

Network Working Group
Internet-Draft
Intended status: Standards Track

Y. Jiang, Ed.
Y. Luo
Huawei
E. Mallette, Ed.
Charter Communications
Y. Shen
Juniper Networks
W. Cheng
China Mobile
September 28, 2016

Expires: March 2017

**Multi-chassis Passive Optical Network (PON) Protection in MPLS
draft-ietf-pals-mc-pon-05**

Abstract

Multi-Protocol Label Switching (MPLS) is being extended to the edge of operator networks including the network access nodes. Separately network access nodes such as Passive Optical Network (PON) Optical Line Terminations (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 specifies the Inter-Chassis Communication Protocol (ICCP) extension to support it.

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/1id-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 March 28, 2017.

Copyright Notice

Copyright (c) 2016 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	3
1.1.	Conventions used in this document	5
1.2.	Terminology	5
2.	ICCP Protocol Extensions	6
2.1.	Multi-chassis PON Application TLVs	6
2.1.1.	PON Connect TLV	6
2.1.2.	PON Disconnect TLV	7
2.1.3.	PON System Configuration TLV	8
2.1.4.	PON State TLV	9
3.	Considerations on PON ONU Database Synchronization	10
4.	Multi-chassis PON application procedures	10
4.1.	Protection procedure upon PON link failures	12
4.2.	Protection procedure upon PW failures	12
4.3.	Protection procedure upon the working OLT failure	13
5.	Security Considerations	13
6.	IANA Considerations	14
7.	References	14
7.1.	Normative References	14
7.2.	Informative References	14
8.	Acknowledgments	15
	Contributors	15
	Authors' Addresses	16

1. Introduction

Multi-Protocol Label Switching (MPLS) is being extended to the edge of operator networks, as is described in the Multi-Segment Pseudowires with Passive Optical Network (PON) access use case [[RFC6456](#)]. Combining MPLS with Optical Line Termination (OLT) access further facilitates a low cost multi-service convergence.

Tens of millions of Fiber-to-the-x (FTTx, x = H for home, P for premises, C for curb) 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 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 Long Term Evolution (LTE) small cells and Wi-Fi hotspots are deployed. PON is considered a viable low cost backhaul solution for these mobile services. Besides its high bandwidth and scalability, PON further provides frequency and time synchronization features, e.g., SyncE [[G.8261](#)] and IEEE 1588v2 [[IEEE-1588](#)] 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.

Unlike typical residential service where a single or handful of end-users hangs off 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 a point-to-point access portfolio.

Some optical layer 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 [[G.983.1](#)].

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 Optical Network Units (ONUs). This is different from the more complex and costly Tree 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 depicts a typical scenario of Trunk protection.

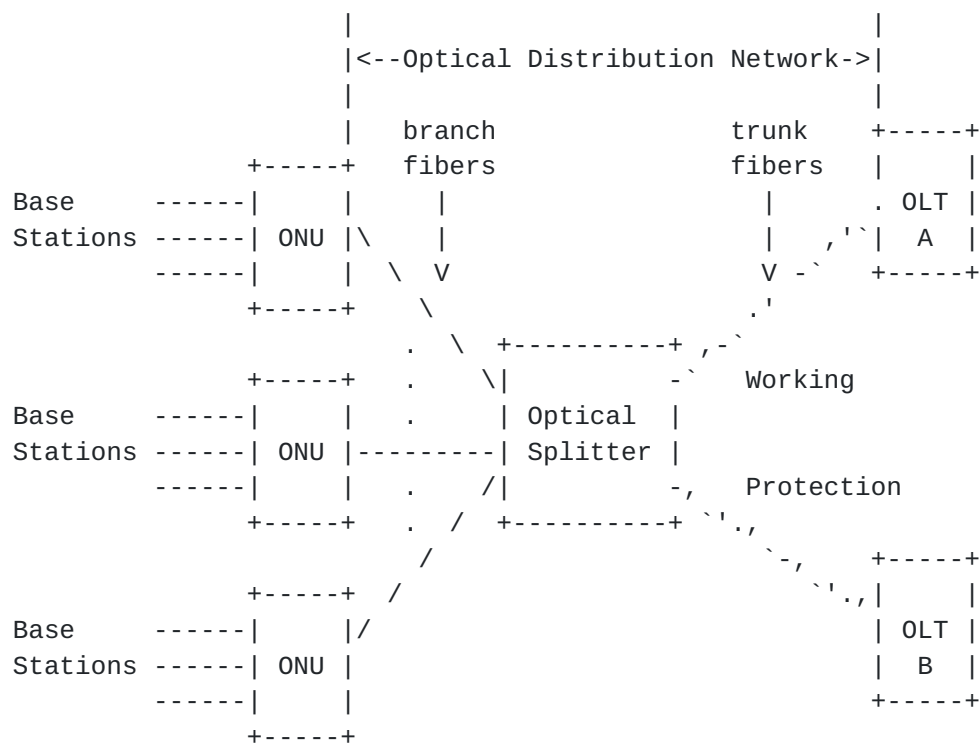


Figure 1 Trunk Protection Architecture in PON

Besides small cell backhaul, this protection architecture can also be applicable to other services, for example, Digital Subscriber Line (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) or a DOCSIS Remote PHY device [[remote-phy](#)], and it may further be attached with dozens of Customer Premise devices.

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

The PON architecture as depicted in Figure 1 can provide redundancy in its physical topology, however, all traffic including link Operation Administration and Maintenance (OAM) are blocked on the protection link which frustrates end to end protection mechanisms such as those specified in ITU-T G.8031 [[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 rapidly and reliably, especially when the OLTs also support MPLS.

Inter-Chassis Communication Protocol (ICCP) [[RFC7275](#)] provides a framework for inter-chassis synchronization of state and configuration data between a set of two or more Provider Edges (PEs). Currently ICCP only defines application specific messages for Pseudowire (PW) redundancy and Multi-Chassis LACP (mLACP), but it can be easily extended to support PON as an Attachment Circuit (AC) redundancy.

This document proposes the extension of ICCP to support Multi-chassis PON protection in MPLS.

[1.1.](#) 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](#)].

[1.2.](#) 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

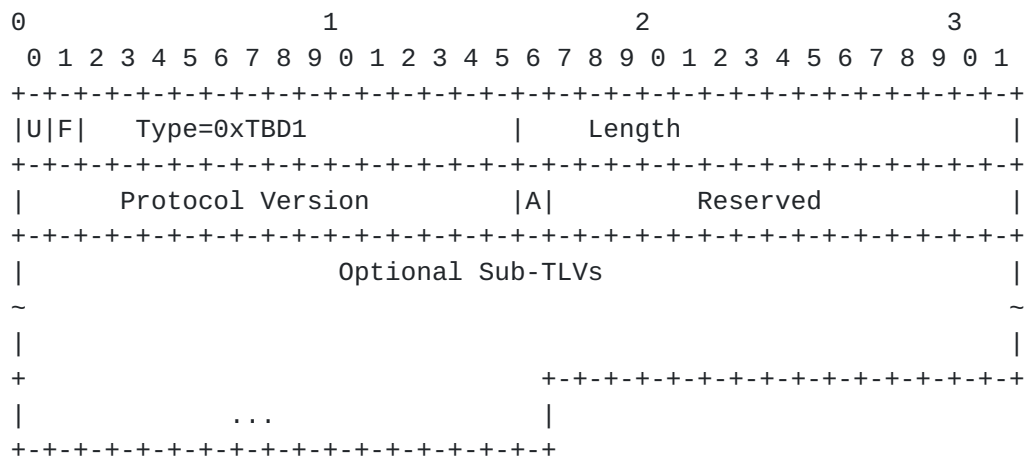
2. ICCP Protocol Extensions

2.1. Multi-chassis PON Application TLVs

A set of multi-chassis PON application Type-Length-Values (TLVs) are defined in the following sub-sections.

2.1.1. PON Connect TLV

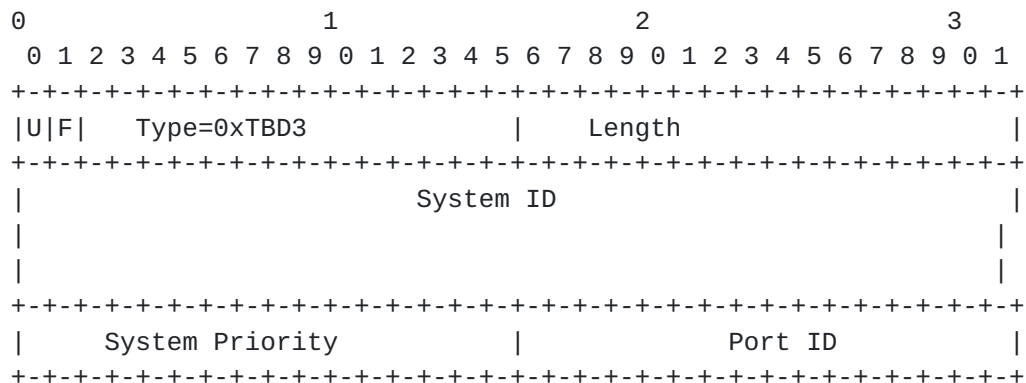
This TLV is included in the Redundancy Group (RG) Connect message to signal the establishment of PON application connection.



- U and F Bits, both are set to 0.
- Type, set to 0xTBD1 for "PON Connect TLV".
- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- Protocol Version, the version of this PON specific protocol for the purposes of inter-chassis communication. This is set to 0x0001.
- A Bit, Acknowledgement Bit. It MUST be set to 1 if the sender has received a PON Connect TLV from the recipient. Otherwise, set to 0.
- Reserved, Reserved for future use, and MUST be set to zero.
- Optional Sub-TLVs, there are no optional Sub-TLVs defined for this version of the protocol. The structure of Optional Sub-TLVs is defined as follows:

2.1.3. PON System Configuration TLV

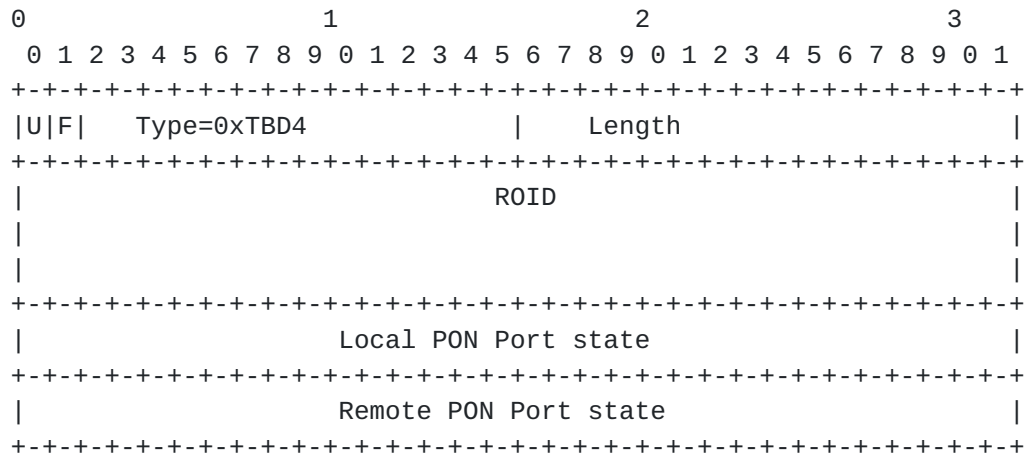
The "PON System Configuration TLV" is included in the "RG Application Data" message, and announces an OLT's system parameters to other members in the same RG.



- U and F Bits, both are set to 0.
- Type, set to 0xTBD3 for "PON System 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, a 2-octet value assigned by management or administration policy, the OLT with the numerically lower value of System Priority has the higher priority.
- Port ID, 2 octets PON Port ID.

2.1.4. 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 0xTBD4 for "PON State TLV"
- Length, Length of the TLV in octets excluding the U-bit, F-bit, Type, and Length fields.
- ROID, Redundant Object ID (ROID) as defined in [Section 4.3 of \[RFC7275\]](#).
- 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; 0 - in normal).
- Remote PON Port State, the status of the remote PON port as determined by the remote peer of the sending OLT (i.e., the sending PE). The last bit is defined as Fault indication of the PON Port associated with this PW (1 - in fault; 0 - in normal).

3. Considerations on 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 working and protection OLTs need to know about the protected ONUs. To enable service continuity a mechanism needs to be employed such that the operational state and significant configuration data of both the protected ONU and the services provisioned to it can be distributed to the working and protection OLT.

The specific ONUs configuration and operational data can be synchronized by some policy mechanism or provisioned in the management plane. Alternatively said synchronization could occur by some other signaling options. Describing how to synchronize the configuration objects associated with both protected ONU as well as the services constructed to the ONU (e.g. ONU MAC address, IPv4 addresses, IPv6 addresses, VLAN identifiers, etc.) is outside of the scope of this document.

4. 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 Customer Edge (CE), and the PWs can provide protection for each other.

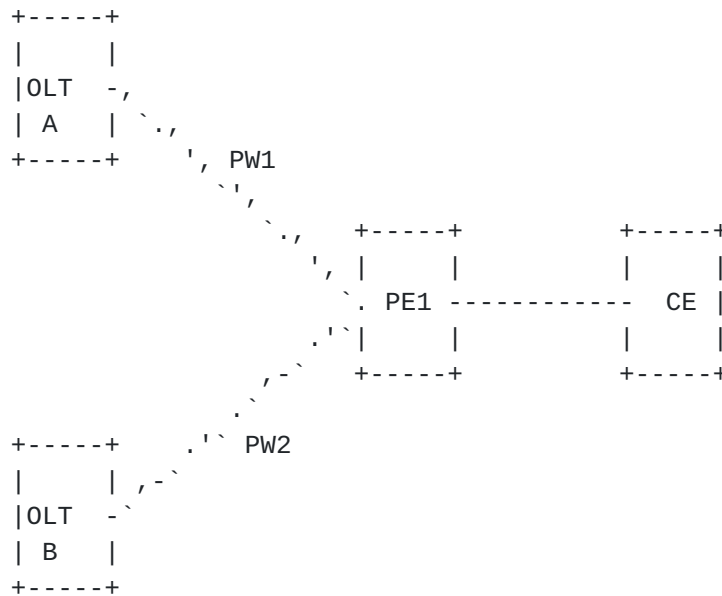


Figure 2 An MPLS Network with a Single PE

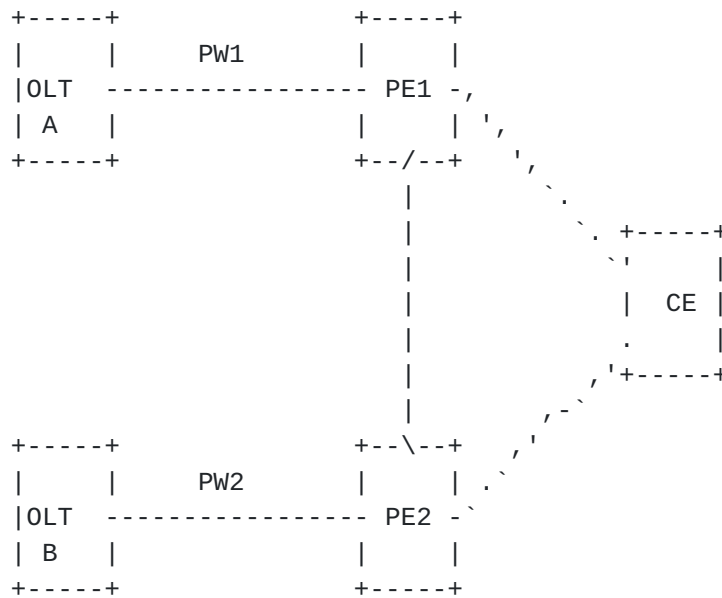


Figure 3 An MPLS Network with Dual-homing PEs

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 the independent mode of PW redundancy [[RFC6870](#)]).

4.1. Protection procedure upon PON link failures

When a fault is detected on a working PON link, a working OLT switches to the corresponding protection PON link attached with its protection OLT, i.e., the working OLT turns off its faulty PON interface so that the protection trunk link to its protection OLT can be activated. The working OLT then 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 over which data traffic is sent.

4.2. 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.

4.3. 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 an LDP notification message on the protection PW with the Request Switchover bit set.

Upon receiving an 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 as described in [Section 7.1 of \[RFC7275\]](#) 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.

5. Security Considerations

Similar to ICCP itself, this ICCP application SHOULD only be used in well-managed and highly monitored service provider PON access networks in a single administrative domain, including the implementation of rogue ONU attachment detection and mitigation via device authentication. Thus many of the security considerations as described in [\[RFC7275\]](#) apply here as well.

Again, similar to ICCP, activity on the attachment circuits may cause security threats or be exploited to create denial-of-service attacks. In many passive optical networks, the optical paths between OLT and ONUs traverse publicly accessible facilities including public attachments (e.g. telephone poles), which opens up the risk of excessive link bouncing by optical layer impairment. While ICCP for MC-PON interconnects in the MPLS domain and does not traverse the PON network, risks do include introduction of a malicious ONU which could cause, for example, excessive link bouncing. This link bouncing could result in increased ICCP exchanges similar to the malicious CE case described in [\[RFC7275\]](#). Operators of such networks should take additional care to restrict unauthorized ONUs and to limit the impact of link bouncing at the OLT, as these could result in service impairment.

6. IANA Considerations

The IANA maintains a top-level registry called "Pseudowire Name Spaces (PWE3)". It has a subregistry called "ICC RG Parameter Types". The following values are requested from this subregistry:

0xTBD1	PON Connect TLV
0xTBD2	PON Disconnect TLV
0xTBD3	PON Configuration TLV
0xTBD4	PON State TLV

[Note to IANA, to be removed by the RFC Editor: consecutive values in the IETF Review range are requested.]

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
- [RFC6870] Muley, P., Aissaoui, M., "Pseudowire Preferential Forwarding Status Bit", [RFC 6870](#), February 2013
- [RFC7275] Martini, L. et al, "Inter-Chassis Communication Protocol for L2VPN PE Redundancy", [RFC 7275](#), June 2014

7.2. Informative References

- [RFC6456] Li, H., Zheng, R., and Farrel, A., "Multi-Segment Pseudowires in Passive Optical Networks", [RFC 6456](#), November 2011
- [G.983.1] ITU-T, "Broadband optical access systems based on Passive Optical Networks (PON)", ITU-T G.983.1, January, 2005
- [G.8031] ITU-T, "Ethernet Linear Protection Switching", ITU-T G.8031, January, 2015
- [G.8261] ITU-T, "Timing and synchronization aspects in packet networks", ITU-T G.8261, August, 2013
- [IEEE-1588] IEEE Std. 1588, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Instrumentation and Measurement Society, July, 2008

- [IEEE-1904.1] IEEE Std. 1904.1, "Standard for Service Interoperability in Ethernet Passive Optical Networks (SIEPON)", IEEE Computer Society, June, 2013
- [TR-221] BBF TR-221, "Technical Specifications for MPLS in Mobile Backhaul Networks", <https://www.broadband-forum.org/technical/download/TR-221.pdf>, the Broadband Forum, October, 2011
- [remote-phy] CableLabs, "Remote PHY Specification", http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-R-PHY-I01_150615.pdf, June, 2015

8. Acknowledgments

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

Contributors

The following people made significant contributions to this document:

Chengbin Shen
China Telecom
1835 South Pudong Road
Shanghai 200122, China
Email: shencb@sttri.com.cn

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

Authors' Addresses

Yuanlong Jiang (Editor)
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 (Editor)
Charter Communications
4145 S. Falkenburg Road
Tampa, FL 33578 USA
Email: edwin.mallette@gmail.com

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