Internet Engineering Task Force (IETF)
Request for Comments: 8184
Category: Informational
ISSN: 2070-1721

W. Cheng
L. Wang
H. Li
China Mobile
S. Davari
Broadcom Corporation
J. Dong
Huawei Technologies

June 2017

Dual-Homing Protection for MPLS and the MPLS Transport Profile (MPLS-TP) Pseudowires

Abstract

This document describes a framework and several scenarios for a pseudowire (PW) dual-homing local protection mechanism that avoids unnecessary switchovers and does not depend on whether a control plane is used. A Dual-Node Interconnection (DNI) PW is used to carry traffic between the dual-homing Provider Edge (PE) nodes when a failure occurs in one of the Attachment Circuits (AC) or PWs. This PW dual-homing local protection mechanism is complementary to existing PW protection mechanisms.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 7841.

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/rfc8184.

Table of Contents

1. Introduction

[RFC6372] and [RFC6378] describe the framework and mechanism of MPLS Transport Profile (MPLS-TP) linear protection, which can provide protection for the MPLS Label Switched Path (LSP) or pseudowire (PW) between the edge nodes. This mechanism does not protect against failure of the Attachment Circuit (AC) or the Provider Edge (PE) node. [RFC6718] and [RFC6870] describe the framework and mechanism for PW redundancy to provide protection against AC or PE node failure. The PW redundancy mechanism is based on the signaling of the Label Distribution Protocol (LDP), which is applicable to PWs with a dynamic control plane. [RFC8104] describes a fast local repair mechanism for PW egress endpoint failures, which is based on PW redundancy, upstream label assignment, and context-specific label switching. The mechanism defined in [RFC8104] is only applicable to PWs with a dynamic control plane.

There is a need to support a dual-homing local protection mechanism that avoids unnecessary switches of the AC or PW and can be used regardless of whether a control plane is used. In some scenarios, such as mobile backhauling, the MPLS PWs are provisioned with dual-homing topology in which at least the Customer Edge (CE) node on one side is dual-homed to two PEs. If some fault occurs in the primary AC, operators usually prefer to have the switchover only on the dual-homing PE side and keep the working pseudowires unchanged if possible. This is to avoid massive PW switchover in the mobile backhaul network due to AC failure in the mobile core site; such massive PW switchover may in turn lead to congestion caused by migrating traffic away from the preferred paths of network planners. Similarly, as multiple PWs share the physical AC in the mobile core site, it is preferable to keep using the working AC when one working PW fails in the Packet Switched Network (PSN) to potentially avoid unnecessary switchover for other PWs. To meet the above requirements, a fast dual-homing local PW protection mechanism is needed to protect against the failures of an AC, the PE node, and the PSN.

This document describes the framework and several typical scenarios of PW dual-homing local protection. A Dual-Node Interconnection (DNI) PW is used between the dual-homing PE nodes to carry traffic when a failure occurs in the AC or PW side. In order for the dual-homing PE nodes to determine the forwarding state of AC, PW, and DNI-PW, necessary state exchange and coordination between the dual-homing PEs is needed. The necessary mechanisms and protocol extensions are defined in [RFC8185].

2. Reference Models of Dual-Homing Local Protection

This section shows the reference architecture of the dual-homing PW local protection and the usage of the architecture in different scenarios.

2.1. PE Architecture

Figure 1 shows the PE architecture for dual-homing local protection. This is based on the architecture in Figure 4a of [RFC3985]. In addition to the AC and the service PW between the local and remote PEs, a DNI-PW is used to connect the forwarders of the dual-homing PEs. It can be used to forward traffic between the dual-homing PEs when a failure occurs in the AC or service PW side. As [RFC3985] specifies: "any required switching functionality is the responsibility of a forwarder function". In this case, the forwarder is responsible for switching the payloads between three entities: the AC, the service PW, and the DNI-PW.

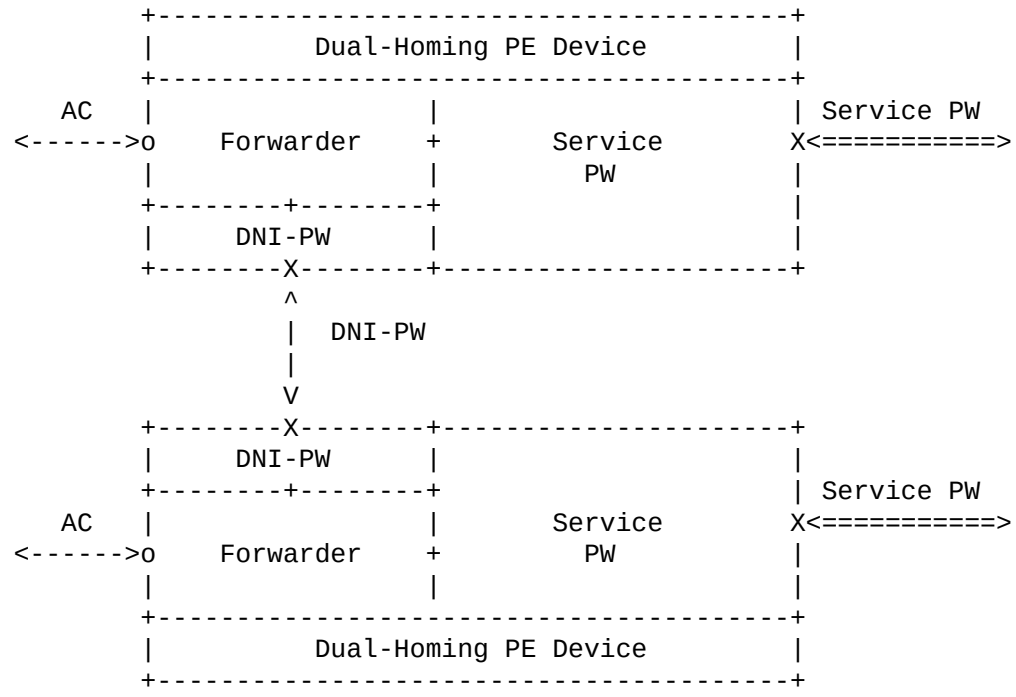

Figure 1: PE Architecture for Dual-Homing Protection

2.2. Dual-Homing Local Protection Reference Scenarios

2.2.1. One-Side Dual-Homing Protection

Figure 2 illustrates the network scenario of dual-homing PW local protection where only one of the CEs is dual-homed to two PE nodes. CE1 is dual-homed to PE1 and PE2, while CE2 is single-homed to PE3. A DNI-PW is established between the dual-homing PEs, which is used to bridge traffic when a failure occurs in the PSN or the AC side. A dual-homing control mechanism enables the PEs and CE to determine which AC should be used to carry traffic between CE1 and the PSN. The necessary control mechanisms and protocol extensions are defined in [RFC8185].

This scenario can protect against node failure of PE1 or PE2 or failure of one of the ACs between CE1 and the dual-homing PEs. In addition, dual-homing PW protection can protect against failure occurring in the PSN that impacts the working PW; thus, it can be an alternative solution of PSN tunnel protection mechanisms. This topology can be used in mobile backhauling application scenarios. For example, CE2 might be an equipment cell site such as a NodeB, while CE1 is the shared Radio Network Controller (RNC). PE3 functions as an access-side MPLS device, while PE1 and PE2 function as core-side MPLS devices.

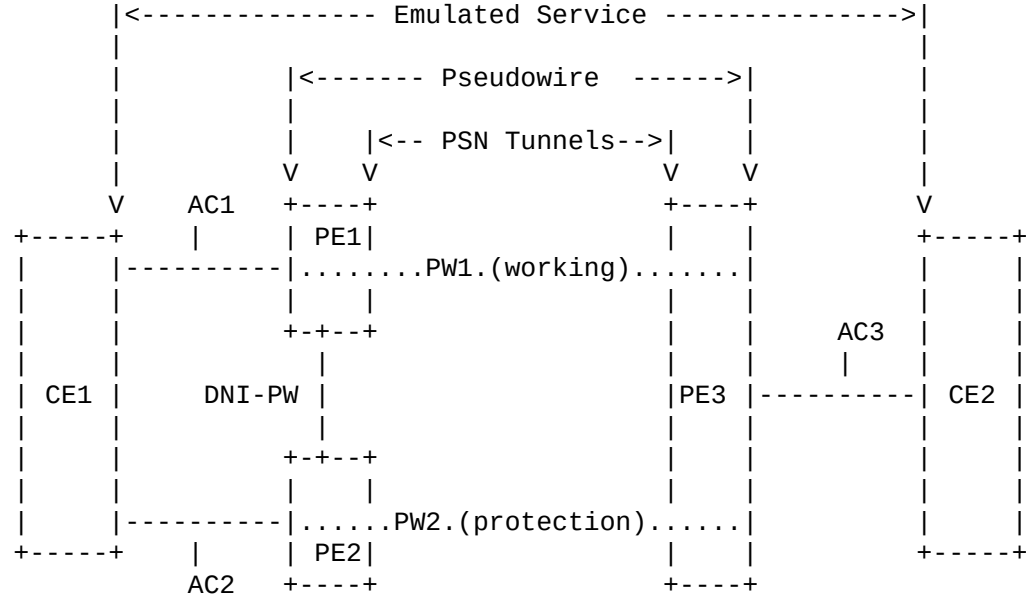

Figure 2: One-Side Dual-Homing PW Protection

Consider the example where in normal state AC1 from CE1 to PE1 is initially active and AC2 from CE1 to PE2 is initially standby. PW1 is configured as the working PW and PW2 is configured as the protection PW.

When a failure occurs in AC1, then the state of AC2 changes to active based on the AC dual-homing control mechanism. In order to keep the switchover local and continue using PW1 for traffic forwarding as preferred according to traffic planning, the forwarder on PE2 needs to connect AC2 to the DNI-PW, and the forwarder on PE1 needs to connect the DNI-PW to PW1. In this way, the failure in AC1 will not impact the forwarding of the service PWs across the network. After the switchover, traffic will go through the bidirectional path: CE1-(AC2)-PE2-(DNI-PW)-PE1-(PW1)-PE3-(AC3)-CE2.

When a failure in the PSN affects the working PW (PW1), according to PW protection mechanisms [RFC6378], traffic is switched onto the protection PW (PW2) while the state of AC1 remains active. Then, the forwarder on PE1 needs to connect AC1 to the DNI-PW, and the forwarder on PE2 needs to connect the DNI-PW to PW2. In this way, the failure in the PSN will not impact the state of the ACs. After the switchover, traffic will go through the bidirectional path: CE1-(AC1)-PE1-(DNI-PW)-PE2-(PW2)-PE3-(AC3)-CE2.

When a failure occurs in the working PE (PE1), it is equivalent to a failure of the working AC, the working PW, and the DNI-PW. The state of AC2 changes to active based on the AC dual-homing control mechanism. In addition, according to the PW protection mechanism, traffic is switched on to the protection PW "PW2". In this case, the forwarder on PE2 needs to connect AC2 to PW2. After the switchover, traffic will go through the bidirectional path: CE1-(AC2)-PE2-(PW2)-PE3-(AC3)-CE2.

2.2.2. Two-Side Dual-Homing Protection

Figure 3 illustrates the network scenario of dual-homing PW protection where the CEs in both sides are dual-homed. CE1 is dual-homed to PE1 and PE2, and CE2 is dual-homed to PE3 and PE4. A dual-homing control mechanism enables the PEs and CEs to determine which AC should be used to carry traffic between the CE and the PSN. DNI-PWs are used between the dual-homing PEs on both sides. One service PW is established between PE1 and PE3, and another service PW is established between PE2 and PE4. The role of working and protection PWs can be determined by either configuration or existing signaling mechanisms.

This scenario can protect against node failure on one of the dual-homing PEs or failure on one of the ACs between the CEs and their dual-homing PEs. Also, dual-homing PW protection can protect against the occurrence of failure in the PSN that impacts one of the PWs; thus, it can be used as an alternative solution of PSN tunnel protection mechanisms. Note, this scenario is mainly used for services requiring high availability as it requires redundancy of the PEs and network utilization. In this case, CE1 and CE2 can be regarded as service access points.

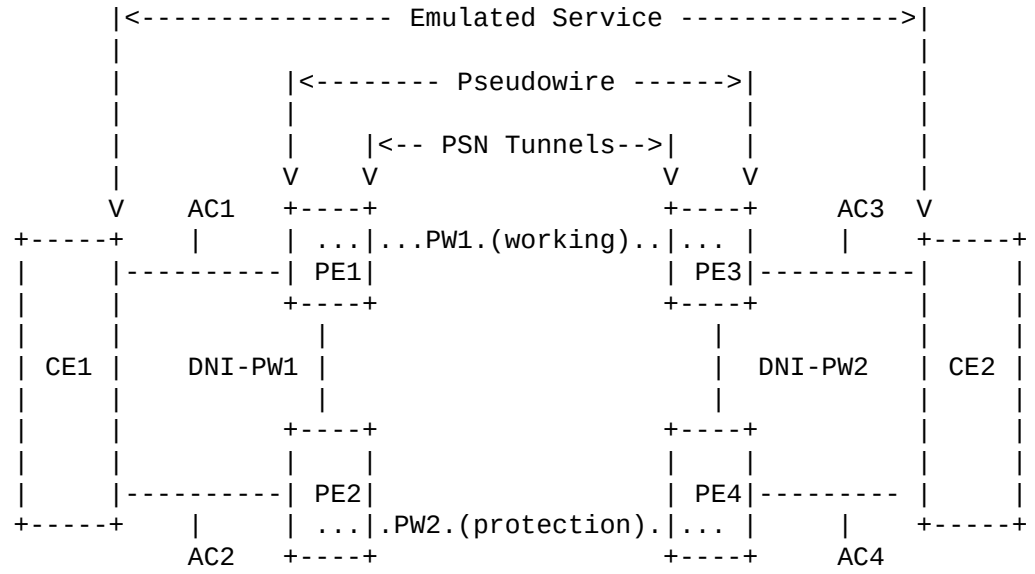

Figure 3: Two-Side Dual-Homing PW Protection

Consider the example where in normal state AC1 between CE1 and PE1 is initially active, AC2 between CE1 and PE2 is initially standby, AC3 between CE2 and PE3 is initially active and AC4 from CE2 to PE4 is initially standby. PW1 is configured as the working PW and PW2 is configured as the protection PW.

When a failure occurs in AC1, the state of AC2 changes to active based on the AC dual-homing control mechanism. In order to keep the switchover local and continue using PW1 for traffic forwarding, the forwarder on PE2 needs to connect AC2 to the DNI-PW1, and the forwarder on PE1 needs to connect DNI-PW1 with PW1. In this way, failures in the AC side will not impact the forwarding of the service PWs across the network. After the switchover, traffic will go through the bidirectional path:
CE1-(AC2)-PE2-(DNI-PW1)-PE1-(PW1)-PE3-(AC3)-CE2.

When a failure occurs in the working PW (PW1), according to the PW protection mechanism [RFC6378], traffic needs to be switched onto the protection PW "PW2". In order to keep the state of AC1 and AC3 unchanged, the forwarder on PE1 needs to connect AC1 to DNI-PW1, and the forwarder on PE2 needs to connect DNI-PW1 to PW2. On the other side, the forwarder of PE3 needs to connect AC3 to DNI-PW2, and the forwarder on PE4 needs to connect PW2 to DNI-PW2. In this way, the state of the ACs will not be impacted by the failure in the PSN. After the switchover, traffic will go through the bidirectional path: CE1-(AC1)-PE1-(DNI-PW1)-PE2-(PW2)-PE4-(DNI-PW2)-PE3-(AC3)-CE2.

When a failure occurs in the working PE (PE1), it is equivalent to the failures of the working AC, the working PW, and the DNI-PW. The state of AC2 changes to active based on the AC dual-homing control mechanism. In addition, according to the PW protection mechanism, traffic is switched on to the protection PW "PW2". In this case, the forwarder on PE2 needs to connect AC2 to PW2, and the forwarder on PE4 needs to connect PW2 to DNI-PW2. After the switchover, traffic will go through the bidirectional path: CE1-(AC2)-PE2-(PW2)-PE4-(DNI-PW2)-PE3-(AC3)-CE2.

3. Generic Dual-Homing PW Protection Mechanism

As shown in the above scenarios, with the described dual-homing PW protection, failures in the AC side will not impact the forwarding behavior of the PWs in the PSN, and vice-versa.

In order for the dual-homing PEs to coordinate traffic forwarding during failures, synchronization of the status information of the involved entities and coordination of switchover between the dual-homing PEs are needed. For PWs with a dynamic control plane, such synchronization and coordination information can be achieved with a dynamic protocol, such as that described in [RFC7275], possibly with some extensions. For PWs that are manually configured without a control plane, a new mechanism is needed to exchange the status information and coordinate switchover between the dual-homing PEs, e.g., over an embedded PW control channel. This is described in [RFC8185].

4. IANA Considerations

This document does not require any IANA action.

5. Security Considerations

The scenarios defined in this document do not affect the security model as defined in [RFC3985].

With the proposed protection mechanism, the disruption of a dual-homed AC, a component that is outside the core network, would have a reduced impact on the traffic flows in the core network. This could also avoid unnecessary congestion in the core network.

The security consideration of the DNI-PW is the same as for service PWs in the data plane [RFC3985]. Security considerations for the coordination/control mechanism will be addressed in the companion document, RFC 8185, which defines the mechanism.

6. References

6.1. Normative References

[RFC3985] Bryant, S., Ed. and P. Pate, Ed., "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, DOI 10.17487/RFC3985, March 2005, <http://www.rfc-editor.org/info/rfc3985>.

[RFC8185] Cheng, W., Wang, L., Li, H., Dong, J., and A. D'Alessandro, "Dual-Homing Coordination for MPLS Transport Profile (MPLS-TP) Pseudowires Protection", RFC 8185, DOI 10.17487/RFC8185, June 2017.

6.2. Informative References

[RFC6372] Sprecher, N., Ed. and A. Farrel, Ed., "MPLS Transport Profile (MPLS-TP) Survivability Framework", RFC 6372, DOI 10.17487/RFC6372, September 2011, <http://www.rfc-editor.org/info/rfc6372>.

[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>.

[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>.

[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>.

[RFC7275] Martini, L., Salam, S., Sajassi, A., Bocci, M., Matsushima, S., and T. Nadeau, "Inter-Chassis Communication Protocol for Layer 2 Virtual Private Network (L2VPN) Provider Edge (PE) Redundancy", RFC 7275, DOI 10.17487/RFC7275, June 2014, <http://www.rfc-editor.org/info/rfc7275>.

[RFC8104] Shen, Y., Aggarwal, R., Henderickx, W., and Y. Jiang, "Pseudowire (PW) Endpoint Fast Failure Protection", RFC 8104, DOI 10.17487/RFC8104, March 2017, <http://www.rfc-editor.org/info/rfc8104>.

Contributors

The following individuals substantially contributed to the content of this document:

Kai Liu
Huawei Technologies
Email: alex.liukai@huawei.com

Alessandro D'Alessandro
Telecom Italia
Email: alessandro.dalessandro@telecomitalia.it

Authors' Addresses

Weiqiang Cheng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: chengweiqiang@chinamobile.com

Lei Wang
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: Wangleiyj@chinamobile.com

Han Li
China Mobile
No.32 Xuanwumen West Street
Beijing 100053
China

Email: Lihan@chinamobile.com

Shahram Davari
Broadcom Corporation
3151 Zanker Road
San Jose 95134-1933
United States of America

Email: davari@broadcom.com

Jie Dong
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: jie.dong@huawei.com