Layer Two Tunneling Protocol - Setup of TDM Pseudowires

Abstract

This document defines extensions to the Layer Two Tunneling Protocol (L2TP) for support of structure-agnostic [RFC4553] and structure-aware [PWE3-CESoPSN] pseudowires.

Conventions used in this document

In this document we refer to control plane as the packets that contain control information (via AVP) and the mechanism that handle these packets.

In this document we refer to the data plane as the packets that contain transported user data.
Table of Contents

1. Introduction.......................................................2
2. L2TP Extension......................................................2
   2.1 TDM PW AVP  (ICRQ, OCRQ).....................................3
   2.2 RTP AVP  (ICRQ, OCRQ, ICRP, OCRP)..........................4
   2.3 Changes in the Control Connection AVPs.....................5
   2.4 Changes in the Session Connection AVPs...................5
3. Creation of the TDM Pseudowire Session.........................5
4. IANA Considerations..............................................6

Security Considerations............................................7
Copyright notice....................................................7
Normative references...............................................8
Informative references.............................................8
Authors’ Addresses..................................................8

1. Introduction

This document defines extensions to the Layer Two Tunneling Protocol (L2TP) for support of structure-agnostic [RFC4553] and structure-aware [PWE3-CESoPSN] pseudowires. Setup of structure-aware pseudowires using encapsulations described in [PWE3-TDMoIP] has been left for further study.

2. L2TP Extension

The L2TP Control Connection is responsible for 3 main operations:
1. Establishment and validation of session.
2. Ending (tearing down) of session.
3. Transferring of End Point status.

Tearing down of session is identical to [RFC3931].

[PWE3-CESoPSN] and [RFC4553] describe how to transfer the End Point status via the data plane. This is therefore RECOMMENDED to not use the Set-Link-Info (SLI) described in [RFC3931].

The next sections describe the extensions to the L2TP for establishment and validation of TDM pseudowire sessions.

There are 2 new AVPs for the Session Connection Messages. One AVP describe the TDM pseudowire attributes. The second AVP describe the RTP attributes for this TDM pseudowire.
2.1 TDM PW AVP (ICRQ, OCRQ)

This AVP MAY be hidden (the H bit MAY be 0 or 1). The M bit for this AVP SHOULD be set to 0. The Length (before hiding) of this AVP is 12.

Bit Rate is defined in [RFC4446]. Its usage for all types of TDM PWs implies the following semantics:

1) Only the following values MUST be specified for structure-agnostic emulation (see [RFC4553]):
   a) Structure-agnostic E1 emulation - 32
   b) Structure-agnostic T1 emulation:
      i) MUST be set to 24 for the basic mode
      ii) MUST be set to 25 for the "Octet-aligned T1" mode
   c) Structure-agnostic E3 emulation - 535
   d) Structure-agnostic T3 emulation - 699

2) For all kinds of structure-aware emulation, this parameter MUST be set to the number of DS0 channels in the corresponding attachment circuit.

Note: for structure-agnostic T1 emulation the value 24 does not indicate the exact bit rate, and is used for convenience only.

CEP/TDM Payload Bytes has been defined in [RFC4446]. It can be used for setup of all types of TDM PWs without any changes in its encoding (see [RFC4446]) with the following semantics:

1) For Structure-agnostic emulation any value of the payload bytes can be specified.

2) For CESoPSN PWs:
   a) The specified value MUST be an integer multiple of number of DS0 channels in the corresponding attachment circuit.
   b) For trunk-specific NxDS0 with CAS, (Payload Bytes/number of DS0 channels) must be an integer factor of the number of frames per corresponding trunk multiframe.

The Reserved bits are reserved. They MUST be set to 0 on transmission and MUST be ignored on reception.
CAS bits define the trunk type for trunk-specific CESoPSN services with CAS. These bits:

1) MUST be set to 0 for all pseudowire types excluding trunk-specific CESoPSN with CAS.

2) For trunk-specific CESoPSN with CAS these bits must be set to:
   a) '01' in the case of an E1 trunk
   b) '10' in the case of a T1/ESF trunk
   c) '11' in the case of a T1/SF trunk.

2.2 RTP AVP (ICRQ, OCRQ, ICRP, OCRP)

This AVP MUST appear if and only if the RTP header is used in the TDM pseudowire encapsulation. This AVP MAY be hidden (the H bit MAY be 0 or 1). The M bit for this AVP SHOULD be set to 0. The Length (before hiding) of this AVP is 16.

The D bit indicates the timestamping mode (absolute or differential) in the RTP header. These modes are described in, e.g., [RFC4553], Section 4.3.2. If the D bit is set to 1 then the differential timestamping mode is used, otherwise absolute timestamping mode is used. Differential mode can be used only if both sides use RTP and use differential time stamping.

The C bit indicates the ordering of the RTP header and the control word as following:

- If the C bit is set to 1 the RTP header appears after the control word in the data channel of the TDM pseudowire. This mode is described as SAToP/CESoPSN encapsulation over IPv4/IPv6 PSN with L2TPv3 demultiplexing in [RFC4553] and [PWE3-CESoPSN] respectively.
- If the C bit is set to 0 the RTP header appears before the control word. This mode is described as the old mode of the SAToP/CESoPSN encapsulation over L2TPv3 in [RFC4553], Appendix A, and [PWE3-CESoPSN], Annex C, respectively.
PT is the payload type expected in the RTP header. Value of zero indicates that the payload type is ignored and will not be used to detect malformed packets. Timestamp Clock Frequency is the clock frequency used for the time stamping in 8 KHz.

SSRC indicates the expected value of SSRC ID in the RTP header. A zero in this field means that SSRC ID will not be used for detecting misconnections. Since L2TP provides an alternative security mechanism via the cookies, if the cookie length is larger then zero the SSRC SHOULD be zero.

### 2.3 Changes in the Control Connection AVPs

Control Connection that support TDM MUST add the appropriate PW Type value to the list in the Pseudowire Capabilities List AVP. The exact value is TBA by IANA and is listed in the next section.

#### 2.4 Changes in the Session Connection AVPs

PW Type AVP should be set to one of the following values:

1. Structure-agnostic emulation [RFC4553] of:
   a. E1 circuits - TBA-SAToP-E1 by IANA. The value 0x0011 is suggested for alignment with [RFC4446]
   b. T1 circuits - TBA-SAToP-T1 by IANA. The value 0x0012 is suggested for alignment with [RFC4446]
   c. E3 circuits - TBA-SAToP-E3 by IANA. The value 0x0013 is suggested for alignment with [RFC4446]
   d. T3 circuits - TBA-SAToP-T3 by IANA. The value 0x0014 is suggested for alignment with [RFC4446]

2. Structure-aware emulation [PWE3-CESoPSN] of:
   a. CESoPSN basic mode - TBA-CESoPSN-Basic by IANA. The value 0x0015 is suggested for alignment with [RFC4446]
   b. Trunk-specific CESoPSN service with CAS - TBA-CESoPSN-CAS by IANA. The value 0x0017 is suggested for alignment with [RFC4446].

TDM pseudowires use their own control word. Therefore the L2-Specific Sublayer AVP MUST either be omitted or set to zero.

TDM pseudowires use their own sequencing. Therefore the Data Sequencing AVP MUST either be omitted or set to zero.

### 3. Creation of the TDM Pseudowire Session

When LCCE wants to open a Session for TDM PW it MUST include the TDM PW AVP (in any case) and the RTP AVP (if RTP and only if the RTP header is used) in the ICRQ or OCRQ message. The LCCE peer must validate the TDM PW AVP and make sure it can meet the requirements.
derived from the RTP AVP (if it exist). If the peer agrees with the TDM AVP it will send an appropriate ICRP or OCRP message with the matching RTP AVP (if needed). The Initiator need to validate that it can supply the requirements derived from the received RTP AVP.

The two peers MUST agree on the values in the TDM PW AVP:

1. Bit Rate values MUST be equal on both sides. If they are different, the connection will be rejected with return code RC-TBD-1 and error code EC-TBD-1.
2. In the case of trunk-specific CESoPSN with CAS, the trunk type (as encoded in the CAS bits of the TDM AVP) MUST be the same for the two sides. Otherwise the connection will be rejected with return code RC-TBD-1 and error code EC-TBD-2.
3. If one side does not support the payload bytes value proposed by the other one, the connection will be rejected with return code RC-TBD-1 and error code EC-TBD-3.
4. If one side cannot send RTP header requested by the other side, the connection will be rejected with return code RC-TBD-1 and error code EC-TBD-4.
5. If one side can send RTP header but not with the requested timestamp clock frequency, the connection will be rejected with return code RC-TBD-1 and error code EC-TBD-5.

4. IANA Considerations

This draft requires assignment of the following values by IANA:

PW types listed in Section 2.1 above. It is RECOMMENDED to use the same values as defined in [RFC4446].

New attribute value pair IDs:

1. AVP-TBD-1 - TDM Pseudowire AVP
2. AVP-TBD-2 - RTP AVP

New return codes and error codes:

1. RC-TBD-1 - return code to indicate connection refused because of TDM PW parameters. The exact error code is as follows.
2. EC-TBD-1 - indicate Bit Rate values disagree.
3. EC-TBD-2 - indicate different trunk types in the case of trunk-specific CESoPSN with CAS
4. EC-TBD-3 - requested payload size too big or too small.
5. EC-TBD-4 - RTP header cannot be generated.
6. EC-TBD-5 - requested timestamp clock frequency cannot be generated.
Security Considerations

There are no additional security considerations on top of the ones discussed in [RFC3931]

Copyright notice

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IPR Validity Disclaimer

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.
Normative references

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


Informative references


Authors’ Addresses

Sharon Galtzur
Rawflow Inc.
The Old Pump House, 19 Hooper St.,
London E1 8BU,
UK
Email: sharon@rawflow.com

Alexander Vainshtein,
Axerra Networks,
24 Raoul Wallenberg St.,
Tel Aviv, Israel
Email: sasha@axerra.com