

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 19, 2014

W. Cheng
L. Wang
H. Li
China Mobile
K. Liu
Huawei Technologies
S. Davari
Broadcom Corporation
J. Dong
Huawei Technologies
July 01, 2014

Dual-Homing Protection for MPLS Transport Profile (MPLS-TP) Pseudowires
draft-cheng-pwe3-mpls-tp-dual-homing-protection-00

Abstract

In some scenarios, the MPLS Transport Profile (MPLS-TP) Pseudowires (PWs) are provisioned through either static configuration or management plane, where a dynamic control plane is not available. A fast protection mechanism for MPLS-TP PWs is needed to protect against the failure of Attachment Circuit (AC), the failure of Provider Edge (PE) and also the failure in the Packet Switched Network (PSN). This document proposes a dual-homing protection mechanism for MPLS-TP PWs, which can provide fast protection for comprehensive failure scenarios including the failure of AC, the PE node or the PSN network.

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].

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 December 19, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. MPLS-TP PW Dual-Homing Protection Scenarios	3
2.1. One-side Dual-Homing Protection	3
2.2. Two-side Dual-Homing Protection	4
3. Overview of the Proposed Solution	5
4. Protocol Extensions for MPLS-TP PW Dual-Homing Protection . .	6
4.1. Information Exchange Between Dual-Homing PEs	6
4.2. Protection Procedures	9
5. IANA Considerations	11
6. Security Considerations	11
7. References	11
7.1. Normative References	12
7.2. Informative References	12
Authors' Addresses	12

1. Introduction

[RFC6372] and [RFC6378] describe the framework and mechanism of MPLS-TP Linear protection, which can provide protection for the MPLS LSP or PW between the edge nodes. Such mechanism does not protect the failure of the Attachment Circuit (AC) or the edge node. [RFC6718] [RFC6870] describe the framework and mechanism for PW redundancy to provide protection for AC or PE node failure. The PW redundancy mechanism is based on the signaling of Label Distribution Protocol (LDP), which is applicable to MPLS PWs or MPLS-TP PWs with a dynamic control plane. [I-D.ietf-pwe3-endpoint-fast-protection] 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. Such mechanism is applicable to PWs with a dynamic control plane.

In some scenarios such as mobile backhauling, the MPLS-TP PWs are provisioned through either static configuration or management plane, where a dynamic control plane is not available. A fast protection mechanism is needed for these MPLS-TP PWs to protect against the failure of AC, the PE node or the PSN network.

In addition, if at least one side CE node is dual-homed to two PEs, and a fault occurs in the primary AC, operators usually prefer to perform switchover only in the AC side and keeps using the working pseudowire if possible. The purpose is to avoid massive PW switchover caused by AC failure in mobile backhaul networks and to achieve efficient and balanced link bandwidth utilization in the PSN network.

This document proposes a dual-homing protection mechanism for static MPLS-TP PWs, which can provide fast protection for comprehensive failure scenarios including failure of AC, the PE node or the PSN network, and meet the requirement of avoiding PW switchover when possible. The mechanism defined in this document is complementary to the existing protection mechanisms.

The proposed mechanism has been deployed in several mobile backhaul networks which use static MPLS-TP PWs for the backhauling of mobile traffic from the RF sites to the core sites.

2. MPLS-TP PW Dual-Homing Protection Scenarios

The following sections describe the typical topology and application scenarios of MPLS-TP PW dual-homing protection. The scenarios can be classified into two categories: one-side dual-homing and two-side dual-homing.

2.1. One-side Dual-Homing Protection

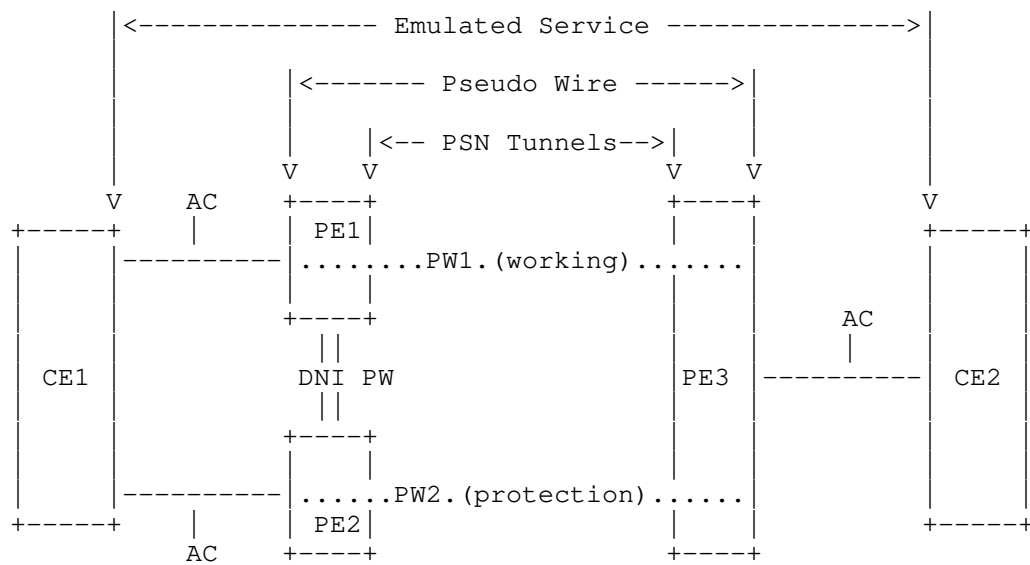


Figure 1. One-side PW dual-homing protection

Figure 1 illustrates the network scenario of one-side CE dual-homing protection. CE1 is dual-homed to PE1 and PE2, while CE2 is single-homed to PE3. This topology protects the node failures of PE1 and PE2 and the AC link failures between CE1 and PE1, PE2. This scheme can be used in mobile backhauling application scenarios. For example, NodeB serves as CE2 while RNC serves as CE1. PE3 works as an access side MPLS-TP device while PE1 and PE2 works as a core side MPLS-TP device.

2.2. Two-side Dual-Homing Protection

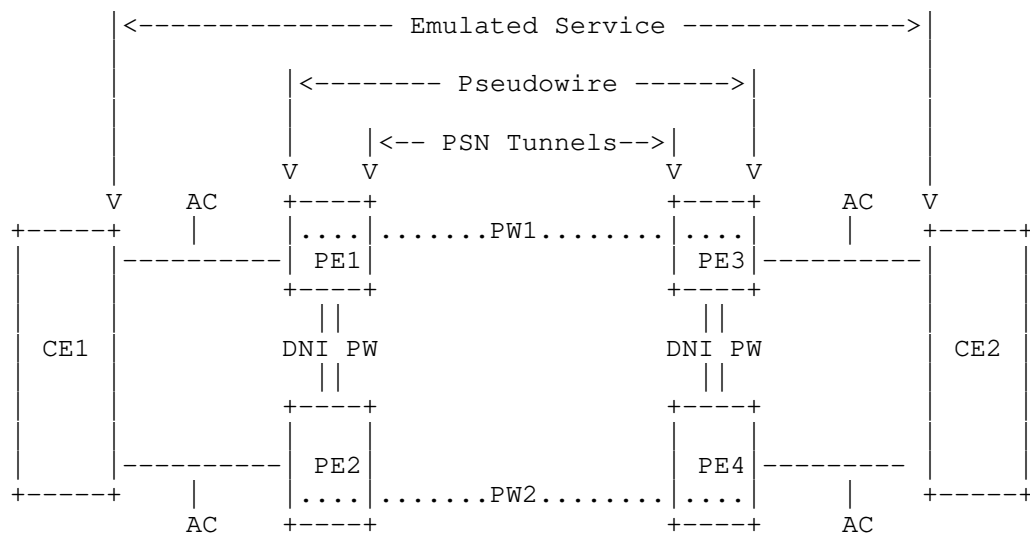


Figure 2. Two-side PW dual-homing protection

Figure 2 illustrates the network scenario of two-side CE dual-homing. CE1 is dual-homed to PE1 and PE2, and CE2 is dual-homed to PE3 and PE4. This topology can protect the node failure of the dual-homing PEs on both sides, and also protects the AC link failures between the CEs and their dual-homing PEs. Meanwhile, dual-homing PW protection can protect the failure occurred in the PSN network. This scenario is mainly used for services providing for important business customers. In this case, CE1 and CE2 can be regarded as service access points.

3. Overview of the Proposed Solution

The linear protection mechanisms for MPLS-TP network are defined in [RFC6378] [I-D.ietf-mpls-tp-psc-itu]. When such mechanisms are applied to PW linear protection, both the working PW and the protection PW need to terminate on the same PE nodes. This section extends these mechanisms to provide dual-homing protection for MPLS-TP PWs.

With MPLS-TP PW dual-homing protection mechanism, the linear protection mechanisms on the Single-homing PE (e.g. PE3 in figure 3) are not changed, while on the dual-homing side the working PW and protection PW are terminated on two dual-homing PEs (e.g. PE1 and PE2 in figure 3) respectively, to provide protection for the dual-homing PEs and the connected ACs. A dedicated Dual-Node Interconnection (DNI) PW is established between the two dual-homing PE nodes, which is used to bridge the PW traffic when failure happens in the working PW or the primary AC. In order to make the linear

The format of an MPLS-TP DHC message is shown below:

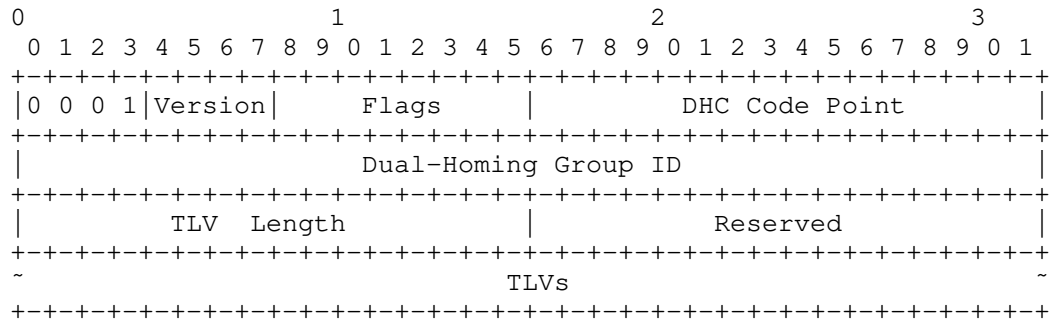


Figure 4. MPLS-TP Dual-Homing Coordination Message

The Dual-Homing Group ID is a 4-octet unsigned integer to identify the dual-homing PEs in the same dual-homing group.

2 TLVs are defined in MPLS-TP Dual-Homing Coordination message for MPLS-TP PW dual-homing protection:

Type	Description	Length
1	PW Status	20 Bytes
2	Dual-Node Switching	16 Bytes

The PW Status TLV is used by a dual-homing PE to report its Service PW status to the other dual-homing PE in the same dual-homing group.

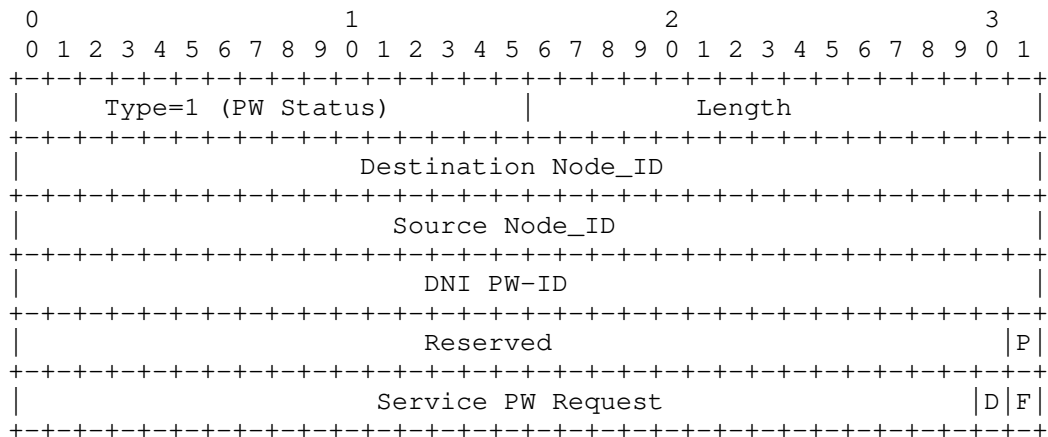


Figure 5. PW Status TLV

- The Destination Node_ID is the 32-bit Node_ID of the receiving PE.
- The Source Node_ID is the 32-bit Node_ID of the sending PE.

- The DNI PW-ID field contains PW-ID of the DNI PW.
- The P (Protection) bit indicates whether the message is sent by the working PE (P=0) or by the protection PE (P=1).
- The Service PW Request field indicates the protection request generated on the Service PW between the sending PE and the remote PE. Two bits are defined in the Service PW Request field:
 - o F bit: Indicates Signal Fail (SF) request is generated on the service PW. It can be either a local request or a remote request received from the remote PE.
 - o D bit: Indicates Signal Degrade (SD) request is generated on the service PW. It can be either a local request or a remote request received from the remote PE.
 - o Other bits are reserved and MUST be set to 0 and SHOULD be ignored upon receipt.

The Dual-Node Switching TLV is used by the protection dual-homing PE to send protection state coordination to the working dual-homing PE.

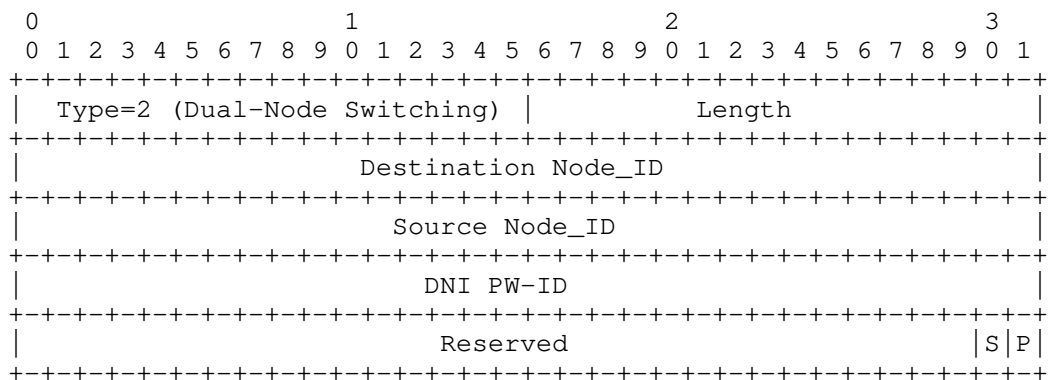


Figure 6. Dual-node Switching TLV

- The Destination Node_ID is the 32-bit Node_ID of the receiving PE.
- The Source Node_ID is the 32-bit Node_ID of the sending PE.
- The DNI PW-ID field contains PW-ID of the DNI PW.
- The P (Protection) bit indicates whether the message is sent by the working PE (P=0) or by the protection PE (P=1). With the mechanism described in this document, only the protection PE could send out the DHC message with the Dual-node Switching TLV.

- The S (PW Switching) bit indicates which service PW is used for transporting user traffic. It is set to 0 when traffic is transported on the working PW, and is set to 1 if traffic will be transported on the protection PW. The value of the S bit is determined by the protection coordination mechanism between the dual-homing protection PE and the remote PE.

4.2. Protection Procedures

MPLS-TP PW dual-homing protection mechanism can work with the existing AC side redundancy mechanisms, e.g. MC-LAG. On PSN network side, PSN tunnel protection mechanism is not required, as the dual-homing PW protection can also protect the failure happened in the PSN network.

For the single-homing PE, it just treats the working PW and protection PW as if they terminate on the same remote PE node, thus normal protection coordination mechanisms still apply to the single-homing PE.

The protection behavior of the dual-homing PEs is determined by the components shown in the figure below:

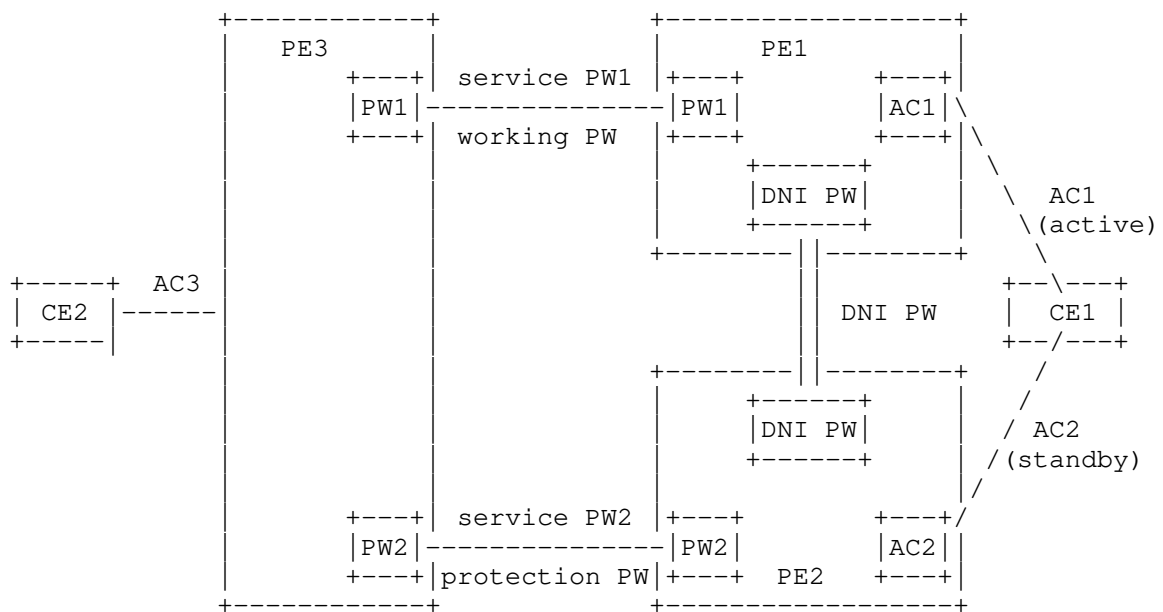


Figure 7. Components of PW Dual-Homing protection

In figure 7, for a dual-homing PE, Service PW is the PW which carries service between dual-homing PE and the remote PE. The status of

Service PW is determined by the OAM and protection switching coordination mechanisms between the dual-homing PEs and the remote PE.

DNI PW is the PW between the two dual-homing PE nodes. It is used to bridge traffic when failure occurs in PSN network or in the AC side. The status of DNI PW is determined by OAM protocol running between the dual-homing PEs.

AC is the link which connects the dual-homing PEs to the dual-homed CE. The AC status is determined by MC-LAG or other AC redundancy mechanisms.

The PW status and protection coordination requests are exchanged between the dual-homing PEs using the DHC message defined in section 4.1.

After the exchange of PW status information using the MPLS-TP DHC Message, both dual-homing PEs obtain the status of working and protection service PWs, the AC and the DNI PW. The forwarding behaviour of dual-homing PE nodes are determined by the forwarding state machine shown in the following table:

Service PW	AC	DNI PW	Forwarding Behavior
Active	Active	Up	Service PW <-> AC
Active	Standby	Up	Service PW <-> DNI PW
Standby	Active	Up	DNI PW <-> AC
Standby	Standby	Up	Drop all packets

Table 1. Dual-homing PE Forwarding State Machine

In normal state, the working PW is in active state, and the primary AC is active state, according to Table 1, PW traffic will be forwarded between the working service PW and the primary AC (AC1). No traffic will go through the protection PE or the DNI PW, as both the protection service PW and the AC connecting to the protection PE are in standby state.

If AC1 goes down due to some fault, the AC side redundancy mechanism would switchover to the backup AC (AC2), the state of AC2 changes to active. There is no change in the status of working and protection PW. According to Table 1, PE1 starts to forward traffic between the working PW and the DNI PW, while PE2 starts to forward traffic

between DNI PW and AC2. Note that in this case only AC switchover takes place, in PSN network traffic keeps transporting on the working PW and PW switchover is no needed.

If the working PW is down due to some fault in the PSN network, both the remote PE (PE3) and the working PE (PE1) would detect the failure using MPLS-TP OAM mechanisms, then PE3 would send a normal protection coordination message on the protection path to inform its peer node (PE2) to switchover to the protection PW. PE1 would also inform PE2 the working PW status (down) using the MPLS-TP DHC message. Then according to Table 1, PE2 starts to forward traffic between the protection PW and the DNI PW, and PE1 starts to forward traffic between the DNI PW and AC1.

If the working PE (PE1) goes down, both the remote PE (PE3) and the protection PE (PE2) would detect the failure using MPLS-TP OAM mechanisms, the state of AC1 would change to down, and the state of AC2 will change to active according to AC side redundancy mechanism. Then PE3 would send a normal protection coordination message on the protection path to inform its peer node (PE2) to switchover to the protection PW. Then according to table 1, PE2 starts to forward traffic between the protection PW and AC2.

5. IANA Considerations

IANA needs to assign one new channel type for "MPLS-TP Dual-Homing Coordination message" from the "Pseudowire Associated Channel Types" registry.

This document creates a new registry called "MPLS-TP DHC TLVs" registry. 2 new TLVs are defined in this document:

Type	Description	Length
1	PW Status	20 Bytes
2	Dual-Node Switching	16 Bytes

6. Security Considerations

Procedures and protocol extensions defined in this document do not affect the security model of MPLS-TP linear protection as defined in [RFC6378]. Please refer to [RFC5920] for MPLS security issues and generic methods for securing traffic privacy and integrity.

7. References

7.1. Normative References

- [I-D.ietf-mpls-tp-psc-itu]
Ryoo, J., Gray, E., Helvoort, H., D'Alessandro, A.,
Cheung, T., and E. Osborne, "MPLS Transport Profile (MPLS-
TP) Linear Protection to Match the Operational
Expectations of SDH, OTN and Ethernet Transport Network
Operators", draft-ietf-mpls-tp-psc-itu-04 (work in
progress), March 2014.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC6372] Sprecher, N. and A. Farrel, "MPLS Transport Profile (MPLS-
TP) Survivability Framework", RFC 6372, September 2011.
- [RFC6378] Weingarten, Y., Bryant, S., Osborne, E., Sprecher, N., and
A. Fulignoli, "MPLS Transport Profile (MPLS-TP) Linear
Protection", RFC 6378, October 2011.

7.2. Informative References

- [I-D.ietf-pwe3-endpoint-fast-protection]
Shen, Y., Aggarwal, R., Henderickx, W., and Y. Jiang, "PW
Endpoint Fast Failure Protection", draft-ietf-pwe3-
endpoint-fast-protection-00 (work in progress), December
2013.
- [RFC5920] Fang, L., "Security Framework for MPLS and GMPLS
Networks", RFC 5920, July 2010.
- [RFC6718] Muley, P., Aissaoui, M., and M. Bocci, "Pseudowire
Redundancy", RFC 6718, August 2012.
- [RFC6870] Muley, P. and M. Aissaoui, "Pseudowire Preferential
Forwarding Status Bit", RFC 6870, February 2013.

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

Kai Liu
Huawei Technologies
Huawei Base, Bantian, Longgang District
Shenzhen 518129
China

Email: alex.liukai@huawei.com

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

Email: davari@broadcom.com

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

Email: jie.dong@huawei.com

Internet Working Group
Internet Draft
Intended status: Standards Track

Y. Jiang
Y. Luo
Huawei
E. Mallette
Bright House Networks
Y. Shen
Juniper Networks
G. Zhou
China Unicom

C. Shen
China Telecom
W. Cheng
China Mobile

Expires: April 2015

October 25, 2014

Multi-chassis PON Protection in MPLS
draft-jiang-pwe3-mc-pon-03.txt

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 25, 2013.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

MPLS is being deployed deeper into operator networks, often to or past the access network node. Separately network access nodes such as PON OLTs have evolved to support first-mile access protection, where one or more physical OLTs provide first-mile diversity to the customer edge. Multi-homing support is needed on the MPLS-enabled PON OLT to provide resiliency for provided services. This document describes the multi-chassis PON protection architecture in MPLS and also proposes the ICCP extension to support it.

Table of Contents

1.	Conventions used in this document	3
2.	Terminology	3
3.	Introduction	3
4.	ICCP Protocol Extensions	6
4.1.	Multi-chassis PON Application TLVs	6
4.1.1.	PON Connect TLV	6
4.1.2.	PON Disconnect TLV	7
4.1.3.	PON Configuration TLV	7
4.1.4.	PON State TLV	8
4.1.5.	PON ONU Database Sync TLV	9
5.	PON ONU Database Synchronization	11
6.	Multi-chassis PON application procedures	11
6.1.	Protection procedure upon PON link failures	13
6.2.	Protection procedure upon PW failures	13
6.3.	Protection procedure upon the working OLT failure	13
7.	Security Considerations	14
8.	IANA Considerations	14
9.	References	14
9.1.	Normative References	14
9.2.	Informative References	15
10.	Acknowledgments	15
	Authors' Addresses	16

1. Conventions used in this document

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 [RFC2119].

2. Terminology

DSL Digital Subscriber Line

FTTx Fiber-to-the-x (FTTx, x = H for home, P for premises, C for curb)

ICCP Inter-Chassis Communication Protocol

OLT Optical Line Termination

ONU Optical Network Unit

MPLS Multi-Protocol Label Switching

PON Passive Optical Network

RG Redundancy Group

3. Introduction

MPLS is being extended to the edge of operator networks, as is described in the seamless MPLS use cases [SEAMLESS], and the MS-PW with PON access use case [RFC6456]. Combining MPLS with OLT access further facilitates a low cost multi-service convergence.

Tens of millions of FTTx lines have been deployed over the years, with many of those lines being some PON variant. PON provides operators a cost-effective solution for delivering high bandwidth (1Gbps or even 10Gbps) to a dozen or more subscribers simultaneously.

In the past, access technologies such as Passive Optical Network (PON) and Digital Subscriber Line (DSL) are usually used for subscribers, and no redundancy is provided in their deployment.

But with the rapid growth of mobile data traffic, more and more LTE small cells and Wi-Fi hotspots are deployed. PON is considered as a viable low cost backhaul solution for these mobile services. Besides its high bandwidth and scalability, PON further provides synchronization features, e.g., SyncE and IEEE1588 functionality, which can fulfill synchronization needs of mobile backhaul services.

The Broadband Forum specifies reference architecture for mobile backhaul network using MPLS transport in [TR-221] where PON can be the access technology, and is further working on PON-based mobile backhaul network architecture in [SD-331].

Unlike typical residential service where a single or handful of end-users hangs off of a single PON OLT port in a physical optical distribution network, a PON port that supports a dozen LTE small cells or Wi-Fi hotspots could be providing service to hundreds of simultaneous subscribers. Small cell backhaul often demands the economics of a PON first-mile and yet expects first-mile protection commonly available in point-to-point access portfolio.

Some optical layer of protection mechanisms, such as Trunk and Tree protection, are specified in [IEEE-1904.1] to avoid single point of failure in the access. They are called Type B and Type C protection respectively in [G983.1].

Trunk protection architecture is an economical PON resiliency mechanism, where the working OLT and the working link between the working splitter port and the working OLT (i.e., the working trunk fiber) is protected by a redundant protection OLT and a redundant trunk fiber between the protection splitter port and the protection OLT, however it only protects a portion of the optical path from OLT to ONUs. This is different from the more complex and costly Type C protection architecture where there is a working optical distribution network path from the working OLT and a complete protected optical distribution network path from the protection OLT to the ONUs. Figure 1 demonstrates a typical scenario of Trunk protection.

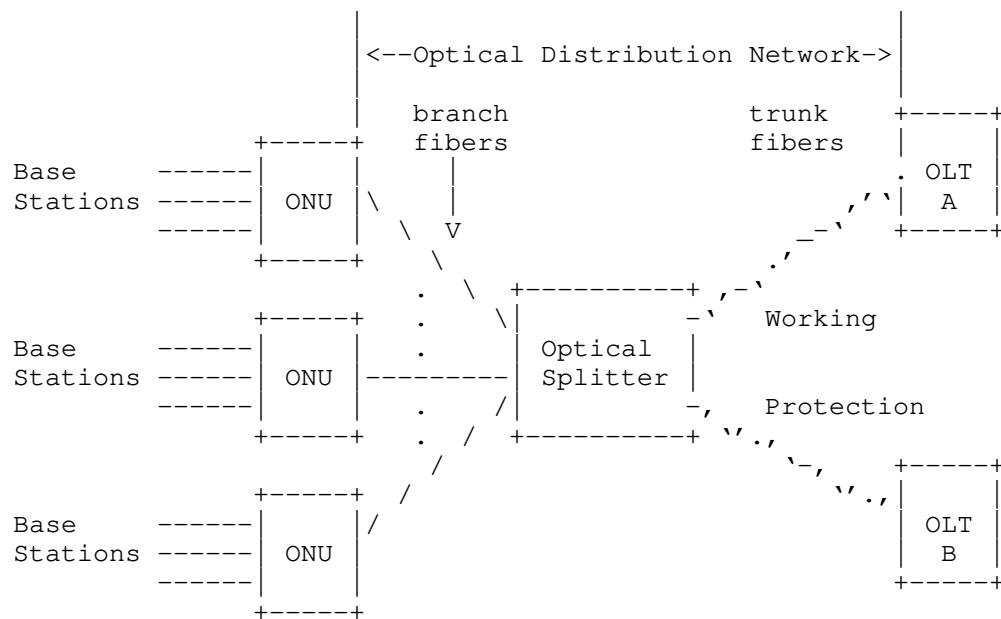


Figure 1 Trunk Protection Architecture in PON

Besides small cell backhaul, this protection architecture can also be applicable to other services, for example, DSL and Multi-System Operator (MSO) services. In that case, an ONU in Figure 1 can play the similar role as a Digital Subscriber Line Access Multiplexer (DSLAM) and dozens of Customer Premises Equipments (CPEs) or cable modems may be attached to it.

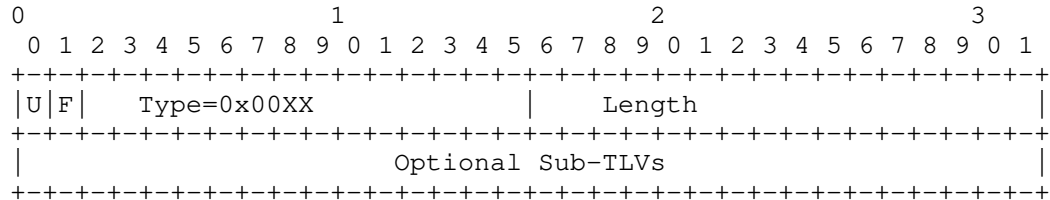
In some deployments, it is also possible that only some ONUs are needed to be protected.

The PON architecture depicted in Figure 1 can provide redundancy in its physical topology, however, all traffic including link OAM are blocked on the protection link which frustrates end to end protection mechanisms such as ITU-T G.8031. Therefore, some standard signaling mechanisms are needed between OLTs to exchange information, for example, PON link status, registered ONU information, and network status, so that protection and restoration can be done both rapidly and reliably, especially when the OLTs also support MPLS.

ICCP [ICCP] provides a framework for inter-chassis synchronization of state and configuration data between a set of two or more PEs. Currently ICCP only defines application specific messages for PW redundancy and mLACP, but it can be easily extended to support PON as an Attachment Circuit (AC) redundancy.

4.1.2. PON Disconnect TLV

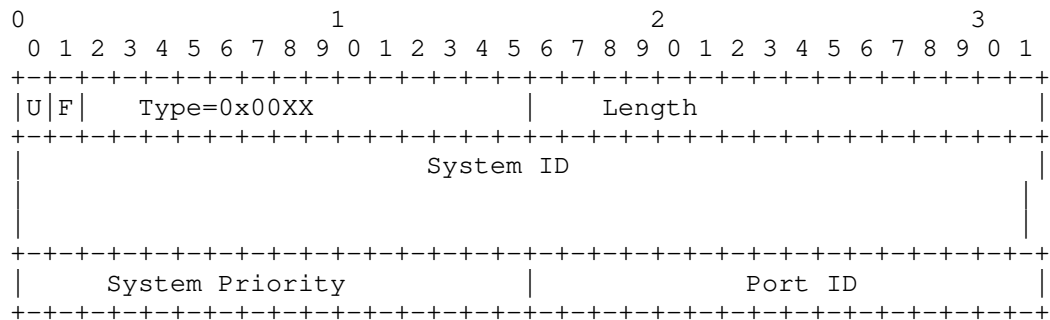
This TLV is included in the RG Disconnect message to indicate that the connection for the PON application is to be terminated.



- U and F Bits, both are set to 0.
- Type, set to 0x00XX for "PON Disconnect TLV".
- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- Optional Sub-TLVs, there are no optional Sub-TLVs defined for this version of the protocol.

4.1.3. PON Configuration TLV

The "PON Configuration TLV" is included in the "RG Application Data" message, and announces an OLT's system parameters to other members in the same RG.



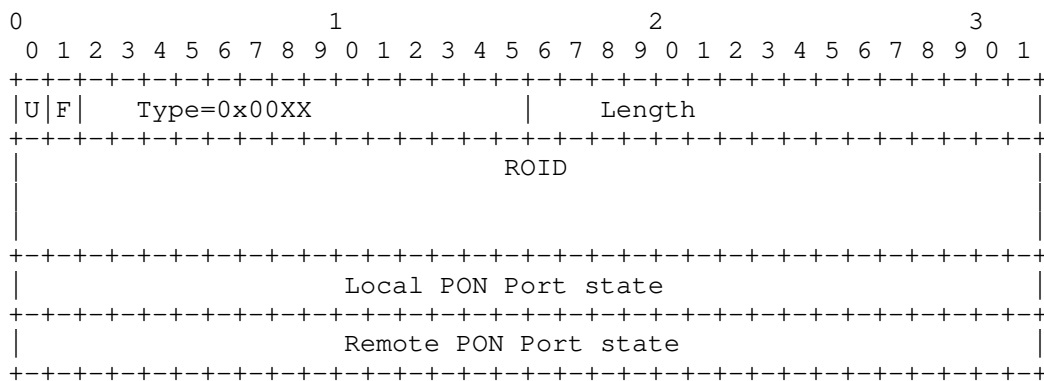
- U and F Bits, both are set to 0.
- Type, set to 0x00XX for "PON Configuration TLV".

- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- System ID, 8 octets encoding the System ID used by the OLT, which is the Chassis MAC address. If a 6 octet System ID is used, the least significant 2 octets of the 8 octet field will be encoded as 0000.
- System Priority, 2 octets encoding the System Priority.
- Port ID, 2 octets PON Port ID.

Further configuration considerations such as multicast table and ARP table for static MAC addresses will be added in a next version.

4.1.4.PON State TLV

The "PON State TLV" is included in the "RG Application Data" message, and used by an OLT to report its PON states to other members in the same RG.

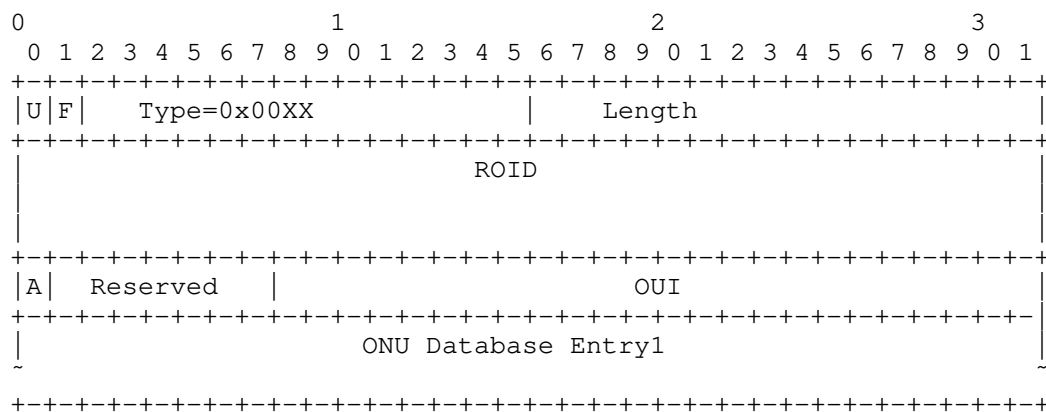


- U and F Bits, both are set to 0.
- Type, set to 0x00XX for "PON State TLV"
- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- ROID, as defined in the ROID section of [ICCP].
- Local PON Port State, the status of the local PON port as determined by the sending OLT (PE). The last bit is defined as Fault indication of the PON Port associated with this PW (1 - in fault).

- Remote PON Port State, the status of the remote PON port as determined by the remote peer of the sending OLT (PE). The last bit is defined as Fault indication of the PON Port associated with this PW (1 - in fault).

4.1.5. PON ONU Database Sync TLV

This TLV is used to communicate the registered ONU database associated with a PON port between the active and standby OLT. This message is used to both transmit the PON ONU Database from working OLT to protect OLT and to communicate the PON ONU database status between protect OLT and working OLT.



- U and F Bits, both are set to 0.
- Type, set to 0x00XX for "PON ONU Database Sync TLV"
- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- ROID, defined in the ROID section of [ICCP].
- A bit, Acknowledgement bit. Set to 1 if the receiver has received a PON ONU Database Sync. Otherwise, set to 0.
- Reserved, reserved for future use.
- OUI, the 3-byte [IEEE-802.3] organization unique identifier that uniquely identifies the format for describing the registered ONU database information. There are multiple PON standards and are varying implementations within a given PON standard which likely have

different required information, format, etc., related to the ONU Database Entry.

- ONU Database Entry, there may be one or more ONU Database Entries transmitted in the PON ONU Database Sync TLV, each of which would describe a registered ONU. The format of the ONU Database Entry is outside the scope of this document and will be defined by the relevant PON standard organization.

5. PON ONU Database Synchronization

Without an effective mechanism to communicate the registered ONUs between the working and protection OLT, all registered ONUs would be de-registered and go through re-registration during a switchover, which would significantly increase protection time. To enable faster switchover capability, the work OLT must be able to communicate the registered ONUs associated with an ROID to the protection OLT.

The PON ONU Database Synchronization would begin once the ICCP PON Application enters OPERATIONAL state. The working OLT, the one with the working link member for the ROID, would begin transmitting the database of actively registered ONUs to the protection OLT for the same ROID. Each instance of the PON ONU Database Sync TLV describes a set of ONU Database Entries. Each ONU Database Entry would describe a registered ONU.

The transmission of PON ONU Database Descriptors for a given ROID is only unidirectional – from the working OLT to the protection OLT. The protection OLT would only be responsible for acknowledging the received message to provide a reliable database synchronization mechanism. As ONUs register and deregister from the working OLT, the working OLT would transmit PON ONU Database Synchronization TLV including only the updated ONU Database Entries.

If protected ONUs and unprotected ONUs are miscellaneously attached to the same splitter, only the protected ONUs needs to be synchronized. The specific ONUs which needs to be synchronized can be policy driven and provisioned in the management plane, or by some other signaling options.

6. Multi-chassis PON application procedures

Two typical MPLS protection network architectures for PON access are depicted in Fig.2 and Fig.3 (their PON access segments are the same as in Fig.1 and thus omitted for simplification). OLTs with MPLS functionality are connected to a single PE (Fig.2) or dual home PEs (Fig.3) respectively, i.e., the working OLT to PE1 by a working PW and the protection OLT to PE1 or PE2 by a protection PW, thus these devices constitute an MPLS network which provides PW transport services between ONUs and a CE.

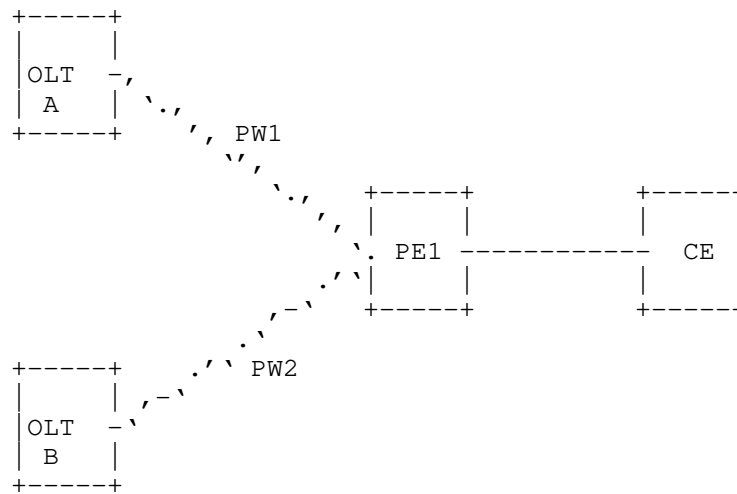


Figure 2 An MPLS Network with a Single PE

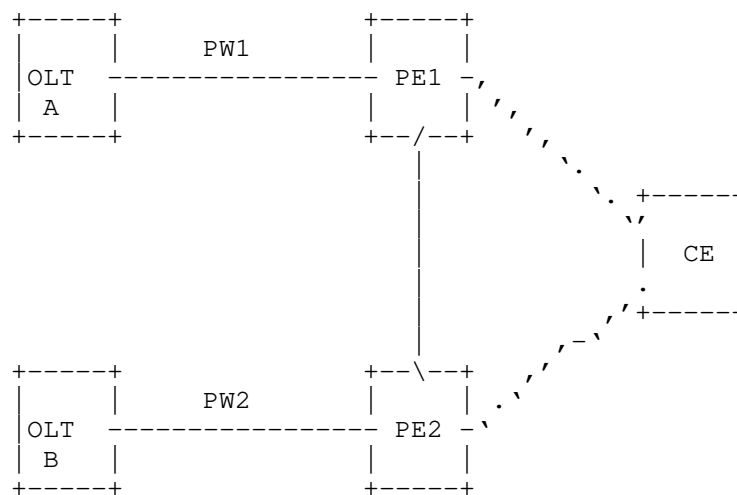


Figure 3 An MPLS Network with Dual-homing PEs

Faults may be encountered in PON access links, or in the MPLS network (including the working OLT). Procedures for these cases are described in this section (it is assumed that both OLTs and PEs are working in independent mode of PW redundancy [RFC6870]).

6.1. Protection procedure upon PON link failures

When a fault is detected on a working PON link, a working OLT MUST turn off its associated PON interface so that the protection trunk link to the protection OLT can be activated, then it MUST send an LDP fault notification message (i.e., with the status bit "Local AC (ingress) Receive Fault " being set) to its peer PE on the remote end of the PW. At the same time, the working OLT MUST send an ICCP message with PON State TLV with local PON Port State being set to notify the protection OLT of the PON fault.

Upon receiving a PON state TLV where Local PON Port state is set, a protection OLT MUST activate the protection PON link in the protection group, and advertise a notification message for the protection PW with the Preferential Forwarding status bit of active to the remote PE.

According to [RFC6870], the remote PE(s) can match the local and remote Preferential Forwarding status and select PW2 as the new active PW to which to send traffic.

6.2. Protection procedure upon PW failures

Usually MPLS networks have its own protection mechanism such as LSP protection or Fast Reroute (FRR). But in a link sparse access or aggregation network where protection for a PW is impossible in its LSP layer, the following PW layer protection procedures can be enabled.

When a fault is detected on its working PW (e.g., by VCCV BFD), a working OLT SHOULD turn off its associated PON interface and then send an ICCP message with PON State TLV with local PON Port State being set to notify the protection OLT of the PON fault.

Upon receiving a PON state TLV where Local PON Port state is set, the protection OLT MUST activate its PON interface to the protection trunk fiber. At the same time, the protection OLT MUST send a notification message for the protection PW with the Preferential Forwarding status bit of active to the remote PE, so that traffic can be switched to the protection PW.

6.3. Protection procedure upon the working OLT failure

As depicted in Fig. 2, a service is provisioned with a working PW and a protection PW, both PW terminated on PE1. If PE1 lost its

connection to the working OLT, it SHOULD send a LDP notification message on the protection PW with the Request Switchover bit set.

Upon receiving a LDP notification message from its remote PE with the Request Switchover bit set, a protection OLT MUST activate its optical interface to the protection trunk fiber and activate the associated protection PW, so that traffic can be reliably switched to the protection trunk PON link and the protection PW.

In the case of Fig.3, PW-RED State TLV [ICCP] can be used by PE1 to notify PE2 the faults in all the scenarios, and PE2 operates the same as described in Section 5.1 to 5.3.

7. Security Considerations

Security considerations as described in [ICCP] apply.

8. IANA Considerations

These values are requested from the registry of "ICC RG parameter type":

0x00X0	PON Connect TLV
0x00X1	PON Disconnect TLV
0x00X2	PON Configuration TLV
0x00X3	PON State TLV
0x00X4	PON ONU Database Sync TLV

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
- [RFC6870] Muley, P., Aissaoui, M., "Pseudowire Preferential Forwarding Status Bit", RFC 6870, February 2013
- [ICCP] Martini, L. and et al, "Inter-Chassis Communication Protocol for L2VPN PE Redundancy", RFC 7275, June 2014

9.2. Informative References

- [RFC6456] Li, H., Zheng, R., and Farrel, A., "Multi-Segment Pseudowires in Passive Optical Networks", RFC 6456, November 2011
- [SEAMLESS] Leymann, N., and et al, "Seamless MPLS Architecture", draft-ietf-mpls-seamless-mpls-04, Work in progress
- [G983.1] ITU-T, "Broadband optical access systems based on Passive Optical Networks (PON)", ITU-T G.983.1, January, 2005
- [IEEE-1904.1] IEEE Std. 1904.1, "Standard for Service Interoperability in Ethernet Passive Optical Networks (SIEPON)", IEEE Computer Society, June, 2013
- [IEEE-802] IEEE Std. 802, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", IEEE Computer Society, December, 2001 with amendments
- [TR-221] BBF TR-221, "Technical Specifications for MPLS in Mobile Backhaul Networks", the Broadband Forum, October, 2011
- [SD-331] BBF SD-331, "Architecture and Technical Requirements for PON-Based Mobile Backhaul Networks", the Broadband Forum, Work in progress

10. Acknowledgments

The authors would like to thank Min Ye, Hongyu Li, Wei Lin, Xifeng Wan, Yannick Legoff and Shrinivas Joshi for their valuable discussions and comments.

Authors' Addresses

Yuanlong Jiang
Huawei Technologies Co., Ltd.
Bantian, Longgang district
Shenzhen 518129, China
Email: jiangyuanlong@huawei.com

Yong Luo
Huawei Technologies Co., Ltd.
Bantian, Longgang district
Shenzhen 518129, China
Email: dennis.luoyong@huawei.com

Edwin Mallette
Bright House Networks
4145 S. Falkenburg Road
Tampa, FL 33578 USA
Email: edwin.mallette@gmail.com

Chengbin Shen
China Telecom
Email: shencb@sttri.com.cn

Yimin Shen
Juniper Networks
10 Technology Park Drive
Westford, MA 01886, USA
Email: yshen@juniper.net

Weiqiang Cheng
China Mobile
No.32 Xuanwumen West Street
Beijing 100053, China
Email: chengweiqiang@chinamobile.com

Guangtao Zhou
China Unicom
No.9 Shouti South Road
Beijing 100048, China
Email: zhouguangtao@chinaunicom.cn

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 2, 2015

H. van Helvoort
L. Andersson
A. Malis
Huawei Technologies Co., Ltd
J. Shin
SK Telecom
L. Wang
China Mobile
A. D'Alessandro
Telecom Italia
July 1, 2014

Encapsulation for PSC for Multi-Segment Pseudowires
draft-shawam-pwe3-ms-pw-protection-00.txt

Abstract

In RFC 6378 'MPLS Transport Profile (MPLS-TP) Linear Protection', as well as in the later updates of this RFC, the Protection State Coordination (PSC) protocol was defined for MPLS LSPs only. This draft extends RFC 6378 to be applicable for pseudowires as well.

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 January 2, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Encapsulation of the PSC protocol for Pseudowires	2
3. Security Considerations	3
4. IANA Considerations	3
5. Acknowledgements	3
6. Normative References	3
Authors' Addresses	3

1. Introduction

In RFC 6378 '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' [I-D.ietf-mpls-psc-updates], the Protection State Coordination (PSC) protocol was defined for MPLS LSPs only.

This draft extends RFC 6378 to be applicable for pseudowires (PWs) as well. This is useful especially in the case of end-to-end static provisioned Multi-Segment PWs (MS-PWs) running over MPLS-TP where we can't rely on tunnel protection alone for end-to-end protection of PWs against switching PE (S-PE) failure.

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). Linear protection protects an LSP 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, it is possible to protect a link by a path. Likewise it is possible to protect a PW with a MS-PW.

From a PSC protocol point of view it is possible to view a PW as a single hop LSP, and a MS-PW as a multiple hop LSP. The PSC protocol will work just as specified in RFC 6378.

Thus the G-ACh carrying the PSC protocol information is placed in the label stack directly beneath the PW identifier.

3. Security Considerations

The security considerations defined for RFC 6378 apply to this document as well. As this is simply a re-use of RFC 6378, there are no new security considerations.

4. IANA Considerations

There are no requests for IANA actions in this document.

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

5. Acknowledgements

TBA

6. Normative References

[I-D.ietf-mpls-psc-updates]

Osborne, E., "Updates to MPLS Transport Profile Linear Protection", draft-ietf-mpls-psc-updates-06 (work in progress), May 2014.

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

[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.

Authors' Addresses

Huub van Helvoort
Huawei Technologies Co., Ltd

Email: huub.van.helvoort@huawei.com

Loa Andersson
Huawei Technologies Co., Ltd

Email: loa@mail01.huawei.com

Andrew G. Malis
Huawei Technologies Co., Ltd

Email: Andrew.Malis@huawei.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