Layer Two Tunneling Protocol "L2TP"
IP Differentiated Services Extension

Status of this Memo

This document is a submission by the L2TP Extensions Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the l2tp@ipsec.org mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:

http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at:


Abstract

The L2TP document [1] defines the base protocol which describes the method of tunneling PPP data. The L2TP base protocol does not address any Differentiated Services extensions.

The ability to outsource dial access with Quality of Service assurances is important to internet applications development. This
draft addresses this issue by allowing each L2TP Data Session to be assigned an appropriate differentiated services indicator.

Table of Contents

1.0 Introduction
  1.1 Conventions

2.0 Differentiated Services Negotiation
  2.1 Differentiated Services Code Point Exchange
  2.2 Error Reporting

3.0 References

4.0 Acknowledgements

5.0 Authors’ Addresses

1.0 Introduction

The L2TP protocol specification does not discuss Quality of Service/Differentiated Services in any way.

This document will describe how two L2TP peers negotiate a differentiated services (Diff Serv) indicator for a dial-in user. Note that each individual session within a tunnel can have its own Diff Serv Indicator.

The mechanism defined in this document assumes that the Tunnel Initiator determines what the user’s appropriate service type is and sends the value in either the ICRQ or OCRQ messages. The Tunnel Terminator can respond to the message by stating what it believes is the user’s appropriate service type. The values of the indicator supplied by the Tunnel Terminator will supersede those provided by the Tunnel Initiator if a difference is found.

In the case where the Tunnel Terminator does not propose ANY indicator (which is inferred by the absence of the QOS AVPs in either the ICRP or OCRP) the Tunnel Initiator will assume no QoS is assigned to the session.

1.1 Conventions

The following language conventions are used in the items of specification in this document:

  o  MUST, SHALL, or MANDATORY -- This item is an absolute requirement of the specification.

  o  SHOULD or RECOMMEND -- This item should generally be followed
o MAY or OPTIONAL -- This item is truly optional and may be followed or ignored according to the needs of the implementor.

2.0 Differentiated Services Negotiation

This section will define the new AVPs which are required for the Quality of Service extension of the L2TP protocol. The AVPs allow designation of a Quality of Service type for a specific data channel.

2.1 Differentiated Services Code Point AVP

The Differentiated Services Code Point (DSCP) occupies either the IPv4 header’s TOS octet[2] or the IPv6 Traffic Class octet[2]. The actual bit interpretation of the IP Precedence and Type of Service bit fields is left to the appropriate documentation[2][3][4]. This document is concerned only with defining a uniform exchange mechanism for the DSCP AVP.

The DSCP AVP MAY be present in ICRQ, ICRP, OCRQ and OCRP. This message is used to inform the tunnel peer that a DSCP value SHOULD be used for all packets related to the data channel associated with the Tunnel and Call Identifiers in the L2TP header [1].

The presence of this AVP in the ICRQ or OCRQ indicates that the tunnel initiator wishes to use a specific DSCP on all data packets. However, the value found in the ICRP or OCRP indicate the value which the Tunnel Terminator is willing to accept.

A tunnel peer which exceeds the negotiated DSCP, depending upon the SLS, MAY have it’s tunnel shutdown.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|1|0|0|        Length         |              43               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                1              |        DSCP  Value            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

This AVP MAY be present in the messages shown above. It is encoded with a Vendor ID of 43 (3Com Corporation) with the attribute set to 1, marked as optional, with the indicator value as data. This AVP SHOULD NOT be hidden and is optional. When present, the L2TP peer is indicating that the specified DSCP is to be used on IP
packets within the session’s data channel.

2.2 Error Reporting

In the event that the peer did not accept the DSCP provided, or is unable to support the DSCP, a Call-Disconnect-Notify is returned to the peer.

If the DSCP provided cannot be used by the peer, the Call-Disconnect-Notify message will include the DSCP AVP as provided in the message that caused the Call-Disconnect-Notify.

3.0 References


4.0 Acknowledgements

The Authors would like to acknowledge John Shriver for his useful comments to an earlier version of this document.

5.0 Authors’ Addresses

Questions about this memo can be directed to:

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, California, 94025
USA

Phone: 1-650-786-7733