Golf Road
Rolling Meadows IL 60008

Phone: +1 847 262 2987
Fax: +1 847 262 2255
EMail: Madhvi_Verma@3com.com

James Carlson
Sun Microsystems
1 Network Drive MS UBUR02-212
Burlington MA 01803-2757

Phone: +1 781 442 2084
Fax: +1 781 442 1677
EMail: james.d.carlson@sun.com

10. Standard Notices

10.1. IETF Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP 11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights, which may cover technology that, may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Acknowledgement

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