Network Working Group
Internet-Draft
Updates: 6870 (if approved)
Intended status: Standards Track
Expires: March 30, 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

September 26, 2014

S-PE Outage Protection for Static Multi-Segment Pseudowires
draft-shawam-pwe3-ms-pw-protection-01.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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on March 30, 2015.

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.

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. The procedures in these RFCs 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.

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.

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.

[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.

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.

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