Network Working Group
Internet-Draft
Updates: 6870 (if approved)
Intended status: Standards Track
Expires: April 13, 2015

A. Malis
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

October 10, 2014

S-PE Outage Protection for Static Multi-Segment Pseudowires
draft-shawam-pwe3-ms-pw-protection-02.txt

Abstract

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 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 PEs (S-PEs) along the path of the MS-PW. This document describes how to achieve this protection by updating the existing procedures in RFC 6870. It also contains an optional approach based on MPLS-TP Linear Protection.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

As described in RFC 5659 [RFC5659], Multi-Segment Pseudowires (MS-PWs) consist of terminating PEs (T-PEs), switching PEs (S-PEs), and PW segments between the T-PEs at each of the MS-PW and the interior S-PEs. 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, PSN 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.

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 Section 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 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, CE1 is connected to PE1 and CE2 is connected to PE2. 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 protocol.

However, statically provisioned PWs (SS-PWs or MS-PWs) do not use the LDP protocol for PW set and signaling, rather they are provisioned by network management systems or other means at each T-PE and S-PE along their path. They also do not use the LDP protocol for status signaling. Rather, they use procedures defined in RFC 6478 [RFC6478] for status signaling via the PW 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 describes 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 the place of LDP-based status signaling, but otherwise operate identically as described in RFC 6870.

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. IANA Considerations

There are no requests for IANA actions in this document.

Note to the RFC Editor - this section can be removed before publication.

6. Acknowledgements

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

Figure 1 and the explanatory paragraph following the figure were taken from RFC 6718.

7. References

7.1. Normative References

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

[RFC6378] Weingarten, Y., Bryant, S., Osborne, E., Sprecher, N., and A. Fulignoli, "MPLS Transport Profile (MPLS-TP) Linear Protection", RFC 6378, October 2011.

[RFC6478] Martini, L., Swallow, G., Heron, G., and M. Bocci, "Pseudowire Status for Static Pseudowires", RFC 6478, May 2012.

[RFC6870] Muley, P. and M. Aissaoui, "Pseudowire Preferential Forwarding Status Bit", RFC 6870, February 2013.

[RFC7271] Ryoo, J., Gray, E., 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, June 2014.

[RFC7324] Osborne, E., "Updates to MPLS Transport Profile Linear Protection", RFC 7324, July 2014.

7.2. Informative References

[RFC5659] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, October 2009.

[RFC6718] Muley, P., Aissaoui, M., and M. Bocci, "Pseudowire Redundancy", RFC 6718, August 2012.

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 this RFC in "MPLS Transport Profile (MPLS-TP) Linear Protection to Match the Operational Expectations of SDH, OTN and Ethernet Transport Network Operators" [RFC7271] and in "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 use RFCs 6378, 7271, and 7324.

This Appendix is optional alternative approach to the one in Section 2, therefore 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. For example, it is possible to protect a link by a path. Likewise it is possible to protect a SS-PW with a MS-PW and vice versa.

From a PSC protocol point of view it is possible to view a SS-PW as a single hop LSP, and a MS-PW as a multiple hop LSP. Thus, this provides end-to-end protection for the SS-PW or MS-PW. The 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.

Authors' Addresses

Andrew G. Malis
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