CONFIDENTIAL INFORMATION
DESTROY BY SHREDDER ONLY

ISOCORE

MPLS-TP Interoperability

MPLS in Transport Networks
MPLS-Transport Profile (MPLS-TP)

August 2012

Document ID: 10366v7
Status: Draft

Revisions

Date	Revisions/Changes
3/15/2010	**First Draft/ New tests**
9/10/2010	**Second Draft/ Updated references, and test cases**
5/6/2011	**Updated test cases to match the updated references**
03/24/2012	**Updated test cases and references**
08/25/2012	**Updated test cases and references**

TABLE OF CONTENTS

1 Terminology

1. **MPLS-TP**: MPLS Transport Profile
2. **G-ACH**: Generic Associated Channel
3. **MEP**: Maintenance End Point
4. **MIP**: Maintenance Intermediate Point
5. **APS**: Automatic Protection Switching
6. **MCC**: Management Communication Channel
7. **FM**: Fault Management
8. **CM**: Configuration Management
9. **PM**: Performance Management
10. **EMF**: Equipment Management Function
11. **MPLS-TP PE**: MPLS-TP enabled Provider Edge node
12. **MPLS-TP P**: MPLS –TP enabled Provider Core node
13. **T-PE**: PW Terminating Provider Edge node
14. **S-PE**: PW Switching Provider Edge node
15. **MPLS-TP LSP:** MPLS-TP Label Switched Path
16. **AIS:** Alarm Indication Signal
17. **CFI:** Client Fault Indication
18. **RDI:** Remote Defect Indication
19. **CC:** Continuity Check
20. **DBN:** Domain Border Node
21. **LPSTME:** LSP path segment tunnel Maintenance Entity
22. **PST:** Path Segment Tunnel
23. **SME:** Section Maintenance Entity
24. **LME:** LSP Maintenance Entity
25. **PPSTME:** MS-PW PST Maintenance Entity
26. **ECC:** Embedded Communication Channel
27. **MCN:** Management Communication Channel
28. **SCC:** Signaling Communication Channel
29. **ME:** Maintenance Entity
30. **MEG:** Maintenance Entity Group

2 Introduction

This document provides a test plan to validate the interoperability of MPLS-TP enabled implementations in a neutral test environment. Isocore has been at the forefront of testing new technologies, and MPLS-TP is being added to the list. This test plan exclusively addresses variety of test scenarios that can be executed to ensure interoperability amongst participants supporting MPLS feature-set for transport networks applicability. As it is a known fact that MPLS although a stable technology does not offer capabilities and mechanisms needed for transport network operations. MPLS-TP [1,3] promises to meet all the requirements and functionalities of a packet-transport network while being backward compatible with installed MPLS base in current Internet. MPLS-TP extends MPLS OAM tools [2,4], support various protection mappings (1+1, 1:1 or 1:N), supports traffic engineering, and has an option to be provisioned with either management plane tools or control plane based on the GMPLS suite of protocols. As classic MPLS, it could support both point-to-point and point-to-multipoint labeled paths.

MPLS-TP enabled nodes (MPLS-TP PE, P, S-PE, T-PE) data plane supports the MPLS forwarding and bidirectional P2P and P2MP LSPs. Supports in-band OAM channel, connectivity check and verification, alarm suppression and fault indication with AIS, RDI and CFI. MPLS-TP LSPs cannot be merged with other LSPs at an MPLS-TP LSR and MPLS-TP enabled nodes should be able to create and maintain LSPs in the absence or presence of dynamic control plane.

The primary goal of this testing effort is to promote rapid adoption of MPLS-TP in transport networks, and help vendors to test their implementation during the development cycle. We will support this objective by validating implementations of MPLS-TP in an independent, multi-vendor network infrastructure. The results of the tests will be used to provide input to the standard development organizations which will help correct any discrepancies in the specifications. In the event that problems or issues are discovered, they will be addressed individually between the vendors involved in full confidentiality.

This document is work-in-progress.

The topologies shown in this document are only preliminary examples. The real carrier network capable of offering real-world environment will be built upon studying the availability of hardware in the lab. The common network infrastructure will be posted 1-week before the test event.

3 Reference Test Setup

Reference diagram for the entire document is presented in figure 1. The test document addresses various components of MPLS-TP such as MPLS-TP forwarding functions, Generic Associated channel, OAM, bidirectional LSPs, static operation of LSPs, and PWs, interoperability between traditional MPLS and MPLS-TP.

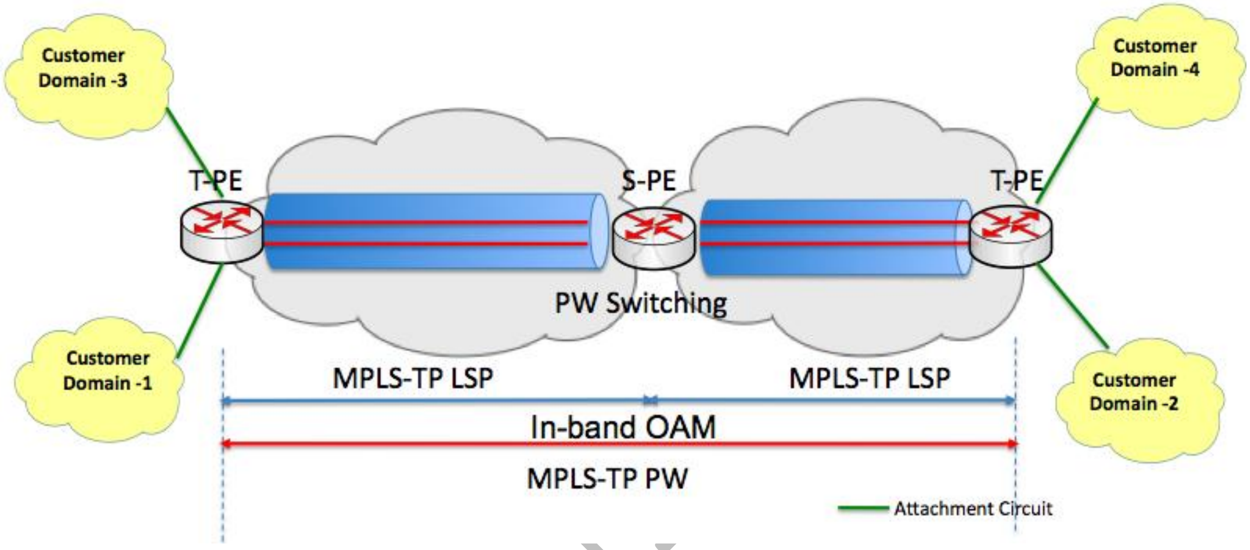


Figure 1: Reference test topology illustrating various network components under test

4 Basic MPLS-TP Data Plane Verification

This section presents tests which focus on verifying the basic functionality of the MPLS-TP data plane in a multi-vendor scenario and evaluate the capability of the implementations to transport client traffic across MPLS-TP enabled LSP or networks.

4.1 Test case: MPLS-TP Data Plane Verification

Purpose:
To verify the ability of the participating implementations to support transport of client traffic across MPLS-TP domain/network [1]

Topology:

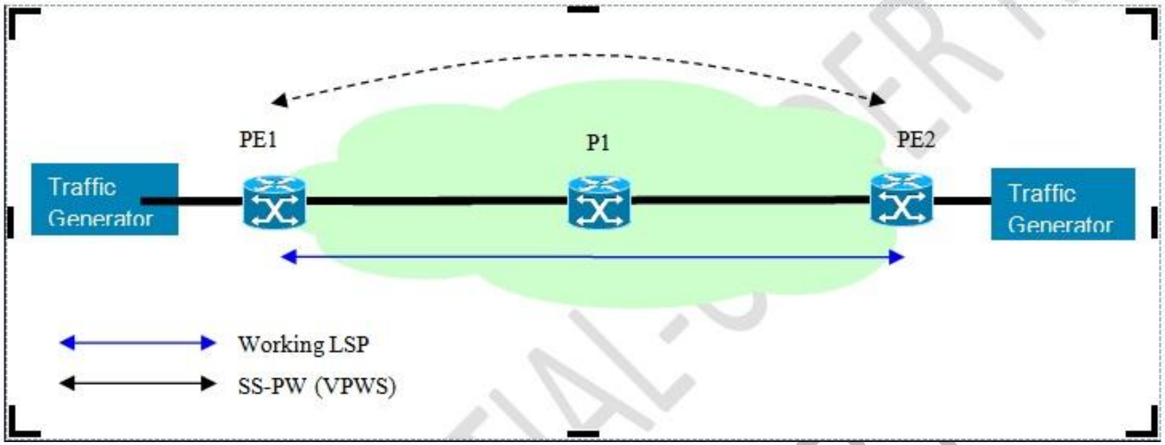


Figure 2: MPLS-TP basic test setup

Procedure:

1. Configure PE1, PE 2, P1, and P2 for MPLS-TP
2. Ensure that there is a direct connection between all the test nodes to isolate any issues
3. Ensure that the tester (emulator as shown in figure 2) is capable of sending traffic across the test setup
4. Configure a static LSP initiating at PE1 and terminating at PE2, if possible and supported create bidirectional co-routed path
5. Use this successful LSP, to provision a static PW from PE1 to PE2 to transport emulated client traffic from customer domain 1 to customer domain 2
6. Verify that the traffic is received successfully at both ends

Expected Results:
Tester receives the traffic at both ends

5 MPLS-TP OAM:

As MPLS-TP [1] standards continue to evolved in IETF, this test plan attempts to find a minimum set of features that can be considered for MPLS-TP OAM interoperability testing. As MPLS-TP defines a profile of the MPLS and PW architectures, it compliments it with the additional set of OAM mechanisms and procedures, which meet the requirements as defined in [2]. MPLS-TP OAM framework [3] is applicable to LSPs and MS-PWs, and supports bidirectional point-to-point LSPs and unidirectional point-to-multipoint paths. MPLS-TP OAM is configured as MEs – which is a relationship between two points along a transport path to which monitoring or maintenance operation applies. A pair of such points is called a MEG – Maintenance Entity Group (MEG), and end points are called MEPs. Figure 2 illustrates the reference test diagram for MPLS-TP OAM for a single domain. This could be easily extended to the multiple domain test setup.

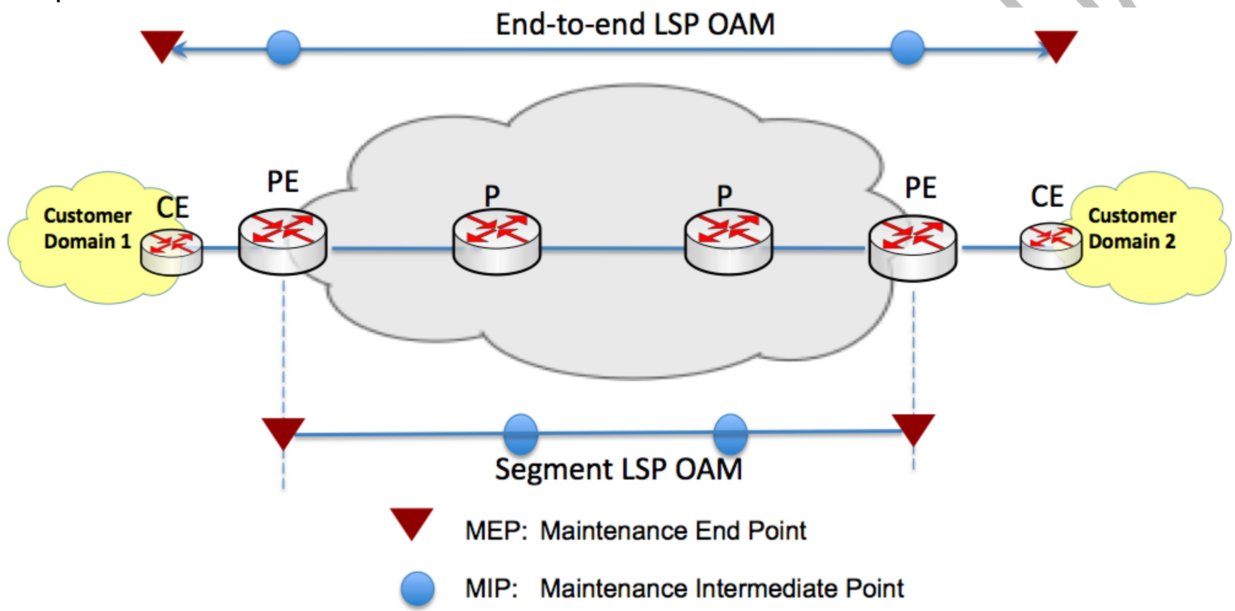


Figure 3: MPLS-TP OAM Reference Test Diagram

There can be multiple points between the MEPs, and which are defined as MIPs – Maintenance Entity Group Intermediate Points (MIPs). MPLS-TP MEG may be defined to monitor the transport path for fault or performance management. To meet the MPLS-TP OAM functional requirements several MPLS-TP MEGs are defined, which include: SME, LME, PME, LPSTME, and PPSTME.

In the preliminary stages of MPLS-TP testing, the focus will be on verifying the OAM operations across multi-vendor products that are configured to be carried out periodically and continuously or act on certain triggers such as alarm signals. MPLS-TP OAM framework [3] terms these as proactive monitoring or in-service monitoring.

5.1 Test case: Establishing BFD and Continuity Check over an MPLS-TP LSP and Associated Channel (GACH)

Purpose:
To verify the ability of the participating implementations to establish BFD sessions and CC over an MPLS-TP LSP and Generic Associated Channel [5]

Topology: Figure 2

Procedure:

1. Configure PE1, PE 2, P1, and P2 for MPLS-TP

2. Ensure that there is a direct connection between all the test nodes to isolate any issues

3. Ensure that the tester (emulator as shown in figure 2) is capable of sending traffic across the test setup

4. Configure a static LSP initiating at PE1 and terminating at PE2, if possible and supported create bidirectional co-routed path

5. Create a pair of MEPs for the ME along the path from PE1 to PE2

6. Initiate the process of sending CC messages between PE1 and PE2
   The options for BFD-CC are
   a. BFD-CC only (ACH channel 7)
   b. interleaved BFD-CC and BFD-CV

7. Verify that the BFD session is UP on both ends (PE1, PE2) by local status verification on both the ends

Expected Results:
The BFD session is properly established, and MEPs periodically send CC packets.

5.2 Test Case: Handling of MPLS-TP OAM Loopback function

Purpose:
To verify the ability of the participating implementations capability in handling loopback function

Topology: Figure 5

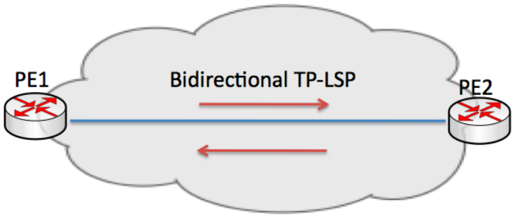


Figure 5: Topology Setup for Loopback tests

Discussion:
OAM loopback is the capability of the node to intercept some specific OAM packets and to generate a reply back to the sender. For this test the setup should enable at least one TP-LSP on a link between the PE1 and PE2, refer figure 4.

Procedure:

1. Configure the PE1 and PE2 to do the loopback test targeting the remote MEP.
2. Configure the PE1 to send the request packet
3. PE2 upon receiving the packet should respond to PE1 with a reply
4. PE1 receives the reply
5. Verify at PE1 if the response is valid, it should display “OK” on the CLI or NMS display, otherwise display NG
6. Repeat the test at PE2 to initiate the request packet
7. The test may be repeated by inserting a P node or MIP in figure 4. Consider Figure 3 for this test

Expected Results: The PE1 or PE2 should be able to validate the messages received from the remote MEP

5.3 Test Case: Handling of Alarm Reporting (AIS)

Purpose:
To verify the capability of participating implementation to handle Alarm Reporting function as required in section 2.2.8 of MPLS-TP OAM requirements [2]

Topology:
Figure 6

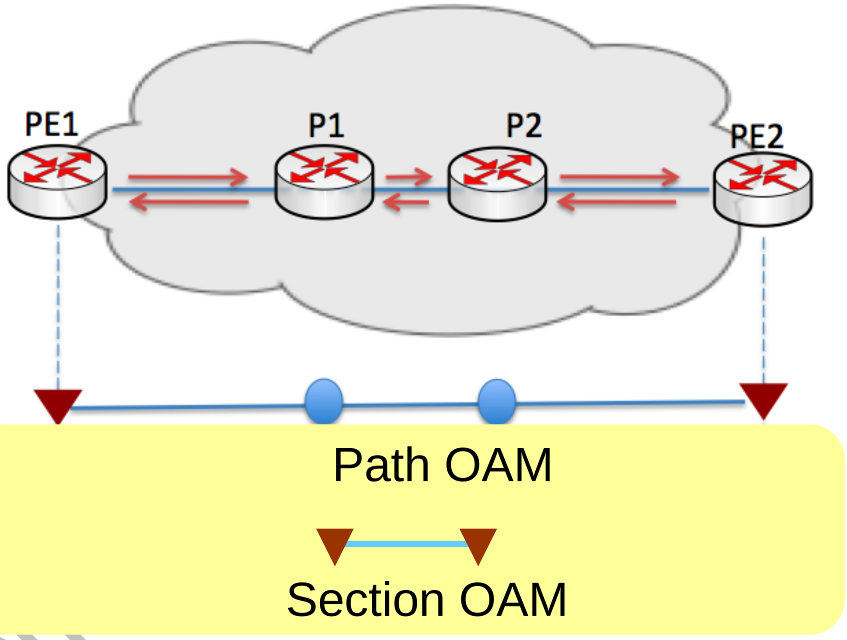


Figure 6: Topology Setup for AIS tests

Discussion:
The Alarm reporting function relies upon Alarm Indication Signal (AIS) messages used to suppress alarms following detection of defect conditions at the server sub layer. A server MEP is responsible for notifying the MPLS-TP layer network adaptation function upon fault detection in the server layer network to which the server MEP is associated. Only client layer adaptation function at an intermediate node will issue the MPLS-TP packets with AIS information. Upon receiving a packet with AIS information an MPLS-TP MEP enters into AIS defect condition and suppresses loss of continuity alarms

associated with its MEP peer. A MIP is transparent to packets with AIS information and therefore does not require the support of AIS functionality.

Procedure:

1. Ensure PE1, P1, P2 and PE2 support MPLS-TP OAM feature-set
2. Configure PE1, P1, P2 or PE2 to turn the CC-V messages
3. Confirm that the PE1,P1, P2 and PE2 can receive the CC-V messages to ensure the working condition
4. Tear the link or simulate a fiber cut between P1 and P2
5. Ensure that P1 sends AIS packets to PE1,and P2 sends AIS packets to PE2, respectively
6. Confirm that PE1 and PE display AIS alert, while LOC is properly suppressed

Expected Results: Upon receiving a packet with AIS information an MPLS-TP MEP (PE1 or PE2) enters an AIS defect condition and suppresses loss of continuity alarms associated with remote MEP peer.

5.4 Test case: Handling of Remote Defect Indication (RDI)

Purpose:
To verify the ability of the participating implementations support Remote Defect Indication, as required by MPLS-TP OAM requirements [2]

Topology:
Figure 4

Discussion:
The Remote Defect Indication (RDI) function is an indicator that is transmitted by a MEP to communicate to its peer MEP that a signal fail condition exists.

RDI is associated with proactive CC-V activation, and the indicator is piggy-backed onto the CC-V packet. When a MEP detects a signal fail condition, it begins transmitting an RDI indicator to its peer MEP. A MEP that receives the packets with the RDI information determines that its peer MEP has encountered a defect condition

Procedure:

1. Configure PE1 and PE 2 to enable the CC-V functionality. If the implementation supports with out any administrative action, then ensure if this functionality is operational.

2. Verify the CC-V functionality while configuring LSP

3. Ensure that PE1 or PE2 can generate CC-V packets

4. Verify that LOC alert is displayed on PE2, when a unidirectional failure event on the link from P1 and P2 is triggered

5. Confirm PE2 generates CC-V with RDI packets to PE1. RDI alert is displayed on PE1

6. Repeat the test for another unidirectional failure event on the link from P2 to P1

Expected Results: RDI messages are generated from a MEP to its peer in case of a signal fail condition.

6 MPLS-TP Linear Protection

MPLS-TP similar to other transport technologies promises to offer survivability mechanisms for protection and restoration. MPLS-TP survivability framework [6] defines the requirements for survivability and functional architecture for recovery mechanisms. MPLS-TP Linear Protection draft [7] further describe the functionality needed and defines protocol functions of the protection state coordination for linear protection. This section defines basic tests to validate the functionality amongst the implementations that support this feature.

6.1 Test Case: To Verify the MPLS-TP Protection Scenario

Purpose:
To verify the ability of the participating implementations to switchover upon failure from the working to the protection path

Topology: Figure 7

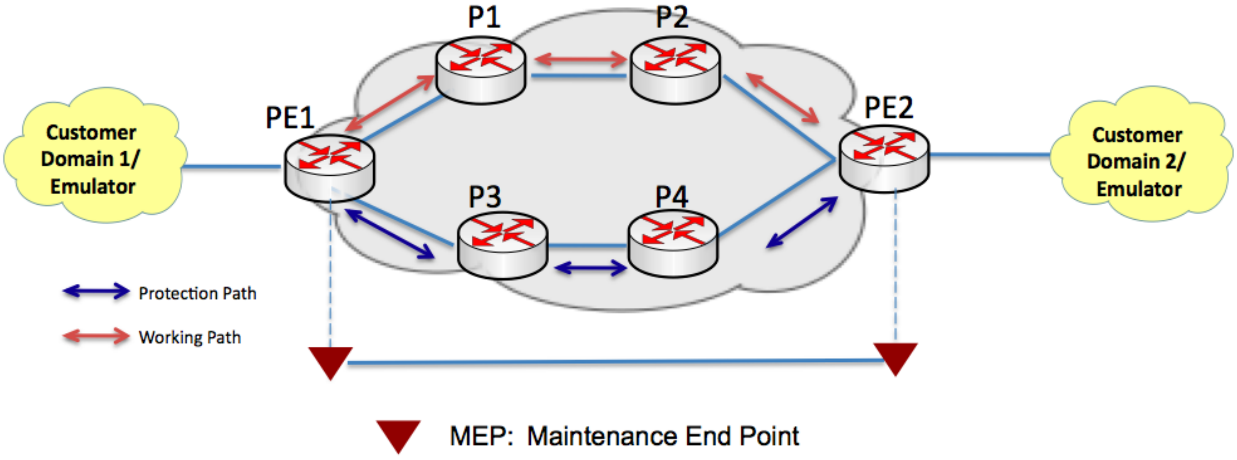

P1
P2
PE1
PE2
P3
P4
Customer Domain 1/ Emulator
Customer Domain 2/ Emulator
Protection Path
Working Path
MEP: Maintenance End Point

Figure 7: MPLS-TP Protection reference topology

Procedure:

1. Ensure that the MPLS-TP is supported by all the nodes in the setup

2. Configure a static LSP-W (with the working path) originating over the path as shown in figure 6. The path contains nodes PE1-P1-P2-PE2

3. Configure a static LSP-P (with the protection path) originating at PE1 over the path as shown in figure 6. The path contains nodes PE1-P3-P4-PE2

4. Create a static PW between PE1 and PE2 using the working path LSP

5. Create MEs for each LSP on PE1 and PE2

6. Create MEPs for each ME on PE1 and PE2

7. Enable initiation of CC packets between PE1 and PE2

8. Ensure that the CC messages are correctly delivered and processed at both ends

9. Verify that the BFD session is established (UP) on remote MEPs

10. Configure the emulator to generate traffic from the tester in both directions – PE1 to PE2, and PE2 to PE1

11. Simulate the fiber cut between the core nodes on the working path (P1-P2)

12. Verify that the PE1 and PE2 detects the a LOC and trigger protection switching

13. Monitor the traffic behavior on the tester on both ends of the LSPs

Expected Result:

- Recovery LSP should become active at PE1 and PE2. This can be verified using the show commands provided by the implementation.
- The traffic should automatically switch over to the protection path and switching times should be less than 50ms
- Traffic flows in both directions should be steady after a brief outage

6.2 Test Case: To test the operator commands

Topology: Figure 7

Procedure:

1. Ensure that the MPLS-TP is supported by all the nodes in the setup

2. Configure a static LSP-W (with the working path) originating over the path as shown in figure 6. The path contains nodes PE1-P1-P2-PE2

3. Configure a static LSP-P (with the protection path) originating at PE1 over the path as shown in figure 6. The path contains nodes PE1-P3-P4-PE2

4. Create a static PW between PE1 and PE2 using the working path LSP

5. Create MEs for each LSP on PE1 and PE2

6. Create MEPs for each ME on PE1 and PE2

7. Enable initiation of CC packets between PE1 and PE2

8. Ensure that the CC messages are correctly delivered and processed at both ends

9. Verify that the BFD session is established (UP) on remote MEPs

10. Configure the emulator to generate traffic from the tester in both directions – PE1 to PE2, and PE2 to PE1

11. Test the local operator commands at PE1

    a) Forced Switch (FS)
    b) Manual Switch (MS) (This is only relevant if there is no currently active fault condition)
    c) Clear
    4) Lockout of Protection

12. Verify that the PE2 detects the a LOC and trigger protection switching

13. Monitor the traffic behavior on the tester on both ends of the LSPs

6.3 Revertive Mode Operation

Purpose:

To verify the ability of the participating implementations re-activate working LSP (revertive mode) when fault on the working LSP is cleared.

Topology:

Figure 7

Procedure:

1. Carry out all steps of Test 6.1 ("Protection Switching").
2. After activating recovery LSP as in Test 6.1, wait till the traffic flows become steady in both directions.

3. Clear the fault on the working LSP.

Expected Results:

After fault is cleared:

- Working LSP should become active at PE1 and PE2. This can be verified using the show commands provided by the implementation.
- Traffic flows in both directions, and no traffic loss is expected during the reversion.

7 MPLS-TP Performance Monitoring

7.1 LSP Loss Measurement (LM) test

Two different modes of LM are supported:

- Direct mode LM computes the actual packet loss of the channel via exchange of data-plane counters. Direct LM works only for MPLS-TP LSPs
- Inferred mode LM computes the loss of a stream of test messages in order to approximate the channel loss. Inferred LM works in both IP/MPLS/MPLS-TE/MPLS-TP.

The two modes use different G-ACh Channel Types but function identically at the protocol level

The PTP 64-bit IEEE 1588 version 1 timestamp format has been chosen as the mandatory default

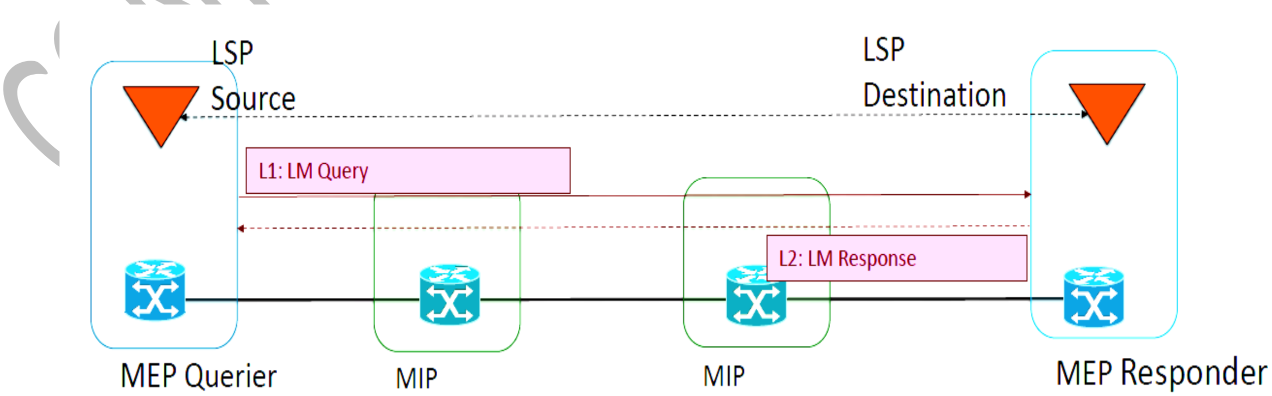
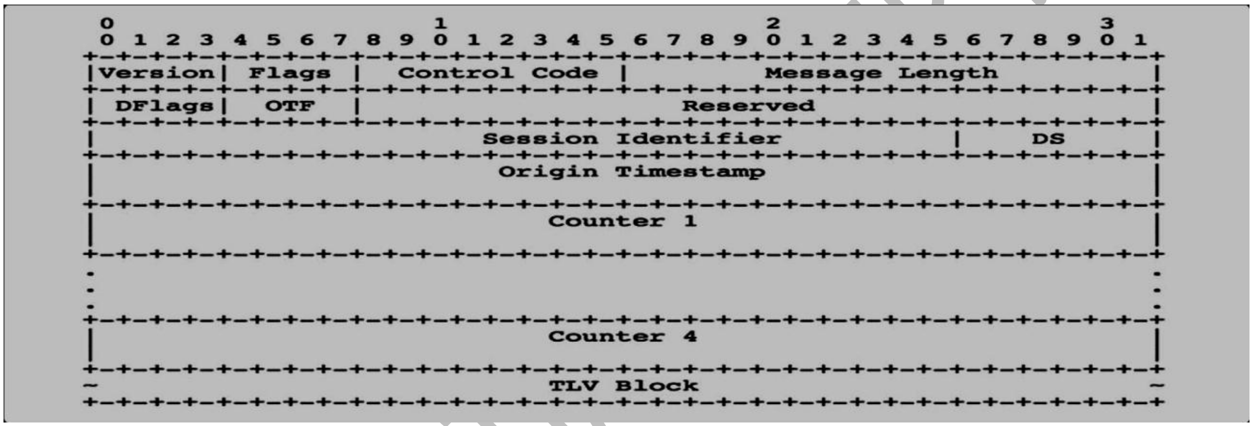


Figure 8: Test set up for LSP Loss Measurement test

1. For LM, each “counter stamp” records the count of packets or octets sent or received over the channel prior to the time this message is sent or received.
2. For LM, loss is measured as a delta between successive messages. For example, a loss measurement in the forward direction is computed as (Q_TxCount[n] – Q_TxCount[n-1]) – (R_RxCount[n] – R_RxCount[n-1])
3. Thus LM requires a small amount of state at the querier: it retains the counter values in the most recently received response



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Flags |  Control Code |        Message Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| DFlags|  OTF  |                    Reserved                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Session Identifier                  |    DS     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Origin Timestamp                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Counter 1                            |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                                                               .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Counter 4                            |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                          TLV Block                            ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9: Loss Measurement (LM) Message Format

Field	**Meaning**
Flags	Query/Response, TC-specific measurement
Control Code	Query type or response code
DFlags	Data format flags: Packet/octet count, 32/64 counter mode
OTF	Origin Timestamp Format
Origin Timestamp	Used for sequencing and throughput measurement
Session Identifier / DS	Unique Session ID, Diffserv class

7.2 LSP Delay Measurement test

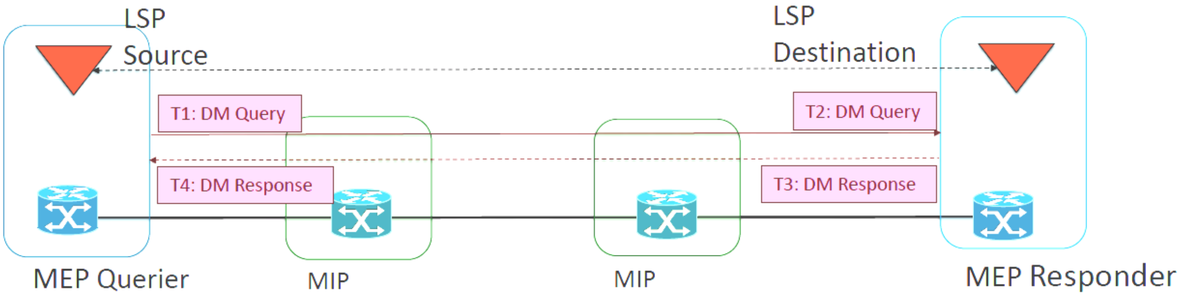


Figure 10: Test set up for LSP Delay Measurement test

1. Create MEPs for on PE1 and PE2
2. The querier begins a measurement session by initiating a stream of query messages at a specific rate
3. Time T1: Query message exits the Querier TX port and is stamped with a time or counter value
4. Time T2: Query message enters the Responder RX port and is time- or counter-stamped
5. Responder inspects and processes the query and generates a response message, which is a copy of the Query with the Response flag set
6. Time T3: Response message exits the Responder TX port and is time- or counter-stamped
7. Time T4: Response message enters the Querier RX port and is time- or counter-stamped
8. Querier now has all four data values and can compute a measurement

Calculation:

- Two-way channel delay = (T4 - T1) - (T3 - T2)

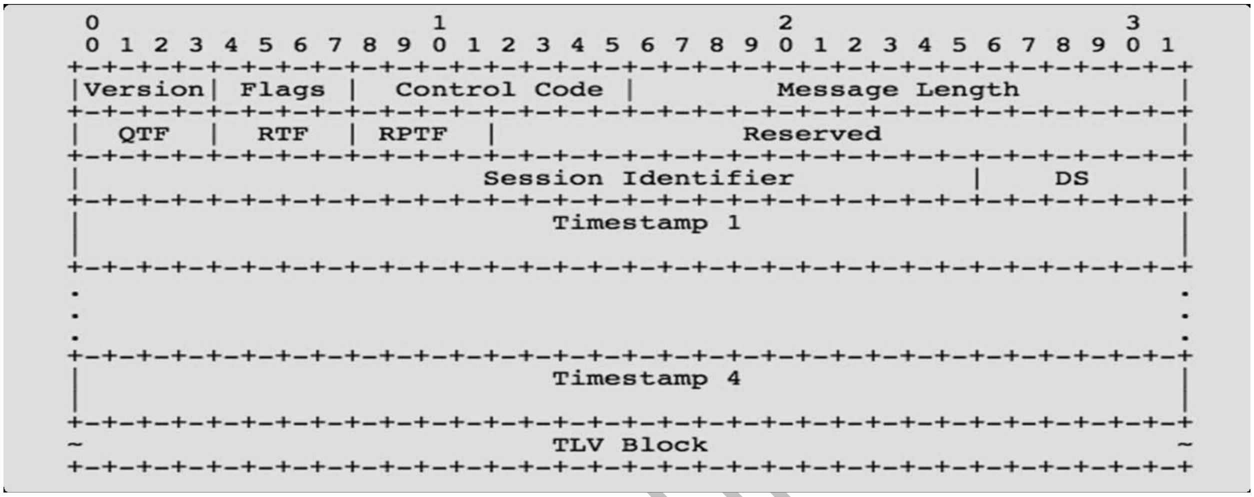
- Round-trip delay = T4 - T1

- If the clocks of MEP1 and MEP2 are known at MEP1 to be synchronized, then both one-way delay values, as well as the two-way channel delay, can be computed at MEP1 as

    - forward one-way delay = T2 - T1

    - reverse one-way delay = T4 - T3

  - two-way channel delay = forward delay + reverse delay.
- IPDV (Inter packet delay variation) represents the difference between the one-way delays of successive packets in a stream.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Flags |  Control Code |        Message Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  QTF  |  RTF  | RPTF  |              Reserved                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Session Identifier          |      DS       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Timestamp 1                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
.                                                               .
.                                                               .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Timestamp 4                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                          TLV Block                            ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 11: Delay Measurement (DM) Message Format

Field	**Meaning**
Flags	Query/Response, TC-specific measurement
Control Code	Query type or response code
QTF/RTF	Query/Response Timestamp Format
RPTF	Responder's Preferred Timestamp Format
Session Identifier / DS	Unique Session ID, Diffserv class

8 Addendum I

8.1 LSP Ping over Working and recovery LSPs

Purpose:

To verify the ability of the participating implementation to verify connectivity of working and recovery LSPs via LSP ping.

Topology:

Same as **Figure 15**.

Procedure:

1. Configure PE1, P1, P2, and PE2 for MPLS-TP.
2. Configure a bi-directional congruent static LSPs. Both working and recovery LSPs must be configured such that paths of these LSPs are not exactly the same.
3. Make sure that working LSP is operationally up using show commands at PE1 and PE2, and check its connectivity by invoking LSP ping at PE1 and PE2.
4. Inject a fault in the path of working LSP, check its connectivity using LSP ping after verifying that the working LSP is down using show command at PE1 and PE2.
5. Clear the fault on the working LSP, and check its connectivity using LSP ping after verifying that the working LSP is down using show command at PE1 and PE2.
6. Repeat steps 3 through 5 above for recovery LSP.

Expected Results:

- When an LSP is operationally up, LSP ping should yield 100% success rate.
- When an LSP is operationally down, LSP ping should yield 0% success rate.

8.2 Stitching Static and Dynamic PW segments (MPLS-TP/MPLS Interoperability)

Purpose:

To verify the ability of the participating implementation to verify stitching of dynamic and static PW segments.

Topology:

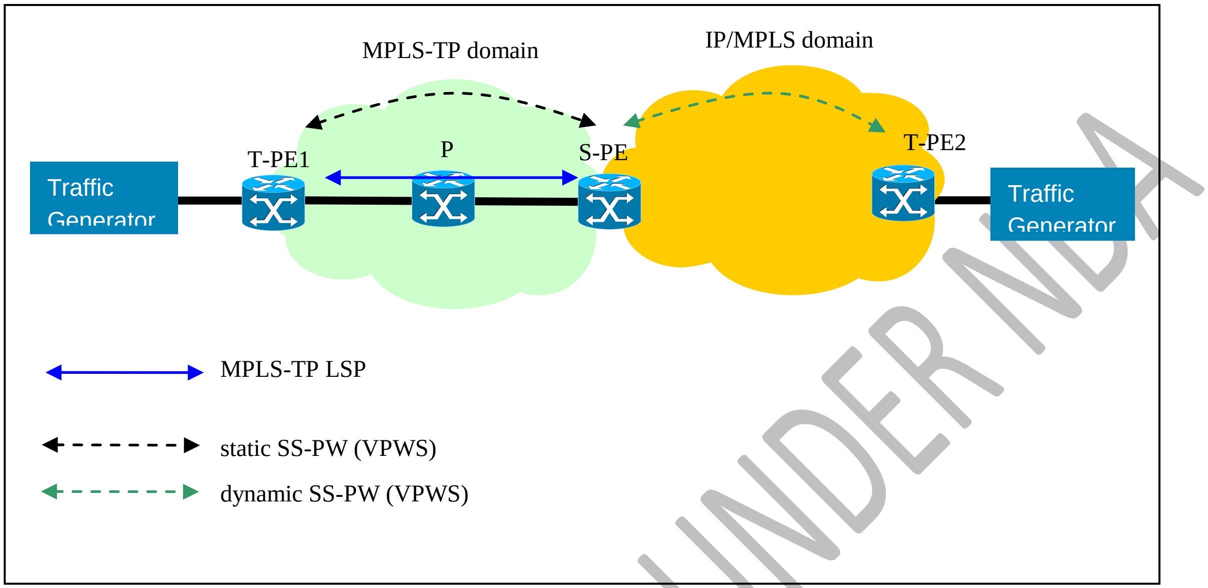


Figure 14: Test setup for verifying PW stitching functionality

Procedure:

1. Configure T-PE1, P, and S-PE nodes for MPLS-TP.
2. Configure MPLS-TP LSP (at least working LSP) between T-PE1 and S-PE.
3. Configure a static PW segment between T-PE1 and S-PE, and pin it down to the MPLS-TP LSP configured in the previous step.
4. Configure a dynamic PW segment between S-PE and T-PE2, and stitch it with the static PW segment.
5. Start traffic generators to send traffic in both directions.
6. Flap the static PW segment (e.g., by flapping AC or transport LSP down), and examine the state of the dynamic PW segment using appropriate show commands provided by the implementation.
7. Flap the dynamic PW segment (e.g., by flapping AC or transport LSP down),fault is propagated properly to the static PW (RFC6478), examine the state of the static PW segment using appropriate show commands provided by the implementation.

Expected Results:

- When one PW segment goes down, the other segment must go down.
- When one PW segment goes down, traffic flow should stop in both directions.

8.3 VPLS over MPLS-TP

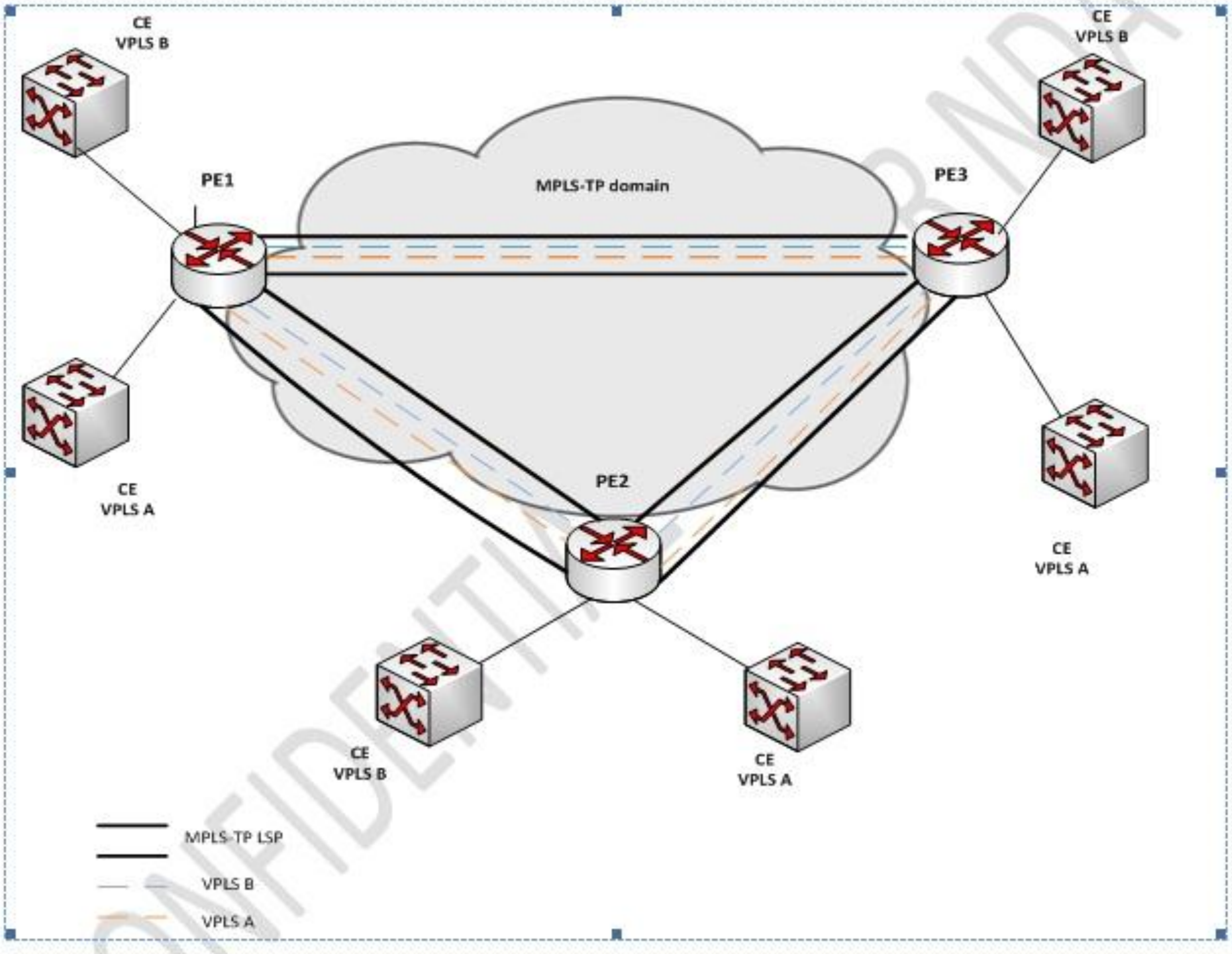


Figure 15: VPLS over MPLS-TP

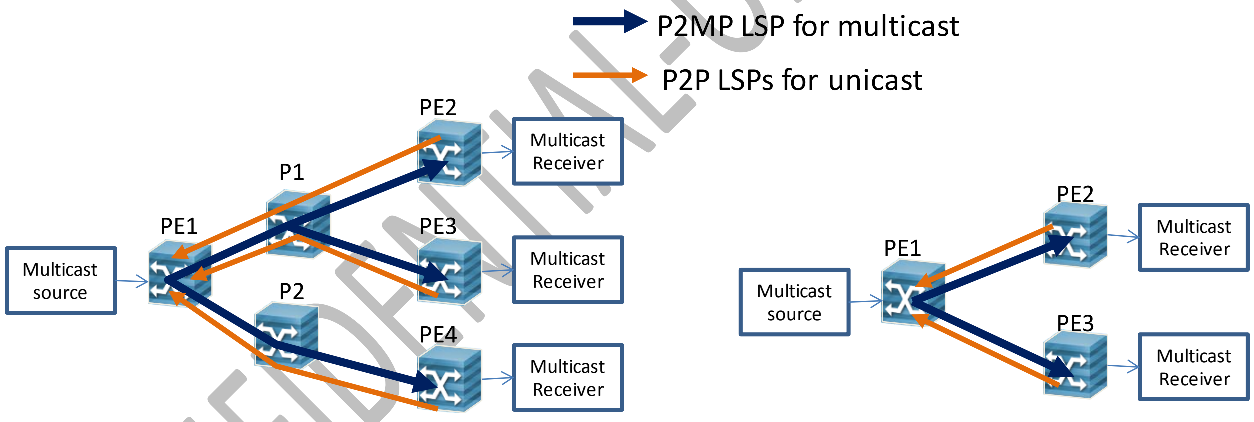
1. Configure all PE nodes for MPLS-TP.
2. Configure all PE nodes for the attachment circuits.
3. Configure full mesh MPLS-TP LSP (at least working LSP) at all PE nodes.

4. Configure a static PW segment between all PE nodes and pin it down to the respective MPLS-TP LSPs configured in the previous step.
5. Depending on the implementation, enable BFD to run on working LSP.
6. Using the show commands provided by the implementations, ensure that working LSP is active at all PE nodes.
7. Using the show commands provided by the implementations, ensure that static pseudowires that have been enabled to route Layer 2 packets on the PE routers.
8. Start traffic generators to emulate customer traffic.

8.4 MPLS-TP P2MP without protection

Purpose:
To verify the ability of MPLS-TP OAM over P2MP bidirectional configuration.

Topology:



MPLS-TP P2MP configuration

MPLS-TP P2MP configuration
(Minimum configuration)

Figure 16

Procedure:

1. Configure P2MP LSP on all PEs and Ps.(PE1:root, PE2-4:leaves)
2. Configure P2P LSPs from leaves to root. (as return paths)
3. Configure static PWs and attachment circuits
4. Enable (BFD or Y.1731) CC over P2MP LSP and P2P LSPs
5. Generate traffic form multicast source to multicast receivers

6. Inject a fault on P2MP LSP

Expected Results:

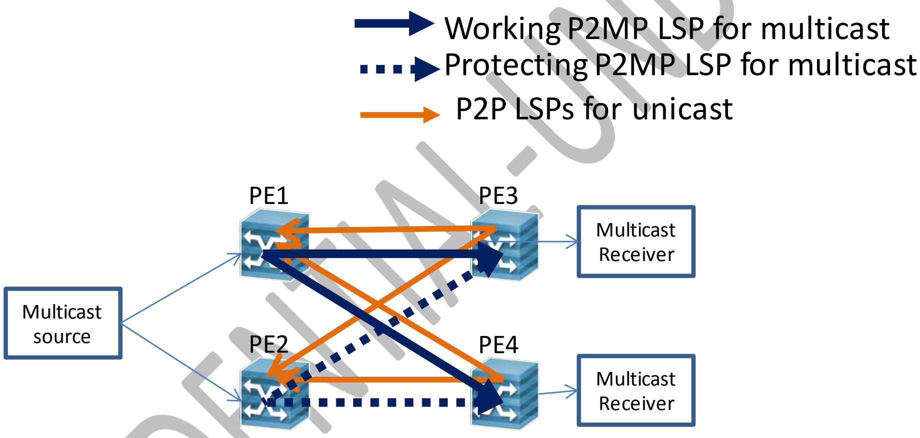
- CC sessions are up for P2MP and P2P LSPs
- All leaves receive traffic without degradation
- Only affected leaves by the failure detect fault and respond with RDI on corresponding P2P LSP.

8.5 MPLS-TP P2MP with protection

Purpose:

To verify the ability of P2MP protection with bidirectional configuration.

Topology:



MPLS-TP P2MP configuration

Figure 17

Procedure:

1. Configure working and protecting P2MP LSP on all PEs and Ps.(PE1-2: redundant roots, PE3-4:leaves).
2. Configure P2P LSPs from leaves to roots. (as return paths)
3. Configure static PWs and attachment circuits for both working and protecting P2MP LSPs.
4. Enable (BFD or Y.1731) CC over working and protecting P2MP LSPs and P2P LSPs

5. Generate traffic form multicast source to multicast receivers
6. Inject a fault on working P2MP LSP

Expected Results:

- CC sessions are up for working and protecting P2MPs and P2P LSPs
- All leaves receive traffic without degradation
- Once detecting fault on working P2MP LSP, multicast traffic is switched over to protecting P2MP.

8.6 PW Redundancy over MPLS-TP

8.6.1 Single-Single homing

Purpose:

To verify the ability of the participating implementation to support Pseudowire redundancy using static PW status. (No LSP protection, just two static PWs (Active / Standby)

Topology:

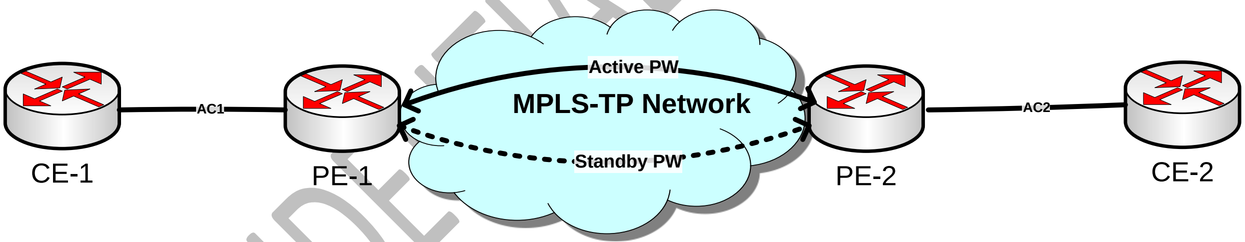


Figure 18: Single-Single homing PW Redundancy

Test Scenarios	Expected Results
AC failure	Traffic will be dropped
Active PW1 failure	PE1 and PE2 detect + switch over to Standby PW2
PE (node) failure	Traffic will be dropped

8.6.2 Single-Dual homing

Purpose:

To verify the ability of the participating implementation to support Pseudowire redundancy using static PW status. (head-end node redundancy)

Topology:

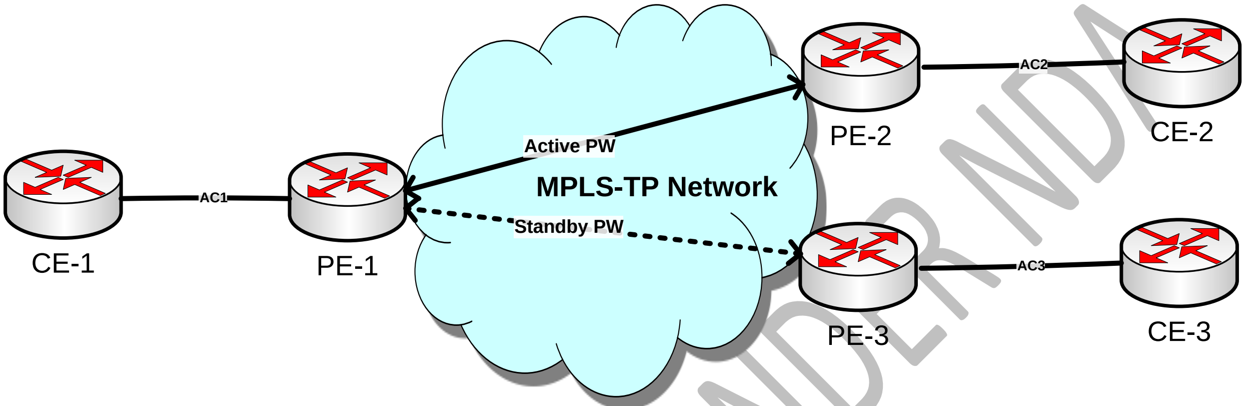


Figure 19: Single-Dual homing PW Redundancy

Test Scenarios	Expected Results
AC failure	PE2 signals to PE1, switch to Standby PW2+AC3
Active PW1 failure	PE1 detect + switch over to Standby PW2
PE (node) failure	PE1 detect + switch over to Standby PW2

9 References

[1] Requirements of an MPLS Transport Profile, RFC 5654

[2] Requirements for OAM in MPLS Transport Networks, RFC5860

[3] A Framework for MPLS in Transport Networks, RFC5921

[4] MPLS-TP OAM Framework, RFC6371

[5] Proactive CV, CC, and RDI for the MPLS Transport Profile, RFC6428

[6] Generic Associated Channel, RFC5586

[6] MPLS-TP Survivability Framework, RFC6372

[7] MPLS-TP Linear Protection, RFC6378

[8] Pseudowire Status for Static Pseudowires, RFC 6478