Network Working Group
Internet Draft
Category: Informational Track
Expires: January 2009

F. Jounay (Ed.)
P. Niger
France Telecom

Y. Kamite
NTT Communications

S. Delord
Uecomm

L. Wang
Telenor

G. Heron
BT

L. Martini
Cisco

R. Aggarwal
Juniper Networks

M. Bocci
M. Vigoureux
Alcatel-Lucent

L. Jin
Nokia Siemens

July 14, 2008

Requirements for Point-to-Multipoint Pseudowire

draft-jounay-pwe3-p2mp-pw-requirements-02.txt

Status of this Memo

Abstract

This document presents a set of requirements for providing an unidirectional Point-to-Multipoint PWE3 (Pseudowire Emulation Edge to Edge) emulation. The requirements identified in this document are related to architecture, signaling and maintenance aspects of a Point-to-Multipoint PW operation. They are proposed as guidelines for the standardization of such mechanisms. Among other potential applications Point-to-Multipoint PWs SHOULD be used to optimize the support of multicast services as defined in the Layer 2 Virtual Private Network working group.

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].

Table of Contents

1. Introduction

1.1. Problem Statement

As defined in the PWE3 WG charter, a Pseudowire (PW) emulates a point-to-point bidirectional link over an IP/MPLS network, and provides a single service which is perceived by its user as an unshared link or circuit of the chosen service. A Pseudowire is used to transport non IP traffic (e.g. Ethernet, TDM, ATM, and FR) in an IP/MPLS-based PSN (Packet Switched Network). PWE3 operates "edge to edge" to provide the required connectivity between the two endpoints of the PW.

The P2MP topology mentioned in [VPMS REQ] and required to provide P2MP L2VPN services can be achieved via a P2MP PW. The use of PW becomes necessary for some P2MP services requiring specific encapsulation capabilities. This could be achieved using a set of point to point PWs, with traffic replication on the PE, but faces obvious bandwidth limitation issues, as traffic is carried multiple time on shared links.

This document defines the use of a Point-to-Multipoint PW (P2MP PW). A Point-to-Multipoint (P2MP) Pseudowire (PW) is a mechanism that emulates the essential attributes of a unidirectional P2MP Telecommunications service such as P2MP ATM over PSN. One of the applicabilities of a P2MP PW is to deliver a non-IP multicast service that carries multicast frames from a multicast source to one or more multicast receivers. The required functions of P2MP PWs include encapsulating service-specific PDUs arriving at an ingress Attachment Circuit (AC), and carrying them across a tunnel to one or more egress ACs, managing their timing and order, and any other operations required to emulate the behavior and characteristics of the service as faithfully as possible.

P2MP PWs extend the PWE3 architecture [RFC3985] to offer a P2MP Telecommunications service. They follow the PWE3 architecture as

described in [RFC3985] with modifications as outlined in this document. One notable difference between point-to-point (P2P) PWs as outlined in [RFC3985] and P2MP PWs is that the former emulate a

bidirectional service whereas the latter emulate a unidirectional service.

This document aims at defining the associated requirements related to the P2MP PW operation (e.g. setup and maintenance, protection, scalability, etc).
It is intended that solutions that specify procedures and protocols or extensions to existing protocols for the signaling of P2MP Pseudowire satisfy these requirements.

1.2. Scope of the document

The document describes the P2MP PW Reference Model architectures and outlines specific signaling requirements for the set up and maintenance of a P2MP PW. The requirements are divided into two parts, i.e. those applicable in a Single-Segment topology and those applicable in a Multi-Segment topology. For other aspects of P2MP PW implementation like packet processing, maintenance, etc, the document refers to [RFC3916].

Some P2MP PW requirements are derived from the signaling requirements for P2MP Traffic-Engineered MPLS Label Switched Paths [RFC4461].

2. Definition

2.1. Acronyms

P2P: Point-to-Point

P2MP: Point-to-Multipoint

PW: Pseudowire

SS-PW: Single-Segment Pseudowire

MS-PW: Multi-Segment Pseudowire

2.2. Terminology

This document uses terminology described in [MS-PW REQ], [MS-PW ARCH], [SEG PW].

It also introduces additional terms needed in the context of unidirectional P2MP PW.

P2MP PW, (also referred as PW Tree)

Point-to-Multipoint Pseudowire. A PW attached to a source used to distribute L1/L2 format traffic to a set of one or more receivers (or leaves). The P2MP PW is unidirectional.

P2MP SS-PW

Point-to-Multipoint Single-Segment Pseudowire. A single segment P2MP PW set up between the PE attached to the source and the PEs attached to the receivers. The P2MP SS-PW relies on a P2MP LSP as PSN tunnel.

P2MP MS-PW

Point-to-Multipoint Multi-Segment Pseudowire. A multi-segment P2MP PW represents an End-to-End PW segmented by means of S-PEs which are in charge of switching the PW label. Each segment can rely on either P2P LSP or a P2MP LSP as PSN tunnel.

Ingress PE

P2MP PW Ingress Provider Edge. Router attached to a Customer Equipment (traffic source) via an Attachment Circuit (AC). In a MS-PW architecture the term used is Ingress T-PE.

Egress PE

P2MP PW Egress Provider Edge. Router attached to a set of on or more Customer Equipments (traffic receivers or leaves) via a set of one or more Attachment Circuits (AC). In a MS-PW architecture the term used is Egress T-PE.

Branch S-PE

The branch S-PE is only defined and required in the context of MS-PW. The branch S-PE has one upstream PW segment and one or several downstream PW segments.

3. P2MP SS-PW Requirements

3.1. P2MP SS-PW Reference Model

A unidirectional P2MP SS-PW provides a Point-to-Multipoint connectivity from an Ingress PE connected to a traffic source to at least two Egress PEs connected to traffic receivers. The PW endpoints connect the PW to its attachment circuits (AC). As for a P2P PW, an AC can be a Frame Relay DLC, an ATM VP/VC, an Ethernet port, a VLAN, a HDLC link on a physical interface.

Figure 1 describes the P2MP SS-PW reference model which is derived from [RFC3985] to support P2MP emulated services.

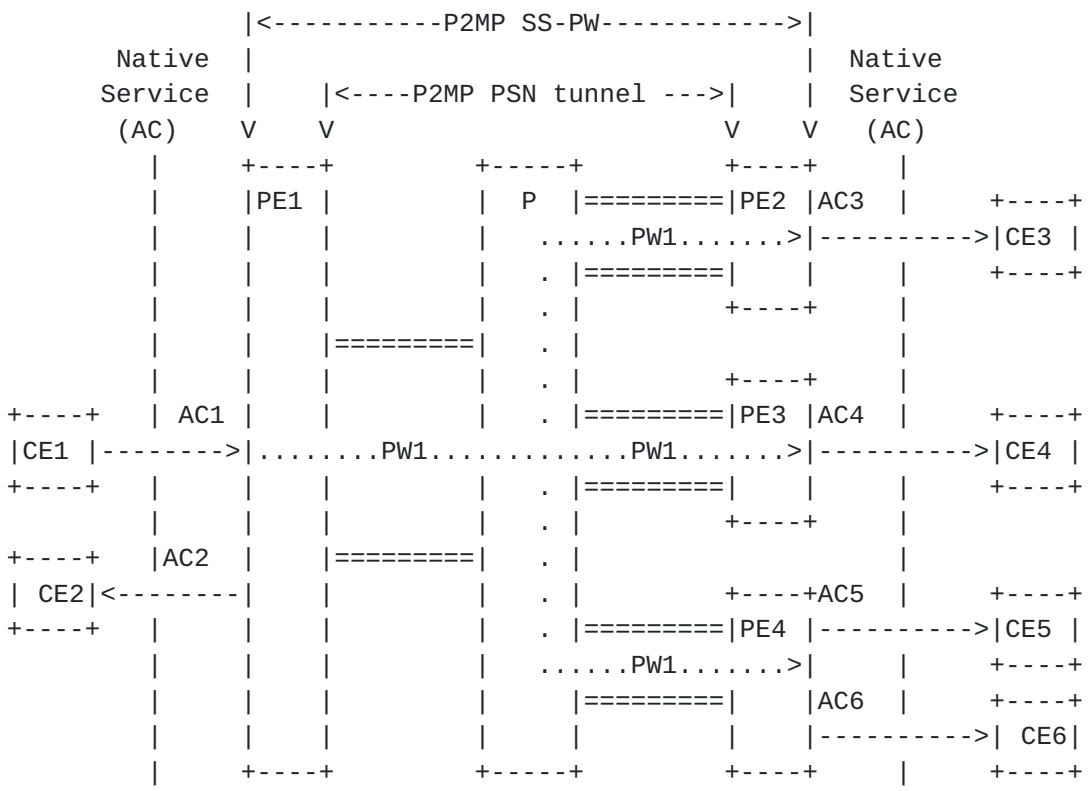

Figure 1 P2MP SS-PW Reference Model

This architecture applies to the case where a P2MP PSN tunnel extends between edge nodes of a single PSN domain to transport a unidirectional P2MP PW with endpoints at these edge nodes.
In this model a single copy of each PW packet is sent over the P2MP PSN tunnel and is received by all Egress PEs due to the P2MP nature of the PSN tunnel. P Router is joining P2MP PSN tunnel operation but is free from signaling of P2MP PW. P2MP PW operation is associated with PE1, PE2, PE3 and PE4.
An AC attached to P2MP PW MUST be configured as "sender" or "receiver" not both. Any AC is associated with the role of either sending side (Tx) or receiving side (Rx) from the view of CE. Thus every AC deals with unidirectional traffic. In Figure 1, AC1 is configured as sending sides while AC2, AC3, AC4, AC5 and AC6 are as receiving sides.

Referring to Figure 1, CE2, CE5 and CE6 MAY want to receive multicast traffic from CE1. P2MP SS-PW (and P2MP MS-PW outlined in section 4) solution MUST support such an operational case where one or more ACs are connected to the same PE and local replication is needed. A PE providing P2MP PW MUST support the following functions:
- Ingress PE MUST support traffic replication over its directly connected ACs toward receiver CEs if necessary, in addition to PSN transport.

- Egress PE MUST support traffic replication over its directly connected ACs toward receiver CEs if necessary.

3.2. P2MP SS-PW Underlying Layer

The P2MP SS-PW implies an underlying P2MP PSN tunnel. Figure 2 gives an example of P2MP SS-PW topology relying on a P2MP LSP. The PW tree is composed of one Ingress PE (i1) and several Egress PEs (e1, e2, e3, e4).

The P2MP PSN MAY be signaled with P2MP RSVP-TE [RFC4875] or MLDP [MLDP].

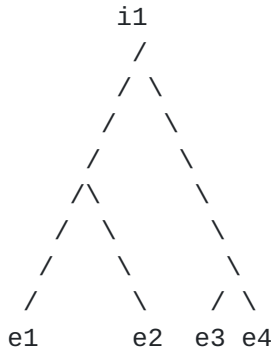

Figure 2 Example of P2MP Underlying Layer for P2MP SS-PW

The P2MP PW MUST be supported over only one P2MP PSN tunnel. This P2MP PSN tunnel MUST be able to serve more than one P2MP PW.

3.3. P2MP SS-PW Signaling Requirements

3.3.1. PW type mismatch

As for P2P PW, the ACs configured at Ingress PE and Egress PEs of a P2MP PW MUST be of the same PW type [RFC4446]. In case of a different type, the passive PE (Ingress or Egress PE, depending on the signaling process) MUST support mechanisms to reject attempts to establish the P2MP PW.

3.3.2. Interface Parameters sub-TLV

Some interface parameters [RFC4446] related to the AC capability have been defined according to the PW type and are signaled during the PW setup from the Egress PE to the Ingress PE.
This mechanism used for the P2P PW setup SHOULD be enhanced for P2MP PW setup so as to ascertain that AC at the Egress PE is capable to support traffic coming from AC at the Ingress PE.

Note that the signaling of such parameters is not mandatory and can also be configured statically at PW endpoints.

When the interface parameters are signaled, the Ingress PE SHOULD take the decision to accept or not an Egress PE in the PW tree based on the interface parameters advertised by the Egress PE. For that purpose the Ingress PE MUST be configured with a threshold value of the advertised interface parameters. E.g. for some interface parameters (e.g. MTU size (Ethernet), number max of concatenated ATM cells, etc), the parameters advertised by the Egress PE MUST be at least superior or equal to those configured at the Ingress PE. For other like CEP/TDM Payload bytes (TDM), the value MUST match exactly at the Ingress and Egress PEs.

Note that when using an Ethernet P2MP PW with the Tag mode, the interface parameter VLAN requested MUST be disabled, since a given Egress PE requesting a VLAN marking at the Ingress PE will impose this value to all Egress PEs belonging to the PW tree.

Note that a translation (VPI/VCI or VLAN service delimiter) SHOULD be enabled only at the Egress PE.

3.3.3. Leaf Grafting/Pruning

Once the PW tree is setup, the solution MUST allow the addition or removal of a leaf, or a subset of leaves to/from the existing tree, without any impact on the PW tree (data and control planes) for the remaining leaves.
The addition or removal of a leaf SHOULD also lead to the P2MP PSN tunnel update accordingly. This MAY cause P2MP PSN tunnel to add or remove the corresponding leaf.

3.4. Failure Reporting and Processing

Since the underlying layer has an End-to-End P2MP topology between the Ingress PE and the Egress PEs, the failure reporting and processing procedures are implemented only on the edge nodes.

Failure events MAY cause one or more Egress PEs and associated leaves to become detached from the PW tree. These events MUST be reported to the Ingress PE, using appropriate out-band OAM messages.
The solution SHOULD allow the Ingress PE to be informed of Egress PEs and associated leaves failure for management purposes.

Based on these failure notifications the solution MUST allow the Ingress PE to update the remaining leaves of the PW tree.

- A solution MUST support in-band OAM mechanism to detect failures: unidirectional point-to-multipoint traffic failure. This SHOULD be realized by enhancing existing unicast PW methods, such as VCCV for

seamless and familiar operation.

- In case of failure, it SHOULD correctly report which leaf PEs are affected. This SHOULD be realized by enhancing existing PW methods, such as LDP Notification for seamless and familiar operation. The notification message SHOULD include the type of fault (P2MP PW, AC or PSN tunnel).

- A solution MAY support OAM message mapping at PE if failure happens i.e., mapping between AC service OAM and P2MP PW OAM.

3.5. Protection and Restoration

It is assumed that if recovery procedures are required the P2MP PSN tunnel will support standard MPLS-based recovery techniques (typically based on RSVP-TE). In that case a mechanism SHOULD be implemented to avoid race conditions between recovery at the PSN level and recovery at the PW level.

3.6. Scalability

The solution SHOULD scale at least as well as linearly with an increase in the number of Egress PEs.

3.7. Order of Magnitude

This section will be filled in a future version.

Number of Egress PE, TAII per Egress PE, dynamicity (Leaf Grafting/Pruning) required, etc.

4. P2MP MS-PW Requirements

4.1. P2MP MS-PW Pseudowire Reference Model

Figure 3 describes the P2MP MS-PW reference model which is derived from [MS-PW ARCH] to support P2MP emulated services.

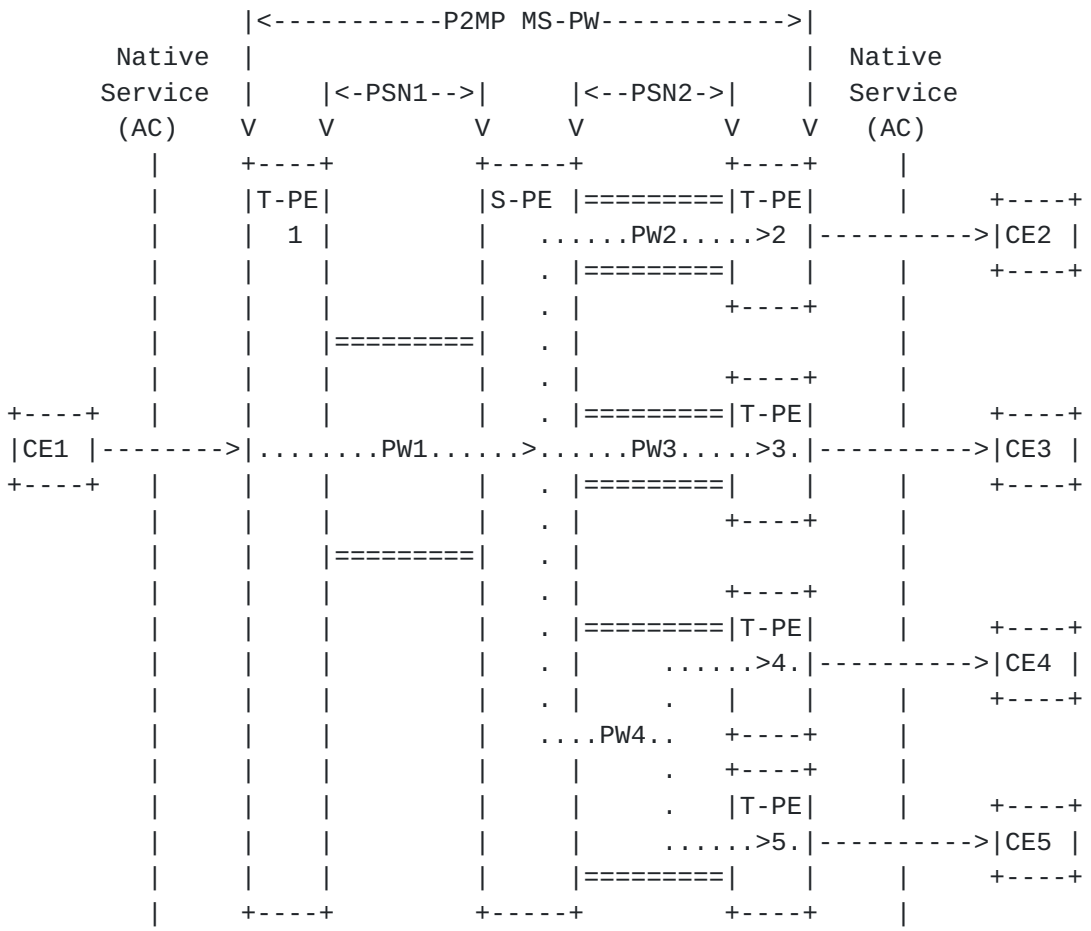

Figure 3 P2MP MS-PW Reference Model

Figure 3 extends the P2MP SS-PW architecture of Figure 1 to a multi-segment configuration. In a P2P MS-PW configuration as described in [MS-PW REQ] the S-PE is responsible to switch a MS-PW from one input segment to only one output segment, based on the PW identifier. Here in a P2MP MS-PW configuration the S-PE is responsible to switch a MS-PW from one input segment to one or several output segments.

Referring to Figure 3 T-PE1 is the Ingress T-PE and T-PE2, T-PE3, T-PE4 and T-PE5 are the Egress T-PEs. In the reference model, the Egress T-PEs are assumed to be located in the same PSN (PSN2), but it could be envisioned that each output PW is located in a different PSN

(PSN2, PSN3, PSN4). The S-PE plays the role of branch S-PE since it is in charge of switching simultaneously the input PW1 segment to the output PW2, PW3, PW4 segments.

Note that a P2MP MS-PW MAY obviously transit through more than one S-PE along its path.

Note that if the P2MP SS-PW case mandatory implies the use of P2MP PSN tunnel (underlying layer) between the edge nodes, the P2MP MS-PW does not imply such a requirement since each PW segment can be supported over a P2P PSN tunnel. However as we will see hereafter, the coexistence of both kind of PSN tunnel (P2P and P2MP) MUST be considered, as described in Figure 3 where the P2MP PW3 segment is supported over P2MP LSP.

Note that as for P2MP SS-PW, T-PE providing P2MP MS-PW MUST support the following functions:
- Ingress T-PE MUST support traffic replication over its directly connected ACs toward receiver CEs if necessary, in addition to PSN transport.
- Egress T-PE MUST support traffic replication over its directly connected ACs toward receiver CEs if necessary.

4.2. P2MP SS-PW Underlying Layer

Figure 4 describes an example of P2MP MS-PW topology relying on a combination of both P2P and P2MP LSPs as PSN tunnels. The PW tree is composed of one Ingress PE (i1) and several Egress PEs (e1, e2, e3, e4). The branch S-PEs are represented as b1, b2, b3, b4, b5. In that case the traffic replication along the path of the PW tree is performed at the PW level. For instance the branch S-PE b5 MUST replicate incoming packets or data received from b2 and send them to Egress T-PEs e3 and e4.

However giving the fact that some PW segments MAY be supported over a P2MP LSP, the traffic replication along the path of these PW segments can be performed as well at the underlying LSP level.

Figure 4 describes the case where each segment is supported over a P2P LSP except for the b1-b3 and b1-b4 segments which are conveyed over a P2MP LSP on this section.

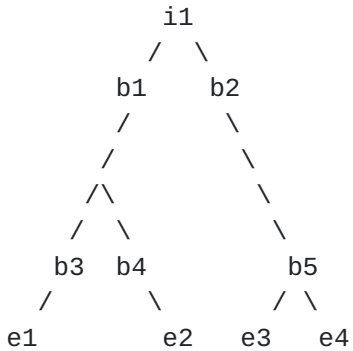

Figure 4 Example of P2P and P2MP underlying Layer for P2MP MS-PW

The P2MP PSN MAY be signaled with P2MP RSVP-TE [RFC4875] or MLDP [MLDP].

.

4.3. P2MP MS-PW Signaling Requirements

4.3.1. Dynamically Instantiated P2MP MS-PW

The PW tree could be statically configured at the T-PEs and each S-PE crossed. However it is RECOMMENDED that a solution provides the ability to dynamically setup a MS-PW tree, by allowing the MS-PW segments to be dynamically stitched.

During the PW tree setup, a branch S-PE SHOULD be capable to inform the upstream PEs, including the Ingress T-PE that a set of Egress T-PEs and associated leaves are not reachable.

4.3.2. P2MP MS-PW Setup Mechanisms

The requirements described in this section assume that dynamic setup of MS-PW segments allows the T-PE and S-PEs to dynamically signal MS-PW segments and stitch these segments in order to build the MS-PW tree.

It is RECOMMENDED that the solution provides various optimization options in the P2MP MS-PW construction (Traffic-Engineered P2MP MS-PW).

4.3.3. PW type mismatch

As described for P2MP SS-PW, the P2MP MS-PW requires ACs of the same PW type. Therefore the segments composing the P2MP MS-PW MUST be also of the same PW type [RFC4446]. The S-PE MAY only support switching PWs of the same PW type. In case of a different type, the passive PE (S-PE or T-PE) MUST support mechanisms to reject attempts to establish the P2MP MS-PW.

4.3.4. Interface Parameters sub-TLV

The section 3.3.2 is also relevant to P2MP MS-PW. The Egress T-PE MAY signal its AC' interface parameters to the Ingress T-PE so as to make sure that AC at the Egress T-PE is capable to support traffic coming from AC at the Ingress T-PE. In the P2MP MS-PW case, S-PEs MUST propagate correctly this information up to the Ingress T-PE.

4.3.5. Leaf Grafting/Pruning

Once the PW tree is setup, the solution MUST allow the addition or removal of a leaf, or a subset of leaves to/from the existing tree,

without any impact on the PW tree (data and control planes) for the remaining leaves.

4.3.6. Explicit Routing

The P2MP MS-PW signaling solution MUST provide a means of establishing arbitrary P2MP MS-PW, according to pre-computed and configured S-PE paths as well as dynamically computed S-PE paths on the Ingress PE.

To support setup of explicitly routed MS-PW tree, the signaling solution SHOULD support some source-based control that can explicitly define particular S-PE nodes as branch S-PEs for the PW tree.

The solution SHOULD let possible Explicit Path Loose Hops (to be defined). Therefore the P2MP MS-PW MAY be partially specified with only a subset of intermediate branch S-PEs.

4.4. Failure Reporting

The solution SHOULD rely on specific OAM mechanisms to detect a node (T-PE and S-PE) or segment failure of a PW tree. The solution SHOULD also support the ability to inform the Ingress T-PE of the failure as well as to indicate the identity of affected Egress T-PEs and associated leaves.

Based on these failure notifications the solution MUST allow the Ingress T-PE to update the remaining Egress PEs and associated leaves of the PW tree.

- A solution MUST support in-band OAM mechanism to detect failures: unidirectional point-to-multipoint traffic failure. This SHOULD be realized by enhancing existing unicast PW methods, such as VCCV for seamless and familiar operation.

- In case of failure, it SHOULD correctly report which leaf T-PEs and branch S-PEs are affected. This SHOULD be realized by enhancing existing unicast PW methods, such as LDP Notification for seamless and familiar operation. The notification message SHOULD include the type of fault (P2MP PW, AC or PSN tunnel).

- A solution MAY support OAM message mapping at T-PE if failure happens i.e., mapping between AC service OAM and P2MP PW OAM. (Need more discussion: in particular, when upstream T-PE AC fails, it can be mapped to all downstream connection. Meanwhile downstream T-PE AC failure does not impose other T-PEs AC.)

4.5. Protection and Restoration

The solution SHOULD provide mechanisms to recover as fast as possible following a failure event. The fast protection/recovery is typically dedicated to P2MP applications sensitive to traffic disruption.

Considering (i) a source-initiated PW tree setup and (ii) that a local repair (PSN-tunnel or PW segment-based) is not feasible after a failure event and that (iii) the PE upstream to the failure receives by means of OAM mechanisms a message indicating that a subset of Egress T-PEs are detached from the PW tree, the solution SHOULD allow the upstream PE to re-compute the path to those particular Egress T-PEs. If the upstream PE failed to compute an alternative path, the procedure SHOULD be propagated upstream until the Ingress-PE is reached.

It is also assumed that recovery procedures can be implemented at the underlying P2P or P2MP LSP layer, using standard MPLS-based recovery techniques. These procedures could be used to provide faster recovery time in case of link or node failure affecting this layer.

A mechanism SHOULD be implemented to avoid race conditions between recovery at the PSN level and recovery at the PW level.

4.6. Scalability

In definition of solution for P2MP MS-PW a particular attention MUST dedicated to scalability.

The solution MUST be designed to scale as well as linearly with an increase in the number of leaves, Egress T-PEs, branch S-PEs. The scalability issues MUST be addressed for the control plane (e.g. addressing of PW endpoints, number of signaling sessions, etc) and for data plane (e.g. duplication of PW segments, OAM mechanism, etc).

4.7. Order of Magnitude

This section will be filled in a future version.

Number of Egress T-PE per tree, TAII per Egress T-PE, S-PE crossed, replication supported per S-PE, dynamicity (Leaf Grafting/Pruning) required, etc.

5. Manageability considerations

The solution SHOULD provide a simple provisioning procedure to build

a P2MP SS-PW or a P2MP MS-PW.

6. Backward Compatibility

The solution SHOULD be completely backward compatible with the current PW standards. The solution SHOULD take into account the capability advertisement and negotiation procedures for the PEs implementing P2MP PW endpoints.

Implementation of OAM mechanisms also implies the advertisement of PE capabilities to support specific OAM features. The solution MAY allow advertising P2MP PW OAM capabilities.

A solution MUST NOT allow PW connection with non-compliant PEs. It MUST have a mechanism to report an error for non-compliant PEs. In this case, it SHOULD report which PE (S-PE and T-PEs) are not compliant.

In some cases, upstream traffic is required from downstream CE to upstream CE.
A solution SHOULD allow co-existing operation with point-to-point PW that provides upstream connection.
In particular, it is expected to be allowed that the same ACs are shared between downstream and upstream direction. For downstream, a CE receives from its connected AC traffic originated by the ingress PE transported over a P2MP PW. For upstream, the CE MAY also send over the same AC traffic destinated to the same remote PE transported over point-to-point PW.

7. Security Considerations

This section will be added in a future version.

8. IANA Considerations

This draft does not define any new protocol element, and hence does not require any IANA action.

9. Acknowledgments

The authors thank the contributors of [RFC4461] since the structure and content of this document were, for some sections, largely inspired by [RFC4461].

Many thanks to JL Le Roux and A. Cauvin for the discussions, comments and support.

10. References

10.1. Normative References

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

[RFC3916] McPherson, D.,Pate, P., Xiao, X., "Requirements for Pseudo-Wire Emulation Edge-to-Edge", September 2004

[RFC3985] Bryant, S., Pate, P. "PWE3 Architecture", March 2005

[RFC4461] Aggarwal, R., Farrel, A., Jork, M., Kamite, Y., Kullberg, A., Le Roux, JL., Malis, A., Papadimitriou, D., Vasseur, JP., Yasukawa, S., "Signaling Requirements for P2MP TE MPLS LSPs",April 2006

[RFC4875] Aggarwal, R., Papadimitriou, D., Yasukawa, S., "Extensions to RSVP-TE for Point-to-Multipoint TE LSPs", MAY 2007

[RFC4446] Martini, L. "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", April 2006

10.2. Informative References

[MS-PW REQ] Bitar, N., Bocci, M., and Martini, L., "Requirements for inter domain Pseudo-Wires", Internet Draft, draft-ietf-pwe3-ms-pw-requirements-07.txt, June 2008

[MS-PW ARCH] Bocci, M., and Bryant, S.,T., " An Architecture for Multi-Segment Pseudo Wire Emulation Edge-to-Edge", Internet Draft, draft-ietf-pwe3-ms-pw-arch-04.txt, June 2008

[SEG PW] Martini et al, "Segmented Pseudo Wire", Internet Draft, draft-ietf-pwe3-segmented-pw-08.txt, June 2008

[MLDP] Minei, I., Wijnands, I., Thomas, B., "Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths", Internet Draft, draft-ietf-mpls-ldp-p2mp-05, June 2008

[VPMS REQ] Kamite, Y., Jounay, F. "Framework and Requirements for Virtual Private Multicast Service (VPMS)", Internet Draft, draft-kamite-l2vpn-vpms-frmwk-requirements-00,

Author's Addresses

Frederic Jounay
France Telecom
2, avenue Pierre-Marzin
22307 Lannion Cedex
FRANCE
Email: frederic.jounay@orange-ftgroup.com

Philippe Niger
France Telecom
2, avenue Pierre-Marzin
22307 Lannion Cedex
FRANCE
Email: philippe.niger@orange-ftgroup.com

Yuji Kamite
NTT Communications Corporation
Tokyo Opera City Tower
3-20-2 Nishi Shinjuku, Shinjuku-ku
Tokyo 163-1421
Japan
Email: y.kamite@ntt.com

Luca Martini
Cisco Systems, Inc.
9155 East Nichols Avenue, Suite 400
Englewood, CO, 80112
EMail: lmartini@cisco.com

Giles Heron
Tellabs
Abbey Place
24-28 Easton Street
High Wycombe
Bucks
HP11 1NT
UK
EMail: giles.heron@tellabs.com

Simon Delord
Uecomm
658 Church St
Richmond, VIC, 3121, Australia
E-mail: sdelord@uecomm.com.au

Lei Wang
Telenor

Snaroyveien 30
Fornebu 1331
Norway
Email: lei.wang@telenor.com

Rahul Aggarwal
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089
Email: rahul@juniper.net

Martin Vigoureux
Alcatel-Lucent France
Route de Villejust
91620 Nozay
FRANCE
Email: martin.vigoureux@alcatel-lucent.fr

Matthew Bocci
Alcatel-Lucent Telecom Ltd,
Voyager Place
Shoppenhangers Road
Maidenhead
Berks, UK
E-mail: matthew.bocci@alcatel-lucent.co.uk

Lizhong JIN
Nokia Siemens Networks
Building 89, 1122 North QinZhou Road,
Shanghai, 200211, P.R.China
Email: lizhong.jin@nsn.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary

rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement