Internet Engineering Task Force (IETF)
Request for Comments: 7771
Updates: 6870
Category: Standards Track
ISSN: 2070-1721

A. Malis, Ed.
L. Andersson
Huawei Technologies Co., Ltd.
H. van Helvoort
Hai Gaoming BV
J. Shin
SK Telecom
L. Wang
China Mobile
A. D'Alessandro
Telecom Italia
January 2016

Switching Provider Edge (S-PE) Protection for MPLS and MPLS Transport Profile (MPLS-TP) Static Multi-Segment Pseudowires

Abstract

In MPLS and MPLS Transport Profile (MPLS-TP) environments, statically provisioned Single-Segment Pseudowires (SS-PWs) are protected against tunnel failure via MPLS-level and MPLS-TP-level tunnel protection. With statically provisioned Multi-Segment Pseudowires (MS-PWs), each segment of the MS-PW is likewise protected from tunnel failures via MPLS-level and MPLS-TP-level tunnel protection. However, static MS-PWs are not protected end-to-end against failure of one of the Switching Provider Edge Routers (S-PEs) along the path of the MS-PW. This document describes how to achieve this protection via redundant MS-PWs by updating the existing procedures in RFC 6870. It also contains an optional approach based on MPLS-TP Linear Protection.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7771.

Table of Contents

1. Introduction

In MPLS and MPLS Transport Profile (MPLS-TP) Packet Switched Networks (PSNs), pseudowires (PWs) are transported by MPLS(-TP) Label Switched Paths (LSPs), also known as tunnels.

As described in RFC 5659 [RFC5659], Multi-Segment Pseudowires (MS-PWs) consist of Terminating Provider Edge Routers PEs (T-PEs), one or more Switching Provider Edge Routers (S-PEs), and a sequence of tunneled PW segments that connects one of the T-PEs with its "adjacent" S-PE, connects this S-PE with the next S-PE in the sequence, and so on until the last S-PE is connected by the last PW segment to the remaining T-PE. In MPLS and MPLS-TP environments, statically provisioned Single-Segment Pseudowires (SS-PWs) are protected against tunnel failure via MPLS-level and MPLS-TP-level tunnel protection. With statically provisioned Multi-Segment

Pseudowires (MS-PWs), each PW segment of the MS-PW is likewise protected from tunnel failure via MPLS-level and MPLS-TP-level tunnel protection. However, tunnel protection does not protect static MS-PWs from failures of S-PEs along the path of the MS-PW.

RFC 6718 [RFC6718] provides a general framework for PW protection, and RFC 6870 [RFC6870], which is based upon that framework, describes protection procedures for MS-PWs that are dynamically signaled using LDP. This document describes how to achieve protection against S-PE failure in a static MS-PW by extending RFC 6870 to be applicable for statically provisioned MS-PWs pseudowires (PWs) as well.

This document also contains an OPTIONAL alternative approach based on MPLS-TP Linear Protection. This approach, described in Appendix A, MUST be identically provisioned in the PE endpoints for the protected MS-PW in order to be used. See Appendix A for further details on this alternative approach.

This document differs from [PW-REDUNDANCY] in that it provides end-to-end resiliency for static MS-PWs, whereas [PW-REDUNDANCY] provides resiliency at intermediate S-PEs and resiliency for both dynamically signaled and static MS-PWs.

PWs based on the Layer 2 Tunneling Protocol Version 3 (L2TPv3) are outside the scope of this document.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Extension to RFC 6870 to Protect Statically Provisioned SS-PWs and MS-PWs

Section 3.2.3 of RFC 6718 and Appendix A.5 of RFC 6870 document how to use redundant MS-PWs to protect an MS-PW against S-PE failure in the case of a singly homed Customer Edge (CE), using the following network model from RFC 6718:

```
       Native   |<----------- Pseudowires ----------->|  Native
       Service  |                                      |  Service
        (AC)    |     |<-PSN1-->|     |<-PSN2-->|     |  (AC)
          |     V     V         V     V         V     V   |
          |     +-----+         +-----+         +-----+   |
   +----+ |     |T-PE1|=========|S-PE1|=========|T-PE2|   |   +----+
   |    |-------|......PW1-Seg1.......|.PW1-Seg2......|-------|    |
   | CE1|       |     |=========|     |=========|     |       | CE2|
   |    |       +-----+         +-----+         +-----+       |    |
   +----+        |.||.|                          |.||.|       +----+
                 |.||.|         +-----+          |.||.|
                 |.||.|=========|     |========== .||.|
                 |.||...PW2-Seg1......|.PW2-Seg2...||.|
                 |.| ===========|S-PE2|============ |.|
                 |.|            +-----+            |.|
                 |.|============+-----+============= .|
                 |.....PW3-Seg1.|     | PW3-Seg2......|
                  ==============|S-PE3|===============
                                |     |
                                +-----+
```

Figure 1: Single-Homed CE with Redundant MS-PWs

In this figure, Customer Edge Router 1 (CE1) is connected to T-PE1, and CE2 is connected to T-PE2 via Attachment Circuits (ACs). There are three MS-PWs. PW1 is switched at S-PE1, PW2 is switched at S-PE2, and PW3 is switched at S-PE3. This scenario provides N:1 protection against S-PE failure for the subset of the path of the emulated service from T-PE1 to T-PE2.

The procedures in RFCs 6718 and 6870 rely on LDP-based PW status signaling to signal the state of the primary MS-PW that is being protected, and the precedence in which redundant MS-PW(s) should be used to protect the primary MS-PW should it fail. These procedures make use of information carried by the PW Status TLV, which, for dynamically signaled PWs, is carried by the LDP.

However, statically provisioned PWs (SS-PWs or MS-PWs) do not use the LDP for PW setup and signaling; rather, they are provisioned by network management systems or other means at each T-PE and S-PE along their paths. They also do not use the LDP for status signaling. Rather, they use procedures defined in RFC 6478 [RFC6478] for status signaling via the PW Operations, Administration, and Maintenance (OAM) message using the PW Associated Channel Header (ACH). The PW Status TLV carried via this status signaling is itself identical to the PW Status TLV carried via LDP-based status signaling, including the identical PW Status Codes.

Sections 6 and 7 of RFC 6870 describe the management of a primary PW and its secondary PW(s) to provide resiliency to the failure of the primary PW. They use status codes transmitted between endpoint T-PEs using the PW Status TLV transmitted by LDP. For this management to apply to statically provisioned PWs, the PW status signaling defined in RFC 6478 MUST be used for the primary and secondary PWs. In that case, the endpoint T-PEs can then use the PW status signaling provided by RFC 6478 in place of LDP-based status signaling, so that the status-signaling-based procedures in RFC 6870 operate identically to when used with LDP-based status signaling. Note that the optional S-PE Bypass Mode defined in Section 5.5 of RFC 6478 cannot be used, as it requires LDP signaling.

3. Operational Considerations

Because LDP is not used between the T-PEs for statically provisioned MS-PWs, the negotiation procedures described in RFC 6870 cannot be used. Thus, operational care must be taken so that the endpoint T-PEs are identically provisioned regarding the use of this document, specifically whether or not MS-PW redundancy is being used, and for each protected MS-PW, the identity of the primary MS-PW and the precedence of the secondary MS-PWs.

4. Security Considerations

The security considerations defined for RFC 6478 apply to this document as well. As the security considerations in RFCs 6718 and 6870 are related to their use of LDP, they are not required for this document.

If the alternative approach in Appendix A is used, then the security considerations defined for RFCs 6378, 7271, and 7324 also apply.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6378] Weingarten, Y., Ed., Bryant, S., Osborne, E., Sprecher, N., and A. Fulignoli, Ed., "MPLS Transport Profile (MPLS-TP) Linear Protection", RFC 6378, DOI 10.17487/RFC6378, October 2011, <http://www.rfc-editor.org/info/rfc6378>.

[RFC6478] Martini, L., Swallow, G., Heron, G., and M. Bocci, "Pseudowire Status for Static Pseudowires", RFC 6478, DOI 10.17487/RFC6478, May 2012, <http://www.rfc-editor.org/info/rfc6478>.

[RFC6870] Muley, P., Ed. and M. Aissaoui, Ed., "Pseudowire Preferential Forwarding Status Bit", RFC 6870, DOI 10.17487/RFC6870, February 2013, <http://www.rfc-editor.org/info/rfc6870>.

[RFC7271] Ryoo, J., Ed., Gray, E., Ed., van Helvoort, H., D'Alessandro, A., Cheung, T., and E. Osborne, "MPLS Transport Profile (MPLS-TP) Linear Protection to Match the Operational Expectations of Synchronous Digital Hierarchy, Optical Transport Network, and Ethernet Transport Network Operators", RFC 7271, DOI 10.17487/RFC7271, June 2014, <http://www.rfc-editor.org/info/rfc7271>.

[RFC7324] Osborne, E., "Updates to MPLS Transport Profile Linear Protection", RFC 7324, DOI 10.17487/RFC7324, July 2014, <http://www.rfc-editor.org/info/rfc7324>.

5.2. Informative References

[PW-REDUNDANCY] Dong, J. and H. Wang, "Pseudowire Redundancy on S-PE", Work in Progress, draft-ietf-pals-redundancy-spe-02, August 2015.

[RFC5659] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, DOI 10.17487/RFC5659, October 2009, <http://www.rfc-editor.org/info/rfc5659>.

[RFC6718] Muley, P., Aissaoui, M., and M. Bocci, "Pseudowire Redundancy", RFC 6718, DOI 10.17487/RFC6718, August 2012, <http://www.rfc-editor.org/info/rfc6718>.

Appendix A. Optional Linear Protection Approach

A.1. Introduction

In "MPLS Transport Profile (MPLS-TP) Linear Protection" [RFC6378], as well as in the later updates of that RFC "MPLS Transport Profile (MPLS-TP) Linear Protection to Match the Operational Expectations of Synchronous Digital Hierarchy, Optical Transport Network, and Ethernet Transport Network Operators" [RFC7271] and "Updates to MPLS Transport Profile Linear Protection" [RFC7324], the Protection State Coordination (PSC) protocol was defined for MPLS LSPs only.

This appendix extends these RFCs to be applicable for PWs (SS-PW and MS-PW) as well. This is useful especially in the case of end-to-end static provisioned MS-PWs running over MPLS-TP where tunnel protection alone cannot be relied upon for end-to-end protection of PWs against S-PE failure. It also enables a uniform operational approach for protection at LSP and PW layers and an easier management integration for networks that already implement the approach in RFCs 6378, 7271, and 7324.

The protection architectures are those defined in [RFC6378]. For the purposes of this appendix, we define the protection domain of a point-to-point PW as consisting of two terminating PEs (T-PEs) and the transport paths that connect them (see Figure 2).

```
+-----+ //=======================\\ +-----+
|T-PE1|//     Working Path        \\|T-PE2|
|    /|                             |\    |
|  ?< |                             | >?  |
|    \|                             |/    |
|     |\\    Protection Path      //|     |
+-----+ \\=======================// +-----+

    |<-------Protection Domain------->|
```

Figure 2: Protection Domain

This Appendix is an OPTIONAL alternative approach to the one in Section 2. For interoperability, all implementations MUST include the approach in Section 2, even if this alternative approach is used. The operational considerations in Section 3 continue to apply when this approach is used, and operational care must be taken so that the endpoint T-PEs are identically provisioned regarding the use of this document.

A.2. Encapsulation of the PSC Protocol for Pseudowires

The PSC protocol can be used to protect against defects on any LSP (segment, link, or path). In the case of MS-PW, the PSC protocol can also protect failed intermediate nodes (S-PE). Linear protection protects an LSP or PW end-to-end and if a failure is detected, switches traffic over to another (redundant) set of resources.

Obviously, the protected entity does not need to be of the same type as the protecting entity. For example, it is possible to protect a link by a path. Likewise, it is possible to protect an SS-PW with an MS-PW, and vice versa.

From a PSC protocol point of view, it is possible to view an SS-PW as a single-hop LSP and an MS-PW as a multiple-hop LSP. Thus, this provides end-to-end protection for the SS-PW or MS-PW. The Generic Associated Channel (G-Ach) carrying the PSC protocol information is placed in the label stack directly beneath the PW identifier. The PSC protocol will then work as specified in RFCs 6378, 7271, and 7324.

Acknowledgements

The authors would like to thank Matthew Bocci, Yaakov Stein, David Sinicrope, Sasha Vainshtein, and Italo Busi for their comments on this document.

Figure 1 and the explanatory paragraph following the figure were taken from RFC 6718. Figure 2 was adapted from RFC 6378.

Authors' Addresses

Andrew G. Malis (editor)
Huawei Technologies Co., Ltd.

Email: agmalis@gmail.com

Loa Andersson
Huawei Technologies Co., Ltd.

Email: loa@mail01.huawei.com

Huub van Helvoort
Hai Gaoming BV

Email: huubatwork@gmail.com

Jongyoon Shin
SK Telecom

Email: jongyoon.shin@sk.com

Lei Wang
China Mobile

Email: wangleiyj@chinamobile.com

Alessandro D'Alessandro
Telecom Italia

Email: alessandro.dalessandro@telecomitalia.it