Internet Engineering Task Force (IETF)
Request for Comments: 6718
Category: Informational
ISSN: 2070-1721

P. Muley
M. Aissaoui
M. Bocci
Alcatel-Lucent

August 2012

Pseudowire Redundancy

Abstract

This document describes a framework comprised of a number of scenarios and associated requirements for pseudowire (PW) redundancy. A set of redundant PWs is configured between provider edge (PE) nodes in single-segment PW applications or between terminating PE (T-PE) nodes in multi-segment PW applications. In order for the PE/T-PE nodes to indicate the preferred PW to use for forwarding PW packets to one another, a new PW status is required to indicate the preferential forwarding status of active or standby for each PW in the redundant set.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The objective of pseudowire (PW) redundancy is to maintain connectivity across the packet switched network (PSN) used by the emulated service if a component in the path of the emulated service fails or a backup component is activated. For example, PW redundancy will enable the correct PW to be used for forwarding emulated service packets when the connectivity of an attachment circuit (AC) changes due to the failure of an AC or when a pseudowire (PW) or packet switched network (PSN) tunnel fails due to the failure of a provider edge (PE) node.

PW redundancy uses redundant ACs, PEs, and PWs to eliminate single points of failure in the path of an emulated service. This is achieved while ensuring that only one path between a pair of customer edge (CE) nodes is active at any given time. Mechanisms that rely on more than one active path between the CEs, e.g., 1+1 protection switching, are out of the scope of this document because they may require a permanent bridge to provide traffic replication as well as support for a 1+1 protection switching protocol in the CEs.

Protection for a PW segment can be provided by the PSN layer. This may be a Resource Reservation Protocol with Traffic Engineering (RSVP-TE) label switched path (LSP) with a fast-reroute (FRR) backup or an end-to-end backup LSP. These mechanisms can restore PSN connectivity rapidly enough to avoid triggering protection by PW redundancy. PSN protection mechanisms cannot protect against the failure of a PE node or the failure of the remote AC. Typically, this is supported by dual-homing a CE node to different PE nodes that provide a pseudowire emulated service across the PSN. A set of PW mechanisms that enables a primary and one or more backup PWs to terminate on different PE nodes is therefore required. An important requirement is that changes occurring on the dual-homed side of the network due to the failure of an AC or PE are not propagated to the ACs on the other side of the network. Furthermore, failures in the PSN are not propagated to the attached CEs.

In cases where PSN protection mechanisms are not able to recover from a PSN failure or where a failure of a switching PE (S-PE) may occur, a set of mechanisms that supports the operation of a primary and one or more backup PWs via a different set of S-PEs or diverse PSN tunnels is therefore required. For multi-segment PWs (MS-PWs), the paths of these PWs are diverse in that they are switched at different S-PE nodes.

In both of these cases, PW redundancy is important to maximize the resiliency of the emulated service. It supplements PSN protection techniques and can operate in addition to or instead of those techniques when they are not available.

This document describes a framework for these applications and associated operational requirements. The framework utilizes a new PW status, called the 'Preferential Forwarding Status' of the PW. This is separate from the operational states defined in RFC 5601 [RFC5601]. The mechanisms for PW redundancy are modeled on general protection switching principles.

2. Terminology

- Up PW: A PW that has been configured (label mapping exchanged between PEs) and is not in any of the PW or AC defect states represented by the status codes specified in [RFC4446]. Such a PW is available for forwarding traffic.

- Down PW: A PW that either has not been fully configured or has been configured and is in any one of the PW or AC defect states specified in [RFC4446]. Such a PW is not available for forwarding traffic.

- Active PW: An up PW used for forwarding Operations, Administration, and Maintenance (OAM) as well as user-plane and control-plane traffic.

- Standby PW: An up PW that is not used for forwarding user traffic but may forward OAM and specific control-plane traffic.

- PW Endpoint: A PE where a PW terminates on a point where native service processing is performed, e.g., a single-segment PW (SS-PW) PE, a multi-segment pseudowire (MS-PW) terminating PE (T-PE), or a hierarchical Virtual Private LAN Service (VPLS) MTU-s or PE-rs.

- Primary PW: The PW that a PW endpoint activates (i.e., uses for forwarding) in preference to any other PW when more than one PW qualifies for the active state. When the primary PW comes back up after a failure and qualifies for the active state, the PW endpoint always reverts to it. The designation of primary is performed by local configuration for the PW at the PE and is only required when revertive behavior is used and is not applicable when non-revertive protection switching is used.

- Secondary PW: When it qualifies for the active state, a secondary PW is only selected if no primary PW is configured or if the configured primary PW does not qualify for active state (e.g., is down). By default, a PW in a redundancy PW set is considered secondary. There is no revertive mechanism among secondary PWs.

- Revertive protection switching: Traffic will be carried by the primary PW if all of the following is true: it is up, a wait-to-restore timer expires, and the primary PW is made the active PW.

- Non-revertive protection switching: Traffic will be carried by the last PW selected as a result of a previous active PW entering the operationally down state.

- Manual selection of a PW: The ability to manually select the primary/secondary PWs.

- MTU-s: A hierarchical virtual private LAN service multi-tenant unit switch, as defined in RFC 4762 [RFC4762].

- PE-rs: A hierarchical virtual private LAN service switch, as defined in RFC 4762.

- n-PE: A network-facing provider edge node, as defined in RFC 4026 [RFC4026].

- 1:1 protection: One specific subset of a path for an emulated service, consisting of a standby PW and/or AC, protects another specific subset of a path for the emulated service. User traffic is transmitted over only one specific subset of the path at a time.

- N:1 protection: N specific subsets of paths for an emulated service, consisting of standby PWs and/or ACs, protect another specific subset of the path for the emulated service. User traffic is transmitted over only one specific subset of the path at a time.

- 1+1 protection: One specific subset of a path for an emulated service, consisting of a standby PW and/or AC, protects another specific subset of a path for the emulated service. Traffic is permanently duplicated at the ingress node on both the currently active and standby subsets of the paths.

This document uses the term 'PE' to be synonymous with both PEs as per RFC 3985 [RFC3985] and T-PEs as per RFC 5659 [RFC5659].

This document uses the term 'PW' to be synonymous with both PWs as per RFC 3985 and SS-PWs, MS-PWs, and PW segments as per RFC 5659.

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Reference Models

The following sections show the reference architecture of the PE for PW redundancy and the usage of the architecture in different topologies and applications.

3.1. PE Architecture

Figure 1 shows the PE architecture for PW redundancy when more than one PW in a redundant set is associated with a single AC. This is based on the architecture in Figure 4b of RFC 3985 [RFC3985]. The forwarder selects which of the redundant PWs to use based on the criteria described in this document.

```
              +----------------------------------------+
              |               PE Device                |
              +----------------------------------------+
     Single   |                 |        Single        | PW Instance
      AC      |                 +     PW Instance      X<===========>
              |                 |                      |
              |                 |----------------------|
      <------>o                 |        Single        | PW Instance
              |    Forwarder    +     PW Instance      X<===========>
              |                 |                      |
              |                 |----------------------|
              |                 |        Single        | PW Instance
              |                 +     PW Instance      X<===========>
              |                 |                      |
              +----------------------------------------+
```

Figure 1: PE Architecture for PW Redundancy

3.2. PW Redundancy Network Reference Scenarios

This section presents a set of reference scenarios for PW redundancy. These reference scenarios represent example network topologies that illustrate the use of PW redundancy. They can be combined together to create more complex or comprehensive topologies, as required by a particular application or deployment.

3.2.1. PW Redundancy for AC and PE Protection: One Dual-Homed CE with Redundant SS-PWs

Figure 2 illustrates an application of single-segment pseudowire redundancy where one of the CEs is dual-homed. This scenario is designed to protect the emulated service against a failure of one of the PEs or ACs attached to the multi-homed CE. Protection against failures of the PSN tunnels is provided using PSN mechanisms such as MPLS fast reroute, so that these failures do not impact the PW.

CE1 is dual-homed to PE1 and PE3. A dual-homing control protocol, the details of which are outside the scope of this document, enables the PEs and CEs to determine which PE (PE1 or PE3) should forward towards CE1 and therefore which AC CE1 should use to forward towards the PSN.

```
            |<-------------- Emulated Service ---------------->|
            |                                                  |
            |          |<------- Pseudo Wire ------>|          |
            |          |                            |          |
            |          |    |<-- PSN Tunnels-->|    |          |
            |          V    V                  V    V          |
            V    AC    +----+                  +----+     AC   V
      +-----+    |     | PE1|==================|    |     |    +-----+
      |     |----------|....|...PW1.(active)...|....|----------|     |
      |     |          |    |==================|    |          | CE2 |
      | CE1 |          +----+                  |PE2 |          |     |
      |     |          +----+                  |    |          +-----+
      |     |          |    |==================|    |
      |     |----------|....|...PW2.(standby)..|    |
      +-----+    |     | PE3|==================|    |
                 AC    +----+                  +----+
```

Figure 2: One Dual-Homed CE and Redundant SS-PWs

In this scenario, only one of the PWs should be used for forwarding between PE1/PE3 and PE2. PW redundancy determines which PW to make active based on the forwarding state of the ACs so that only one path is available from CE1 to CE2. This requires an additional PW state that reflects this forwarding state, which is separate from the operational status of the PW. This is the 'Preferential Forwarding Status'.

Consider the example where the AC from CE1 to PE1 is initially active and the AC from CE1 to PE3 is initially standby. PW1 is made active and PW2 is made standby in order to complete the path to CE2.

On failure of the AC between CE1 and PE1, the forwarding state of the AC on PE3 transitions to active. The preferential forwarding state of PW2 therefore needs to become active, and PW1 standby, in order to re-establish connectivity between CE1 and CE2. PE3 therefore uses PW2 to forward towards CE2, and PE2 uses PW2 instead of PW1 to forward towards CE1. PW redundancy in this scenario requires that the forwarding status of the ACs at PE1 and PE3 be signaled to PE2 so that PE2 can choose which PW to make active.

Changes occurring on the dual-homed side of the network due to a failure of the AC or PE are not propagated to the ACs on the other side of the network. Furthermore, failures in the PSN are not propagated to the attached CEs.

3.2.2. PW Redundancy for AC and PE Protection: Two Dual-Homed CEs with Redundant SS-PWs

Figure 3 illustrates an application of single-segment pseudowire redundancy where both of the CEs are dual-homed. This scenario is also designed to protect the emulated service against failures of the ACs and failures of the PEs. Both CE1 and CE2 are dual-homed to their respective PEs, CE1 to PE1 and PE2, and CE2 to PE3 and PE4. A dual-homing control protocol, the details of which are outside the scope of this document, enables the PEs and CEs to determine which PEs should forward towards the CEs and therefore which ACs the CEs should use to forward towards the PSN.

Note that the PSN tunnels are not shown in this figure for clarity. However, it can be assumed that each of the PWs shown is encapsulated in a separate PSN tunnel. Protection against failures of the PSN tunnels is provided using PSN mechanisms such as MPLS fast reroute, so that these failures do not impact the PW.

```
         |<-------------- Emulated Service ---------------->|
         |                                                  |
         |          |<------- Pseudowire ------->|          |
         |          |                            |          |
         |          |    |<-- PSN Tunnels-->|    |          |
         |          V    V                  V    V          |
         V    AC    +----+                  +----+    AC    V
   +-----+    |     |....|.......PW1........|....|    |     +-----+
   |     |----------| PE1|......   .........| PE3|----------|     |
   | CE1 |          +----+      \ /  PW3    +----+          | CE2 |
   |     |          +----+       X          +----+          |     |
   |     |          |    |....../ \..PW4....|    |          |     |
   |     |----------| PE2|                  | PE4|--------- |     |
   +-----+    |     |....|.....PW2..........|....|    |     +-----+
              AC    +----+                  +----+    AC
```

Figure 3: Two Dual-Homed CEs and Redundant SS-PWs

PW1 and PW4 connect PE1 to PE3 and PE4, respectively. Similarly, PW2 and PW3 connect PE2 to PE4 and PE3. PW1, PW2, PW3, and PW4 are all up. In order to support protection for the emulated service, only one PW MUST be selected to forward traffic.

If a PW has a preferential forwarding status of 'active', it can be used for forwarding traffic. The actual up PW chosen by the combined set of PEs connected to the CEs is determined by considering the preferential forwarding status of each PW at each PE. The mechanisms for communicating the preferential forwarding status are outside the scope of this document. Only one PW is used for forwarding.

The following failure scenario illustrates the operation of PW redundancy in Figure 3. In the initial steady state, when there are no failures of the ACs, one of the PWs is chosen as the active PW, and all others are chosen as standby. The dual-homing protocol between CE1 and PE1/PE2 chooses to use the AC to PE2, while the protocol between CE2 and PE3/PE4 chooses to use the AC to PE4. Therefore, the PW between PE2 and PE4 is chosen as the active PW to complete the path between CE1 and CE2.

On failure of the AC between the dual-homed CE1 and PE2, the preferential forwarding status of the PWs at PE1, PE2, PE3 and PE4 needs to change so as to re-establish a path from CE1 to CE2. Different mechanisms can be used to achieve this and these are beyond the scope of this document. After the change in status, the algorithm needs to evaluate and select which PW to forward traffic on. In this application, each dual-homing algorithm, i.e., {CE1, PE1, PE2} and {CE2, PE3, PE4}, selects the active AC independently.

There is therefore a need to signal the active status of each AC such that the PEs can select a common active PW for forwarding between CE1 and CE2.

Changes occurring on one side of network due to a failure of the AC or PE are not propagated to the ACs on the other side of the network. Furthermore, failures in the PSN are not propagated to the attached CEs. Note that end-to-end native service protection switching can also be used to protect the emulated service in this scenario. In this case, PW3 and PW4 are not necessary.

If the CEs do not perform native service protection switching, they may instead use load balancing across the paths between the CEs.

3.2.3. PW Redundancy for S-PE Protection: Single-Homed CEs with Redundant MS-PWs

Figure 4 shows a scenario where both CEs are single-homed, and MS-PW redundancy is used. The main objective is to protect the emulated service against failures of the S-PEs.

```
       Native   |<----------- Pseudowires ----------->|  Native
       Service  |                                     |  Service
        (AC)    |     |<-PSN1-->|     |<-PSN2-->|     |  (AC)
          |     V     V         V     V         V     V   |
          |     +-----+         +-----+         +-----+   |
   +----+ |     |T-PE1|=========|S-PE1|=========|T-PE2|   |    +----+
   |    |-------|......PW1-Seg1.......|.PW1-Seg2......|-------|    |
   | CE1|       |     |=========|     |=========|     |       | CE2|
   |    |       +-----+         +-----+         +-----+       |    |
   +----+        |.||.|                          |.||.|       +----+
                 |.||.|         +-----+          |.||.|
                 |.||.|=========|     |========== .||.|
                 |.||...PW2-Seg1......|.PW2-Seg2...||.|
                 |.| ===========|S-PE2|============ |.|
                 |.|            +-----+             |.|
                 |.|============+-----+============= .|
                 |.....PW3-Seg1.|     | PW3-Seg2......|
                  ==============|S-PE3|===============
                                |     |
                                +-----+
```

Figure 4: Single-Homed CE with Redundant MS-PWs

CE1 is connected to T-PE1, and CE2 is connected to T-PE2. There are three multi-segment PWs. PW1 is switched at S-PE1, PW2 is switched at S-PE2, and PW3 is switched at S-PE3. This scenario provides N:1 protection for the subset of the path of the emulated service from T-PE1 to T-PE2.

Since there is no multi-homing running on the ACs, the T-PE nodes advertise 'active' for the preferential forwarding status based on a priority for the PW. The priority associates a meaning of 'primary PW' and 'secondary PW' to a PW. These priorities MUST be used if revertive mode is used and the active PW to use for forwarding is determined accordingly. The priority can be derived via configuration or based on the value of the PW forwarding equivalence class (FEC). For example, a lower value of PWid FEC can be taken as a higher priority. However, this does not guarantee selection of same PW by the T-PEs because of, for example, a mismatch in the configuration of the PW priority at each T-PE. The intent of this application is for T-PE1 and T-PE2 to synchronize the transmit and receive paths of the PW over the network. In other words, both T-PE nodes are required to transmit over the PW segment that is switched by the same S-PE. This is desirable for ease of operation and troubleshooting.

3.2.4. PW Redundancy for PE-rs Protection in H-VPLS Using SS-PWs

The following figure (based on the architecture shown in Figure 3 of [RFC4762]) illustrates the application of PW redundancy to hierarchical VPLS (H-VPLS). Note that the PSN tunnels are not shown for clarity, and only one PW of a PW group is shown. A multi-tenant unit switch (MTU-s) is dual-homed to two PE router switches. The example here uses SS-PWs, and the objective is to protect the emulated service against failures of a PE-rs.

```
                                           PE1-rs
                                       +--------+
                                       |  VSI   |
                       Active PW       |   --   |
                        Group..........|../  \..|.
       CE-1                 .          |  \  /  | .
        \                  .           |   --   |  .
         \                .            +--------+   .
          \   MTU-s      .                  .        .     PE3-rs
           +--------+   .                   .         . +--------+
           |   VSI  |  .                    .  H-VPlS  .|  VSI   |
           |   -- ..|..                     .   Core    |.. --   |
           |  /  \  |                       .    PWs    |  /  \  |
           |  \  /..|..                     .           |  \  /  |
           |   --   |  .                    .          .|.. --   |
           +--------+   .                   .         . +--------+
          /              .                  .        .
         /                .            +--------+   .
        /                  .           |  VSI   |  .
       CE-2                 .          |   --   | .
                             ..........|../  \..|.
                       Standby PW      |  \  /  |
                        Group          |   --   |
                                       +--------+
                                         PE2-rs
```

Figure 5: MTU-s Dual-Homing in H-VPLS Core

In Figure 5, the MTU-s is dual-homed to PE1-rs and PE2-rs and has spoke PWs to each of them. The MTU-s needs to choose only one of the spoke PWs (the active PW) to forward traffic to one of the PEs and sets the other PW to standby. The MTU-s can derive the status of the PWs based on local policy configuration. PE1-rs and PE2-rs are connected to the H-VPLS core on the other side of network. The MTU-s communicates the status of its member PWs for a set of virtual switching instances (VSIs) that share a common status of active or standby. Here, the MTU-s controls the selection of PWs used to forward traffic. Signaling using PW grouping with a common group-id in the PWid FEC Element, or a Grouping TLV in Generalized PWid FEC Element as defined in [RFC4447], to PE1-rs and PE2-rs, is recommended for improved scaling.

Whenever an MTU-s performs a switchover of the active PW group, it needs to communicate this status change to the PE2-rs. That is, it informs PE2-rs that the status of the standby PW group has changed to active.

In this scenario, PE devices are aware of switchovers at the MTU-s and could generate Media Access Control (MAC) Address Withdraw messages to trigger MAC flushing within the H-VPLS full mesh. By default, MTU-s devices should still trigger MAC Address Withdraw messages as defined in [RFC4762] to prevent two copies of MAC Address Withdraw messages to be sent (one by the MTU-s and another one by the PE-rs). Mechanisms to disable the MAC withdraw trigger in certain devices are out of the scope of this document.

3.2.5. PW Redundancy for PE Protection in a VPLS Ring Using SS-PWs

The following figure illustrates the use of PW redundancy for dual-homed connectivity between PEs in a VPLS ring topology. As above, PSN tunnels are not shown, and only one PW of a PW group is shown for clarity. The example here uses SS-PWs, and the objective is to protect the emulated service against failures of a PE on the ring.

```
               PE1                            PE2
            +--------+                     +--------+
            |  VSI   |                     |  VSI   |
            |   --   |                     |   --   |
      ......|../  \..|.....................|../  \..|.......
            |  \  /  |     PW Group 1      |  \  /  |
            |   --   |                     |   --   |
            +--------+                     +--------+
                 .                              .
                 .                              .
   VPLS Domain A .                              . VPLS Domain B
                 .                              .
                 .                              .
                 .                              .
            +--------+                     +--------+
            |  VSI   |                     |  VSI   |
            |   --   |                     |   --   |
      ......|../  \..|.....................|../  \..|........
            |  \  /  |     PW Group 2      |  \  /  |
            |   --   |                     |   --   |
            +--------+                     +--------+
               PE3                            PE4
```

Figure 6: Redundancy in a VPLS Ring Topology

In Figure 6, PE1 and PE3 from VPLS domain A are connected to PE2 and PE4 in VPLS domain B via PW group 1 and PW group 2. The PEs are connected to each other in such a way as to form a ring topology. Such scenarios may arise in inter-domain H-VPLS deployments where the Rapid Spanning Tree Protocol (RSTP) or other mechanisms may be used to maintain loop-free connectivity of the PW groups.

[RFC4762] outlines multi-domain VPLS services without specifying how multiple redundant border PEs per domain and per VPLS instance can be supported. In the example above, PW group 1 may be blocked at PE1 by RSTP, and it is desirable to block the group at PE2 by exchanging the PW preferential forwarding status of standby. The details of how PW grouping is achieved and used is deployment specific and is outside the scope of this document.

3.2.6. PW Redundancy for VPLS n-PE Protection Using SS-PWs

```
                          |<----- Provider ----->|
                                    Core
                   +-------+                     +-------+
                   | n-PE  |:::::::::::::::::::::| n-PE  |
        Provider   | (P)   |..........  .........| (P)   | Provider
        Access     +-------+          . .        +-------+ Access
        Network                        X                   Network
          (1)      +-------+          . .        +-------+   (2)
                   | n-PE  |..........  .........| n-PE  |
                   |  (B)  |.....................| (B)   |
                   +-------+                     +-------+
```

Figure 7: Bridge Module Model

Figure 7 shows a scenario with two provider access networks. The example here uses SS-PWs, and the objective is to protect the emulated service against failures of a network-facing PE (n-PE).

Each network has two n-Pes. These n-PEs are connected via a full mesh of PWs for a given VPLS instance. As shown in the figure, only one n-PE in each access network serves as the primary PE (P) for that VPLS instance, and the other n-PE serves as the backup PE (B). In this figure, each primary PE has two active PWs originating from it. Therefore, when a multicast, broadcast, or unknown unicast frame arrives at the primary n-PE from the access network side, the n-PE replicates the frame over both PWs in the core even though it only needs to send the frames over a single PW (shown with :::: in the figure) to the primary n-PE on the other side. This is an unnecessary replication of the customer frames that consumes core-network bandwidth (half of the frames get discarded at the receiving n-PE). This issue gets aggravated when there are three or more n-PEs per provider access network. For example, if there are three n-PEs or four n-PEs per access network, then 67% or 75% of core bandwidth for multicast, broadcast, and unknown unicast are wasted, respectively.

In this scenario, the n-PEs can communicate the active or standby status of the PWs among them. This status can be derived from the active or backup state of an n-PE for a given VPLS.

4. Generic PW Redundancy Requirements

4.1. Protection Switching Requirements

- Protection architectures such as N:1,1:1 or 1+1 are possible. 1:1 protection MUST be supported. The N:1 protection case is less efficient in terms of the resources that must be allocated; hence, this SHOULD be supported. 1+1 protection MAY be used in the scenarios described in the document. However, the details of its usage are outside the scope of this document, as it MAY require a 1+1 protection switching protocol between the CEs.

- Non-revertive behavior MUST be supported, while revertive behavior is OPTIONAL. This avoids the need to designate one PW as primary unless revertive behavior is explicitly required.

- Protection switchover can be initiated from a PE, e.g., using a manual switchover or a forced switchover, or it may be triggered by a signal failure, i.e., a defect in the PW or PSN. Manual switchover may be necessary if it is required to disable one PW in a redundant set. Both methods MUST be supported, and signal failure triggers MUST be treated with a lower priority than any local or far-end forced switch or manual trigger.

- A PE MAY be able to forward packets received from a PW with a standby status in order to avoid black holing of in-flight packets during switchover. However, in cases where VPLS is used, all VPLS application packets received from standby PWs MUST be dropped, except for OAM and control-plane packets.

4.2. Operational Requirements

- (T-)PEs involved in protecting a PW SHOULD automatically discover and attempt to resolve inconsistencies in the configuration of primary/secondary PWs.

- (T-)PEs involved in protecting a PW SHOULD automatically discover and attempt to resolve inconsistencies in the configuration of revertive/non-revertive protection switching mode.

- (T-)PEs that do not automatically discover or resolve inconsistencies in the configuration of primary/secondary, revertive/non-revertive, or other parameters MUST generate an alarm upon detection of an inconsistent configuration.

- (T-)PEs participating in PW redundancy MUST support the configuration of revertive or non-revertive protection switching modes if both modes are supported.

- The MIB(s) MUST support inter-PSN monitoring of the PW redundancy configuration, including the protection switching mode.

- (T-)PEs participating in PW redundancy SHOULD support the local invocation of protection switching.

- (T-)PEs participating in PW redundancy SHOULD support the local invocation of a lockout of protection switching.

5. Security Considerations

The PW redundancy method described in this RFC will require an extension to the PW setup and maintenance protocol [RFC4447], which in turn is carried over the Label Distribution Protocol (LDP) [RFC5036]. This PW redundancy method will therefore inherit the security mechanisms of the version of LDP implemented in the PEs.

6. Contributors

The editors would like to thank Pranjal Kumar Dutta, Marc Lasserre, Jonathan Newton, Hamid Ould-Brahim, Olen Stokes, Dave Mcdysan, Giles Heron, and Thomas Nadeau, all of whom made a major contribution to the development of this document.

Pranjal Dutta
Alcatel-Lucent
EMail: pranjal.dutta@alcatel-lucent.com

Marc Lasserre
Alcatel-Lucent
EMail: marc.lasserre@alcatel-lucent.com

Jonathan Newton
Cable & Wireless
EMail: Jonathan.Newton@cw.com

Hamid Ould-Brahim
EMail: ouldh@yahoo.com

Olen Stokes
Extreme Networks
EMail: ostokes@extremenetworks.com

Dave McDysan
Verizon
EMail: dave.mcdysan@verizon.com

Giles Heron
Cisco Systems
EMail: giles.heron@gmail.com

Thomas Nadeau
Juniper Networks
EMail: tnadeau@lucidvision.com

7. Acknowledgements

The authors would like to thank Vach Kompella, Kendall Harvey, Tiberiu Grigoriu, Neil Hart, Kajal Saha, Florin Balus, and Philippe Niger for their valuable comments and suggestions.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, March 2005.

[RFC4446] Martini, L., "IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)", BCP 116, RFC 4446, April 2006.

[RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4762] Lasserre, M. and V. Kompella, "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", RFC 4762, January 2007.

[RFC5036] Andersson, L., Minei, I., and B. Thomas, "LDP Specification", RFC 5036, October 2007.

[RFC5659] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, October 2009.

8.2. Informative Reference

[RFC5601] Nadeau, T. and D. Zelig, "Pseudowire (PW) Management Information Base (MIB)", RFC 5601, July 2009.

Authors' Addresses

Praveen Muley
Alcatel-Lucent

EMail: praveen.muley@alcatel-lucent.com

Mustapha Aissaoui
Alcatel-Lucent

EMail: mustapha.aissaoui@alcatel-lucent.com

Matthew Bocci
Alcatel-Lucent

EMail: matthew.bocci@alcatel-lucent.com