PPP Working Group
INTERNET DRAFT
Category: Internet Draft
Title: draft-ietf-pppext-l2tpdwin-01.txt
Date: November 1998

Richard Shea
Nortel Networks

L2TP Dynamic Data Window Adjustment

Status of this Memo

Abstract

The Layer Two Tunneling Protocol (L2TP) defines the specification of congestion window sizes for data sessions. In addition, an LNS is given the capability to turn off sequence number processing for a data session, provided the LAC did not include the Sequencing Required AVP during session setup. This document specifies a mechanism whereby an L2TP peer can dynamically change the maximum window size values being used for a data session, in order to provide the flexibility to operate with smaller window sizes when history-bound protocols are operating over a session, and larger window sizes when no history-bound protocols are operating over a session.

1. Introduction

In the L2TP protocol sequence numbers are used for preserving packet order, detecting packet loss, rate pacing, and congestion

control. An effective window size value for congestion control is influenced in opposite directions by two things. First, in the case where protocols with history are being carried, the window size must be small enough so that forced packet loss is not excessive in the case of a real packet drop where resynchronization is necessary. At the same time, the larger the delay between the LAC and LNS, the larger the window size should be so that the available bandwidth between the LAC and LNS is not underutilized due to rate pacing and congestion control.

Unfortunately, the L2TP protocol specifies that the window sizes for a session are determined when the session is established, at a time before it is known whether or not protocol with history will be operating over the session.

It is important for L2TP to provide the flexibility to maximize performance for the cases where history-bound protocols are operating over a data session for a tunnel which is operating over a lossy network and where no history-bound protocols are operating over a data session being tunneled over a high-delay path. Because the knowledge of whether history-bound protocols will be operating over a data session is not known at the time of session setup, a mechanism for dynamically updating the data session window sizes is needed.

It is also not possible in all cases for the LAC to detect when a history-bound protocol is being used or not. A mechanism is also included so the LNS can inform the LAC as to whether or not history-bound protocols are being run over the link.

1.1 Conventions

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

- MUST, SHALL, or MANDATORY -- This item is an absolute requirement of the specification.
- SHOULD or RECOMMEND -- This item should generally be followed for all but exceptional circumstances.
- MAY or OPTIONAL -- This item is truly optional and may be followed or ignored according to the needs of the implementor.

1.2 Terminology

This draft assumes the reader is knowledgable about terms found in [1]. In addition, the following terms are used in this document:

History

Application information that is transferred between peers that spans the information conveyed in more than one datagram.

History-Bound Protocol

A protocol that uses a history during its operation. The canonical example of such protocols in the context of PPP is compression protocols. While compression protocols can be run in a mode where history is not kept between packets, there are some implementations that do not support such a mode; nor is such a mode always the most desirable mode of operation.

2. Protocol overview

The current practice for L2TP is for data session maximum window sizes to be indicated at the time of session setup, and for these maximum window sizes to remain the same for the life of the session.

This document describes an operational addition to L2TP to allow data session maximum window sizes to change during the life of a data session.

There are several factors that an implementation can use when deciding on a value for its maximum receive window size:

- Rate Pacing - Based on the access speed of the physical connection of the client to the LAC, the LAC may desire to rate pace the data to stay at the rate that the physical connection can handle.

- Congestion Control - Based on the load on the box or relative priority of the tunneled user identity.

- Operation of history-bound protocols on the link - In order to get reasonable performance on a link using history-bound protocols in the face of packet loss, the maximum window size should be kept small (4 packets or so).

Furthermore, the detection of whether or not a history-bound

protocol is running over the link is not always possible for an L2TP endpoint. Specifically, a LAC implementation generally does not (and perhaps for performance reasons should not) inspect PPP traffic being forwarded between the LNS and the client being

tunneled.

The additions to the protocol suggested here are therefore to:

1. Provide a method for the LNS to indicate to the LAC whether or not any history-bound protocols are operating over the link.

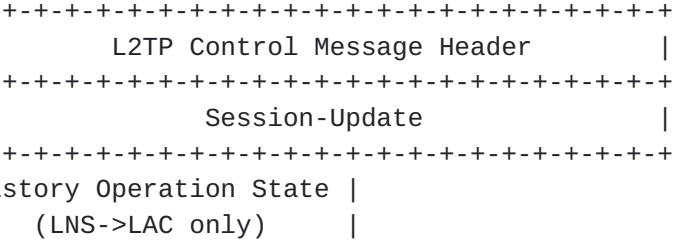
2. Provide a method for the LNS and LAC to communicate changes in their maximum receive window sizes to each other.

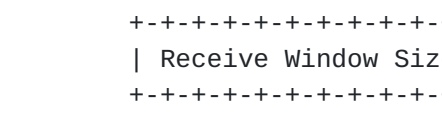
To provide both of these mechanisms a new message is specified. When this message is sent from the LNS to the LAC it includes the current state of history-bound protocol operation and a new maximum receive window size. When this new message is sent from the LAC to the LNS it includes a new maximum receive window size.

3. Protocol additions

This document specifies that the protocol be extended with a new message type: Session-Update (SU). This new message is used during the life of a session to communicate session update information for a data session.

This document further specifies two AVPs that can optionally be included in the SU message. For SU messages sent from the LNS to the LAC a new AVP indicating the current state of history protocol operation over the tunneled session can be included. Both the LNS and the LAC can send the SU with the Receive Window Size AVP included to change the maximum receive window size for the data session.

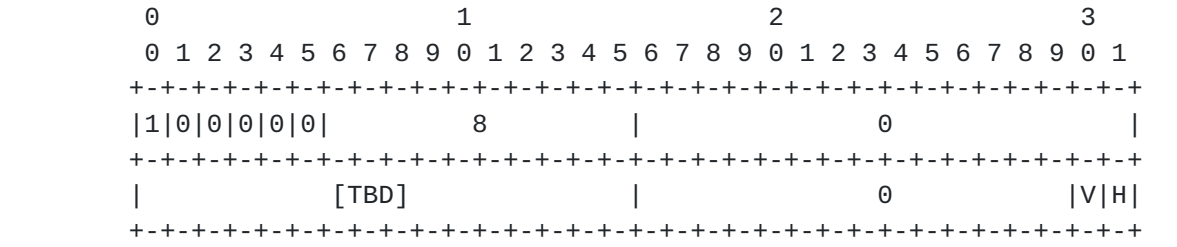




The format of the L2TP control message header is given in [1].

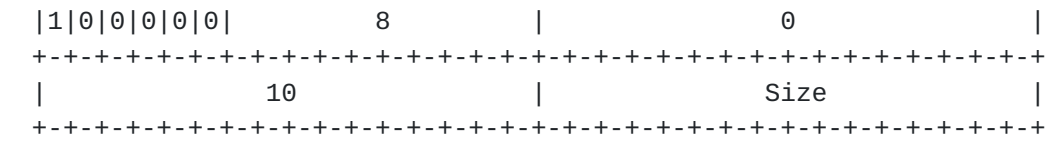
The Message Type AVP for this message contains the value [TBD] indicating that this message is a Session-Update message.

History Operation State



History Operation State encodes the state of history-bound protocol operation using two bits. The V (VJ) bit indicates whether or not VJ TCP/IP header compression [3] is operating over the link. If the V bit is one (1) this indicates that VJ packets are being sent over the tunneled data session be the LNS. This informs the LAC that upon detection of lost data packets, an indication should be sent over the physical connection to the client that a packet was lost (e.g. the LAC can force a CRC error on the physical connection to the client). If the V bit is zero (0) this indicates that VJ packets are not being sent over the tunneled data session by the LNS. The H (History) bit is set if any other history-bound protocol (other than VJ compression) is being run over the tunneled session. Attribute is [TBD], indicating History Operation Status, and is marked mandatory. This AVP MUST be present in an SU sent by the LNS. This AVP MUST NOT be present in an SU sent by the LAC.

Receive Window Size



Receive Window Size AVP encodes the window size being advertised for this call. Attribute is 10, indicating Receive Window Size, and is marked mandatory. This AVP itself is optional. The Size value indicates the number of received data packets the sender of the SU will buffer for this call, which is also the maximum number of data packets the receiver of the SU should send before waiting for an acknowledgment.

4. Protocol Operation

This extension MUST only be used if both L2TP peers have signaled support of this extension during tunnel establishment using the Extensions AVP defined in [4].

When a session is first started it is not known if a history-bound protocol will be negotiated. An implementation should therefore pick a maximum receive window size based on the assumption that a history-bound protocol will be negotiated. If the tunnel is operating over a reliable medium this is not a factor. If the tunnel is not operating over a reliable medium then an appropriately small window size should be chosen (recommend 4?).

When an LNS detects a change in the state of operation of history-bound protocols over the tunneled session it MUST send an SU to the LAC. This allows the LAC to make adjustments to its maximum receive window size, even if the LNS does not make a change itself.

Upon reception of the SU with Receive Window Size AVP, the receiver of the SU MUST begin operating under the rules for Receive Window Size AVP values received during data session setup.

If the value of the Receive Window Size AVP in the SU is greater than the value of the last Receive Window Size AVP received, there is no further action required by the receiver of the SU other than changing its maximum send window accordingly.

If the value of the Receive Window Size AVP in the SU is less than

the value of the last Receive Window Size AVP received, then the receveiver of the SU must take special action. In this case, the receiver of the SU must change its maximum send window accordingly, consider any currently unacknowledged packets as acknowledged, and send an R Bit in the next data packet sent to the peer. This prevents the data session from unnecessarily hanging when the window size is adjusted down.

If for a particular data session a peer does not send the Receive Window AVP during session establishment, the Receive Window AVP MUST NOT be sent in a subsequent SU message.

5. Security Considerations

Security is not addressed in this document.

References

[1] A. Valencia, et al, "Layer Two Tunneling Protocol", Work In Progress: draft-ietf-pppext-l2tp-12.txt, October 1998

[2] D. Rand, "PPP Reliable Transmission". RFC 1663

[3] V. Jacobson, "Compressing TCP/IP Headers for Low-Speed Serial Links", RFC 1144, February 1990

[4] R. Shea, "Framework for L2TP Message Extensions", Work In Progress: draft-ietf-pppext-l2tpmsgext-00.txt, November 1998

Author's Address

Richard Shea
Nortel Networks
125 Nagog Park
Acton, Massachusetts 01720
rshea@BayNetworks.com