

# Black Book

---



Edition 7

**MPLS-TP**



### **Your feedback is welcome**

Our goal in the preparation of this Black Book was to create high-value, high-quality content. Your feedback is an important ingredient that will help guide our future books.

If you have any comments regarding how we could improve the quality of this book, or suggestions for topics to be included in future Black Books, please contact us at [ProductMgmtBooklets@ixiacom.com](mailto:ProductMgmtBooklets@ixiacom.com).

Your feedback is greatly appreciated!

Copyright © 2012 Ixia. All rights reserved.

This publication may not be copied, in whole or in part, without Ixia's consent.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

Ixia, the Ixia logo, and all Ixia brand names and product names in this document are either trademarks or registered trademarks of Ixia in the United States and/or other countries. All other trademarks belong to their respective owners. The information herein is furnished for informational use only, is subject to change by Ixia without notice, and should not be construed as a commitment by Ixia. Ixia assumes no responsibility or liability for any errors or inaccuracies contained in this publication.



## Contents

How to Read this Book.....	vii
Dear Reader.....	viii
Introduction .....	1
Business Drivers for MPLS-TP .....	2
What is MPLS-TP?.....	3
Implementation Challenges of MPLS-TP.....	5
Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW.....	9
Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation .....	19
Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes.....	25
Test Scenario 4: Verify manual APS command functionality .....	39
Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval.....	45
Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs .....	53



## How to Read this Book

The book is structured as several standalone sections that discuss test methodologies by type. Every section starts by introducing the reader to relevant information from a technology and testing perspective.

Each test case has the following organization structure:

<b>Overview</b>	Provides background information specific to the test case.
<b>Objective</b>	Describes the goal of the test.
<b>Setup</b>	An illustration of the test configuration highlighting the test ports, simulated elements and other details.
<b>Step-by-Step Instructions</b>	Detailed configuration procedures using Ixia test equipment and applications.
<b>Test Variables</b>	A summary of the key test parameters that affect the test's performance and scale. These can be modified to construct other tests.
<b>Results Analysis</b>	Provides the background useful for test result analysis, explaining the metrics and providing examples of expected results.
<b>Troubleshooting and Diagnostics</b>	Provides guidance on how to troubleshoot common issues.
<b>Conclusions</b>	Summarizes the result of the test.

## Typographic Conventions

In this document, the following conventions are used to indicate items that are selected or typed by you:

- **Bold** items are those that you select or click on. It is also used to indicate text found on the current GUI screen.
- *Italicized* items are those that you type.

## Dear Reader

Ixia's Black Books include a number of IP and wireless test methodologies that will help you become familiar with new technologies and the key testing issues associated with them.

The Black Books can be considered primers on technology and testing. They include test methodologies that can be used to verify device and system functionality and performance. The methodologies are universally applicable to any test equipment. Step by step instructions using Ixia's test platform and applications are used to demonstrate the test methodology.

This seventh edition of the black books includes eighteen volumes covering some key technologies and test methodologies:

**Volume 1** – Higher Speed Ethernet

**Volume 2** – QoS Validation

**Volume 3** – Advanced MPLS

**Volume 4** – LTE Evolved Packet Core

**Volume 5** – Application Delivery

**Volume 6** – Voice over IP

**Volume 7** – Converged Data Center

**Volume 8** – Test Automation

**Volume 9** – Converged Network Adapters

**Volume 10** – Carrier Ethernet

**Volume 11** – Ethernet Synchronization

**Volume 12** – IPv6 Transition Technologies

**Volume 13** – Video over IP

**Volume 14** – Network Security

**Volume 15** – MPLS-TP

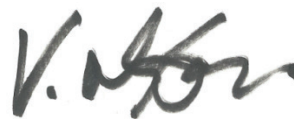
**Volume 16** – Ultra Low Latency (ULL) Testing

**Volume 17** – Impairments

**Volume 18** – LTE Access

A soft copy of each of the chapters of the books and the associated test configurations are available on Ixia's Black Book website at <http://www.ixiacom.com/blackbook>. Registration is required to access this section of the Web site.

At Ixia, we know that the networking industry is constantly moving; we aim to be your technology partner through these ebbs and flows. We hope this Black Book series provides valuable insight into the evolution of our industry as it applies to test and measurement. Keep testing hard.



Victor Alston, CEO



# MPLS-TP

## Test Methodologies

This Black Book provides an introduction to the MPLS-TP technology, its motivation, and business drivers. It presents a summary of MPLS-TP key features and some of the typical implementation challenges. It then details common test scenarios along with step-by-step procedures by using Ixia IxNetwork to achieve the test objectives.

## Introduction

The Multi-Protocol Label Switching - Transport Profile (MPLS-TP) is the result of a joint effort by the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU-T) based on their previously respective and separate work in the area of Provider Backbone Bridging (PBB) and Transport MPLS (T-MPLS). As such, it has generated tremendous interest amongst equipment vendors and service providers, because not only does it have the potential to combine the best of both worlds, but also reflects the collaborative instead of competitive spirit between two separate standard bodies.

MPLS has come a long way since its original goal to allow core routers to switch packets faster by using a simplified header. MPLS is now a foundation of IP-based networks providing value added services, such as traffic engineering and VPN services. The success and familiarity of MPLS in the core is driving service providers to deploy MPLS beyond the core of the network into access, aggregation, and backhaul networks supporting broadband, business, and mobility services.

The expansion of MPLS towards the network edge also exposed some of the weaknesses of MPLS for being a transport technology. MPLS-TP is consequently proposed and is intended to adapt MPLS to be more 'transport like,' such as SONET/SDH is commonly used in TDM networks. The fundamentals of this new technology are to extend the current MPLS wherever necessary to include Operation, Administration and Maintenance (OAM) tools that are well known in traditional transport technologies, such as SONET/SDH. Moreover, to inherit reliability and operational simplicity from SONET/SDH networks, MPLS-TP needs to support Automatic Protection Switching (APS) that is operated either in Linear or Ring mode to provide 1:1 or 1+1 through either Uni- or Bi-directional protection. Additionally, it must support static configuration of LSPs or PWs, by allowing existing SNMP-based tools to continue to be used for circuit provisioning. Envisioned as the new big 'frontier' of MPLS, the impact of MPLS-TP will be far reaching for years to come.

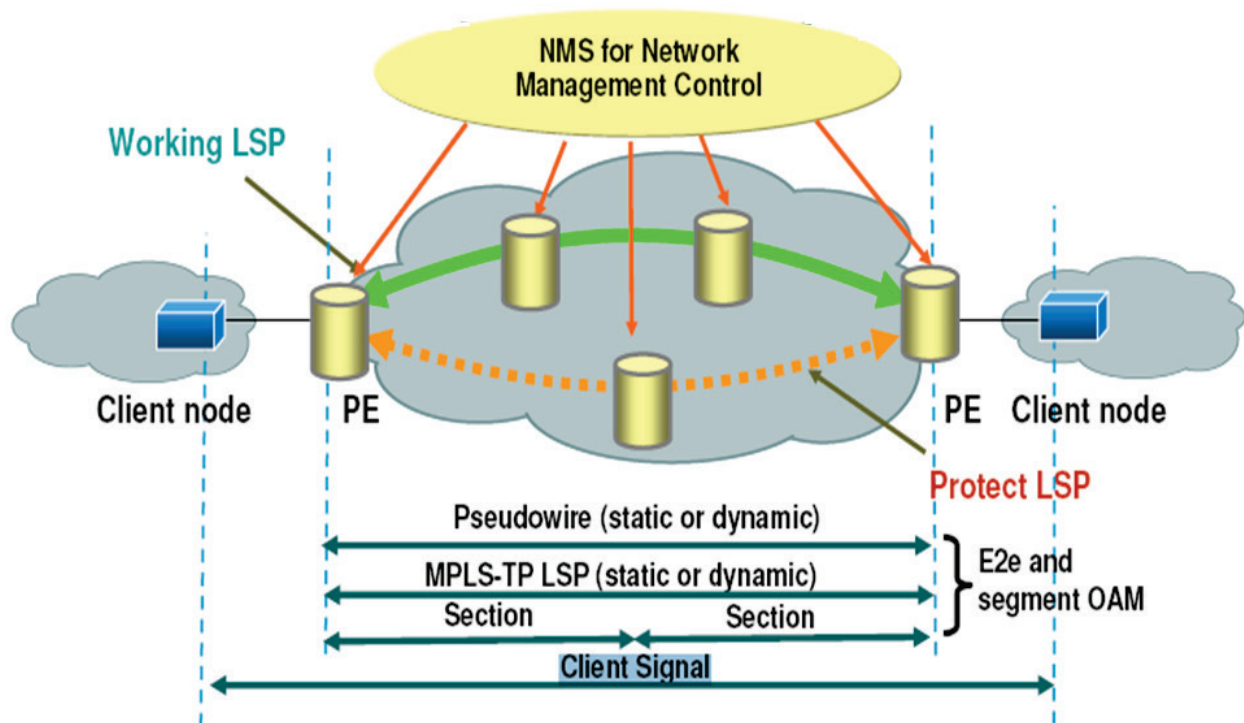
## Business Drivers for MPLS-TP

Time Division Multiplexing (TDM)-based technologies such as SONET/SDH have been playing the transport role for decades. They are not optimal, however, at handling bursty traffic, such as packetized video and voice. The explosion of wireless data has forced the rapid transformation of mobile backhaul infrastructure from TDM-based to Ethernet packet-based networks. On the one hand, MPLS is the preferred (and time proven) technology in the core data network. Carriers around the world have made significant investments to build new networks surrounding MPLS, and therefore, it is critical that converged networks continue to be based on MPLS. These networks, however, must be able to handle all types of traffic—data, mobile, voice and video—to minimize the cost and reduce CAPEX and OPEX. On the other hand, MPLS lacks the OAM and APS capabilities of SONET/SDH as well as support for static configuration (without complex dynamic signaling protocols involved) that carriers like to see for reliability and operational simplicity. Previous attempts with PBB-TE and T-MPLS have generated some momentum, but neither has gained the same traction as MPLS-TP, partly because of the joint effort by the IETF and ITU-T.

## What is MPLS-TP?

In a nutshell, MPLS-TP is a 'simplified' version of IP/MPLS, but with adaptations to make it more transport-like. The following are some of the distinct characteristics of MPLS-TP:

- Reduced MPLS forwarding plane functions (for example, no PHP, LSP merge, or ECMP) for both implementation and deployment simplicity
- Direct inheritance of PWE3 Pseudowire architecture, including device names (P, PE) and circuit names (LSP or PW)

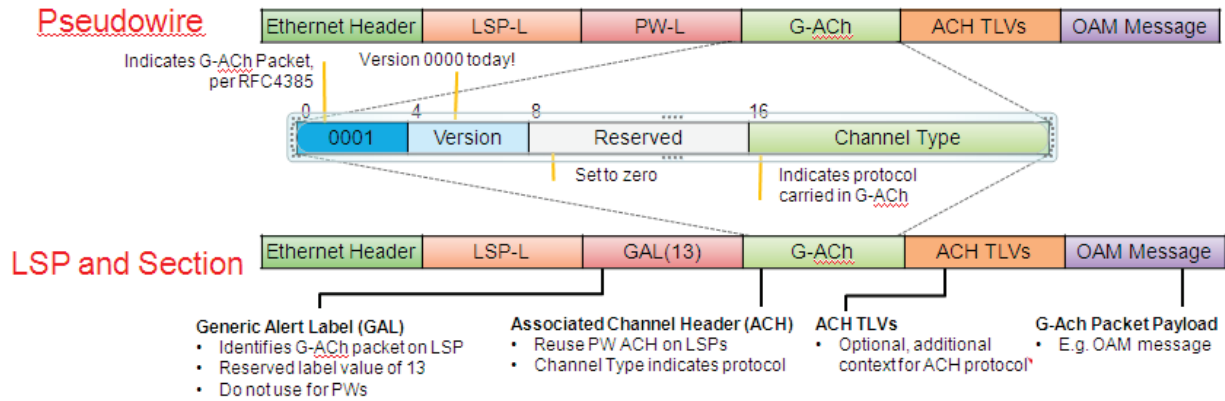


**Figure 1** MPLS-TP Architecture: Direct Inheritance from PWE3 but with Added Functions in OAM, Protection, and Static Configuration

- Centralized NMS management for circuit provisioning (static LSP/PW) or distributed control plane dynamic signaling through G-MPLS
- Major OAM enhancements and functions added for Performance Monitoring (LM, DM), APS, management and signaling communication channels (SCC, MCC)

## What is MPLS-TP?

- Generic Associated Channel (G-ACh) for in-band communication of all OAM, APS, and other types of Fault, Configuration, Accounting, Performance, and Security (FCAPS) functions



**Figure 2 G-ACh and GAL Encapsulation for MPLS-TP PW and LSP**

- Several protection schemes at the data plane similar to those available in traditional transport network (uni- or bi- directional 1:1 and 1+1, ring and linear)
- Synchronization in packet network

## Implementation Challenges of MPLS-TP

MPLS-TP is new to everyone. Many vendors are still in the process of implementation or about to start. There are a number of challenges that vendors are facing today.

### Interoperability

Apart from working functions, interoperability is the most important challenge that faces many vendors. MPLS-TP has introduced a new encapsulation (G-ACh and GAL) and Channel Types, some of which are yet to be defined for many important OAM functions, such as APS, LM, DM, LCK, AIS, and LDI. Channel Type definitions are also missing for some of the on-demand connectivity verification features, such as LSP Ping and Traceroute. This poses issues even for basic multi-vendor interoperability. Moreover, some of the specifications are updated frequently and this creates a gap between vendors who started early and vendors who started later. Sometimes, the specification between different drafts may not be backwards compatible even with basic message formats. This creates huge interoperability challenges. While the majority of vendors support static configuration of LSP and PW, fewer will likely implement the dynamic signaling of LSPs and PWs. Naturally, there is a challenge to do an end-to-end test with multiple segments of an LSP or PW, where some segments are statically configured, while others are dynamically signaled. The challenges range from a simple end-to-end continuity check, or a simple alarm generation and interpretation, to a more complex case where the PW status is statically configured on one part and dynamically exchanged on another.

### OAM

Over the past few years, Carrier Ethernet has made significant progress in the area of OAM. Some of the functions, such as CCM, LBM/LBR, RDI, AIS, DM, TST, and LCK have already been defined in CFM/Y.1731 and they can be directly ported over to MPLS-TP, if Y.1731 is the preferred mechanism. There is a growing interest, however, to use BFD as the generic and protocol independent failure detection mechanism among data centric devices. Choosing BFD means that new OAM functions need to be defined in conjunction with failure detection. New alarm types, for example, AIS, LCK, LDI, and performance monitoring functions, such as LM and DM, are required. There is also a need to use OAM to communicate static PW status to the far end in the case of Multi-Segment PW. On-demand connectivity verification such as LSP Ping and Traceroute are popular in IP/MPLS networks today and can be incorporated and adapted to use with BFD. If Y.1731 is chosen for both Continuity Check (CC) and alarm OAM, however, such on-demand connectivity verification mechanisms are yet to be defined. A full feature

set of OAM functions, coupled with separate CC sessions (at various detection intervals) for each working and protecting LSP and PW, while supporting various performance targets (per port, per card, per system), brings many implementation challenges for any MPLS-TP capable device.

### APS

Automatic Protection Switch (APS) has a reputation for protecting user traffic when failure occurs in a traditional transport network. APS is, however, new to packet-based data network. The closest concept in a data network to provide end-to-end protection is MPLS Fast ReRoute (FRR). It offers protection against either link or node failure, but does not provide protection granularity for individual LSPs or PWs. Additionally, it requires Traffic Engineering (TE) support from routing and MPLS signaling protocols. Configuring MPLS FRR requires in-depth knowledge of data networking and it does not resemble in any way the old and good APS commonly seen in a TDM network where the network operators can issue some simple commands to cause a switchover.

Several protection switching mechanisms have been defined in the past, such as unidirectional versus bidirectional, 1:1 versus 1+1, and linear versus ring topology. MPLS-TP needs to support all of them to be comparable to the existing transport networks. A rich set of triggers, both manual and automatic, needs to be defined to make APS more robust against failure and service disruptions. Note that, however, APS can be applied to either an individual LSP or PW. When the number of working and protecting paths reaches thousands to tens of thousands, ensuring that each working path can be switched over in sub-50 ms in the event of failure, it is very challenging to deliver a robust system that meets the expectation of a transport device.

Additionally, an MPLS-TP device must be tested for different functions when participating in different APS roles. An ingress P/PE router in a protected domain is responsible for monitoring all LSPs and PWs and detecting any error conditions. Should an error occur either because of loss of continuity, or loss of physical signal (or other vendor specific reasons), the ingress P/PE router is responsible for switching over all data plane traffic to protecting paths. The relationship between a working PW and an underlying working LSP which is in turn being protected by another protecting LSP is complex and also falls into the responsibility of an ingress P/PE node. Briefly stated, PWs within an LSP should only be switched over to protecting PWs if and only if both the working LSP and protecting LSP cease to work. This requires extra processing on the ingress node to correlate events with nested protection mechanisms. When a DUT functions as a transit node, processing overhead because of control plane and data plane activities is relatively light—similar to a P router in an MPLS network. When a DUT functions as an egress node, it must select the right data plane traffic based on the protection type and Protocol State Coordination (PSC) messages. In addition, the

egress node must terminate and maintain the right state for the failure detection mechanism, either Y.1731 CCM or BFD.

### MS-PW

Single segment PWs usually exist in a single operator and administrative domain. For MPLS-TP to become a major transport technology for mobile backhaul and access aggregation, it must traverse multiple domains to provide end-to-end services. In this perspective, PWs traversing multiple domains automatically become Multi-Segment PWs (MS-PWs). By definition, a MS-PW consists of many Single-Segment PWs (SS-PWs) where each SS-PW could possess different properties. For example, some segments may be statically configured, and others may be dynamically signaled. The signaling protocol for the dynamic segments could vary as well—there is a choice of using LDP with FEC128 or FEC 129, or even using L2TPv3. While protocols like LDP have the ability to propagate PW status to the far end, a static PW has no such ability, so it must rely on other means such as OAM to provide this. Areas of concern also exist in the interoperability of PW status between a device running OAM and a device running LDP (or another protocol).

APS with MS-PW must work similar to the case of a SS-PW. Each segment of the PW must be responsible for its own CC and CV operations. When a failure occurs, the trigger to switch traffic from working to protecting LSP or PW must be end-to-end.

### IP/MPLS and MPLS-TP Internetworking

An MS-PW consists of multiple SS-PWs where each segment may be established by using different methods, such as static configuration or targeted LDP for dynamic signaling. This idea can be further extended to have some segments of an end-to-end PW traverse an MPLS-TP enabled network while others traverse an IP/MPLS only network. Existing MPLS networks have well established means for signaling (LDP, RSVP-TE, MP-BGP) and fault detection (CFM, BFD, VCCV). To make an end-to-end PW work in this case, the devices that support MPLS-TP on one end and MPLS on the other may need to bridge the continuity check and translation of alarms between the two networks. Additionally, the device would need to provide mapping of APS commands from MPLS-TP to something such as FRR in IP/MPLS. The challenge in this case is the fact that there are few open standards to guide how the mapping or translation is done for CC, CV, Alarms, or even APS between MPLS-TP and IP/MPLS networks. Expect continued standardization work in this area.





## **Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW**

### **Overview**

G-ACh encapsulation for MPLS-TP PW and G-ACh plus GAL encapsulation for MPLS-TP LSP allow an in-band OAM operation along the same path data plane traffic traverses. The idea is very similar to carrying Control Word (CW) for an L2VPN Frame Relay or ATM circuits. G-ACh will be identified by two ends of a pseudowire but will not be visible to any of the transit nodes. GAL (label value 13), on the other hand, is intended to alert the transit node of an LSP to inspect the packet and delineate the G-ACh encapsulated OAM PDU. One of the very basic MPLS-TP function is to ensure that both Y.1731CCM and BFD are working seamlessly with the new encapsulation for both LSP and PW, and also works at various Continuity Check Interval (CCI).

### **Objective**

To test basic interoperability of the DUT to ensure that either Y.1731 CCM or BFD can operate seamlessly within G-ACh encapsulation for PW, or G-ACh plus GAL encapsulation for LSP. In addition, to verify that CCM and BFD can run at various Continuity Check Interval (CCI).

## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

### Setup

One or more Ixia test ports can be used to carry out this interoperability test. Ixia can be used to emulate either Ingress PE or Egress PE, or both as depicted in the following diagram.

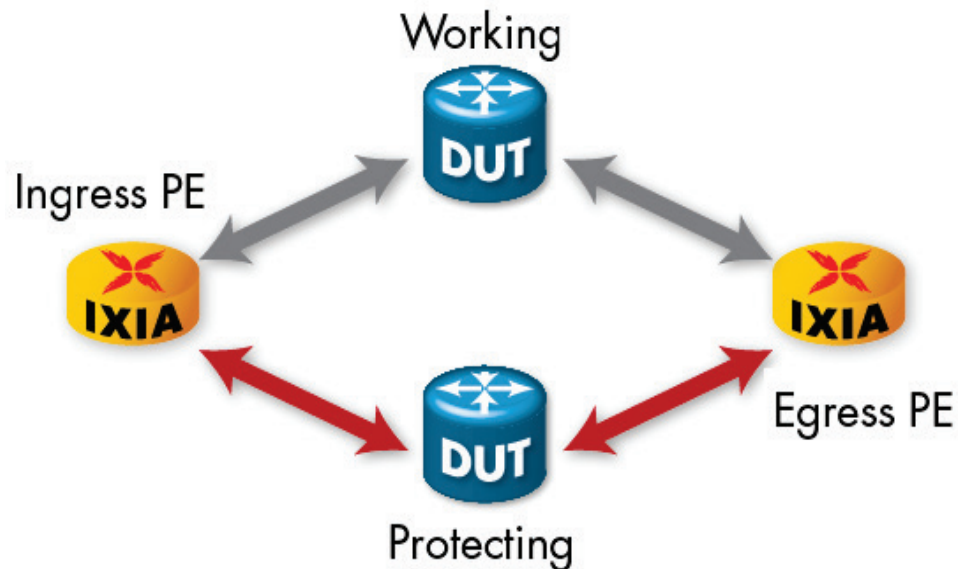
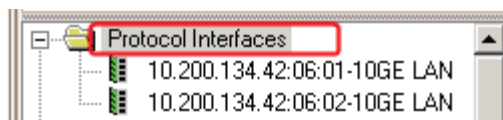


Figure 3 Test Setup for Testing BFD Interop with G-ACh and GAL Encapsulation

### Step-by-Step Procedures by using IxNetwork

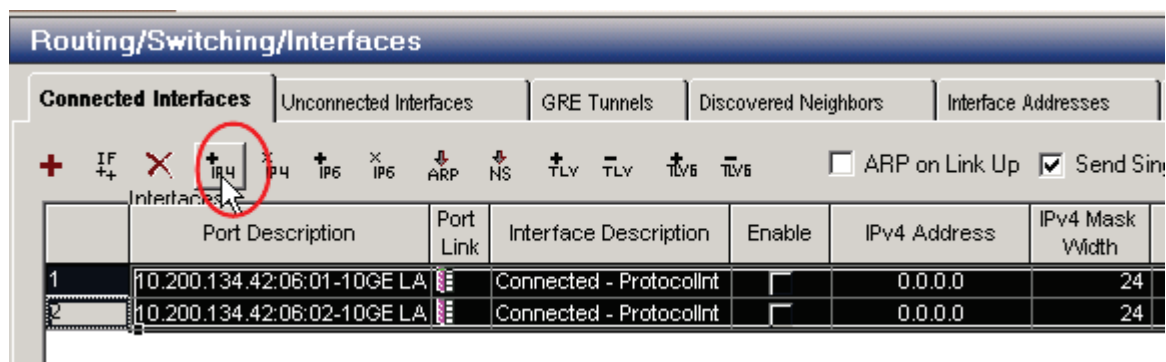
Note: You can configure the test by either using the MPLS-TP wizard or performing the steps manually. As an example, the following steps show the manual approach. Other tests later will show the use of the wizard.

1. Create a Protocol Interface that may contain a valid IP address. Note that MPLS-TP does not depend on IP or VLAN ID, so both are optional. If the DUT does not handle broadcast MAC, note down the DUT MAC address from Discovered Neighbors.
  - a. Click the Protocol Interfaces folder under the Routing/Switching/Interfaces selection.



Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

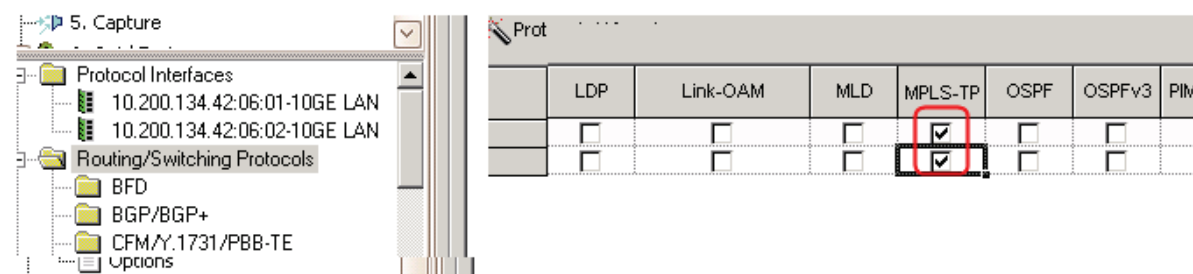
- b. Click to highlight the test port(s) and add an IP address to the protocol interfaces. Change the IP address, as appropriate, and enable the protocol interfaces.



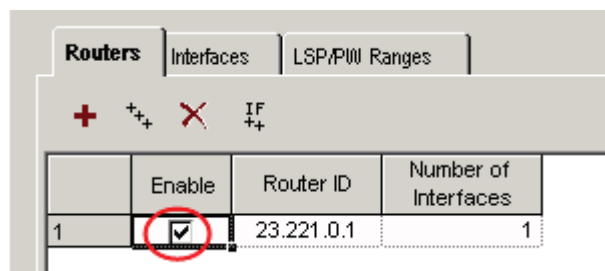
- c. Select the Discovered Neighbors and note down the learned MAC address. This will be used by MPLS-TP config later on.

Connected Interfaces		Unconnected Interfaces	GRE Tunnels	Discovered Neighbors	Interface Address
Port Name	Neighbor IP	Neighbor MAC	Router		
10.200.134.42:06:01-10GE	20.20.20.1	00:00:1a:08:e5:bf			
10.200.134.42:06:02-10GE	20.20.20.2	00:00:1a:08:e5:be			

2. Click the Routing/Switching Protocols folder and select the MPLS-TP check boxes.



3. Click the MPLS-TP folder in the protocol tree pane, and then click the **Routers** tab. Enable the emulated router by selecting the check box.



# Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

4. Configure the Interface to bind the protocol interface created in step 1, and enter the DUT MAC address, which is also noted in step 1. Enable the interface by selecting the check box and enter the number of LSP/PW Ranges as 2.

	Router ID	Enable	Protocol Interface	Dut MAC Address	Number of LSP/PW Ranges
1	23.221.0.1 - (10.200.134.42:06:01-10GE LAN)	<input checked="" type="checkbox"/>	Connected - ProtocolInterface	00 00 1A 08 E5 BF	2

5. Configure the LSP/PW Ranges as follows:

## a. General tab:

Enabled: selected

Type of Ranges: LSP

Range Role: the first range as Working and the second range as Protect

Protect LSP/PW Range: click to select the description that matches the second range

CCCV Type: BFD CC

APS Type: IETF

	Interface	Enable	Description	Type of Range	Range Role	Protect LSP/PW Range	CCCV Type	APS Type
1	Connected - ProtocolInterface - 100.01 -	<input checked="" type="checkbox"/>	IXIA.0001.0001.0001.0001	LSP	Working	IXIA.0001.0001.0001.0002	BFD CC	IETF
2		<input checked="" type="checkbox"/>	IXIA.0001.0001.0001.0002	LSP	Protect		BFD CC	IETF

## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

### b. Static Label Range tab:

Number of LSPs: 2

LSP Outgoing Label: 100 for working and 200 for protect

LSP Incoming Label: 1000 for working and 2000 for protect

The screenshot shows the 'Static Label Range' configuration tab. At the top, there is a note: 'To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field'. Below this is a table with columns: Interface, Enable, Number of LSPs, Number of PWs per LSP, LSP Outgoing Label, LSP Incoming Label, PW Outgoing Label, and PW Incoming Label. Two rows are visible, both with 'Enable' checked. Row 1 has 'Number of LSPs' set to 2, 'LSP Outgoing Label' set to 100, and 'LSP Incoming Label' set to 1000. Row 2 has 'LSP Outgoing Label' set to 200 and 'LSP Incoming Label' set to 2000. At the bottom, there is a navigation bar with tabs: General, Static Label Range (selected), ICC MEP/MEG IDs, IP MEP/MEG IDs, CCCV, APS, Triggered Reply, Static MAC Range, Static IP Range, and All.

	Interface	Enable	Number of LSPs	Number of PWs per LSP	LSP Outgoing Label	LSP Incoming Label	PW Outgoing Label	PW Incoming Label
1	Connected - ProtocolInterface - 100:01 -	<input checked="" type="checkbox"/>	2		100	1000		
2		<input checked="" type="checkbox"/>			200	2000		

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

c. The next two tabs called ICC MEP/MEG IDs and IP MEP/MEG IDs are for Y.1731. We will skip them for this test as this test is using BFD as the failure detection mechanism.

### d. CCCV tab:

CCCV Type: BFD CC

CCCV Interval: 1000 ms

The screenshot shows the 'CCCV' configuration tab. At the top, there is a note: 'To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field'. Below this is a table with columns: Interface, Enable, CCCV Type, CCCV Interval (ms), CCCV Traffic Class, and Support Slow Start. Two rows are visible, both with 'Enable' checked. Row 1 has 'CCCV Type' set to BFD CC, 'CCCV Interval (ms)' set to 1000, 'CCCV Traffic Class' set to 7, and 'Support Slow Start' unchecked. Row 2 has 'CCCV Type' set to BFD CC, 'CCCV Interval (ms)' set to 1000, 'CCCV Traffic Class' set to 7, and 'Support Slow Start' unchecked. At the bottom, there is a navigation bar with tabs: General, Static Label Range, ICC MEP/MEG IDs, IP MEP/MEG IDs, CCCV (selected), APS, Triggered Reply, Static MAC Range, Static IP Range, and All.

	Interface	Enable	CCCV Type	CCCV Interval (ms)	CCCV Traffic Class	Support Slow Start
1	Connected - ProtocolInterface - 100:01 -	<input checked="" type="checkbox"/>	BFD CC	1000	7	<input type="checkbox"/>
2		<input checked="" type="checkbox"/>	BFD CC	1000	7	<input type="checkbox"/>

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

### d. APS tab:

APS Type: IETF

Type of Protection Switching: 1:1 Bidirectional

The screenshot shows the 'APS' configuration tab. At the top, there is a note: 'To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field'. Below this is a table with columns: Interface, Enable, APS Type, Type of Protection Switching, Revertive, Wait To Revert Time (ms), and APS. Two rows are visible, both with 'Enable' checked. Row 1 has 'APS Type' set to IETF, 'Type of Protection Switching' set to 1:1 Bidirectional, 'Revertive' unchecked, and 'Wait To Revert Time (ms)' set to 0. Row 2 has 'APS Type' set to IETF, 'Type of Protection Switching' set to 1:1 Bidirectional, 'Revertive' unchecked, and 'Wait To Revert Time (ms)' set to 0. At the bottom, there is a navigation bar with tabs: General, Static Label Range, ICC MEP/MEG IDs, IP MEP/MEG IDs, CCCV, APS (selected), Triggered Reply, Static MAC Range, Static IP Range, and All.

	Interface	Enable	APS Type	Type of Protection Switching	Revertive	Wait To Revert Time (ms)	APS
1	Connected - ProtocolInterface - 100:01 -	<input checked="" type="checkbox"/>	IETF	1:1 Bidirectional	<input type="checkbox"/>	0	
2		<input checked="" type="checkbox"/>	IETF	1:1 Bidirectional	<input type="checkbox"/>	0	

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

- e. Optionally, configure Static MAC or IP for traffic generation and verification.

Static IP Range tab:

IP Host per LSP: 1

IP Address: 100.100.100.100

	Interface	Enable	IP Host per LSP	IP Type	IP Address	IP Mask	IP Address Step
1	Connected - ProtocolInterface - 100:01 -	<input checked="" type="checkbox"/>	1	IPv4	100.100.100.100	24	1
2		<input checked="" type="checkbox"/>					

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range **Static IP Range** All

6. Optionally, enable and turn on Capture before starting the protocol.

**Test Configuration**

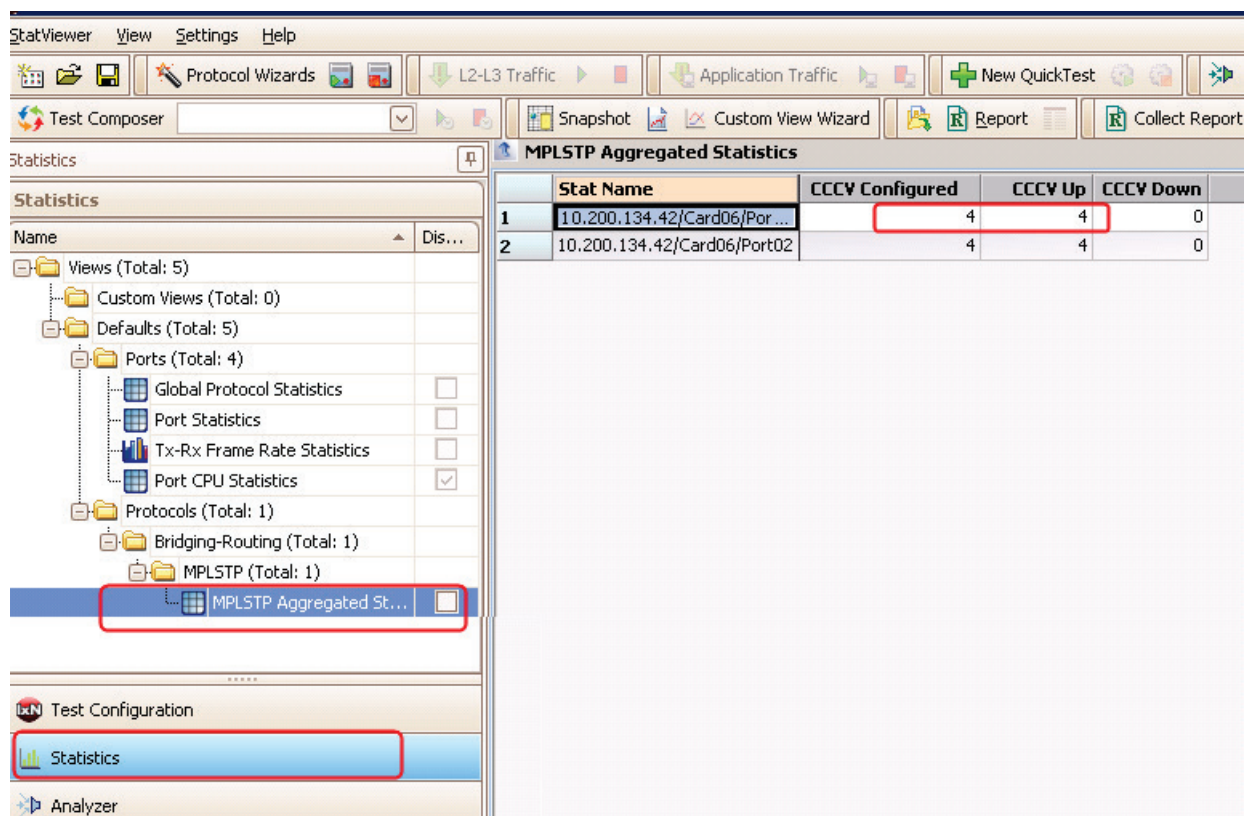
- 1. Port Manager
- 2. Protocols
  - Routing/Switching/Interfaces
  - Auth/Access Hosts/DCB
  - Traffic Groups
  - Options
- 3. Traffic
  - Options
- 4. Statistic Setup
- 5. Capture**
- 6. QuickTests

**Groups** **Protocols**

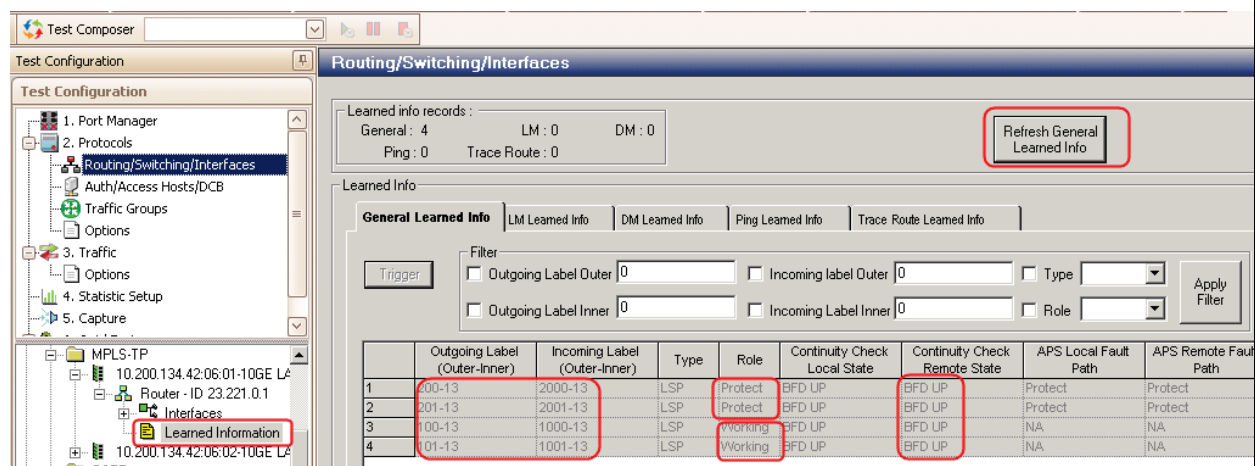
- 10.200.134.42:06:01-10GE LAN
  - ☒ Data
  - ☒ Control
- 10.200.134.42:06:02-10GE LAN
  - ☒ Data
  - ☒ Control

## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

- Start the protocol. Next, click the **Statistics** tab, and then click **MPLSTP Aggregated Stats**. It displays the total number of CCCV sessions configured as well as the Up/Down sessions. In this example, we have 4 sessions because there are two protect LSPs protecting two working LSPs.



- The other place to verify if all BFD sessions are up or not is to navigate to the **MPLS-TP** -> **Learned Information** folder and click **Refresh General Learned Info**. It displays clearly each BFD session status and its incoming and outgoing labels.





## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

9. Optionally, use IxAnalyzer to capture or check the details of working or failed sessions. It displays both the PSC message and BFD CC messages.

10.200.134.42:06:01-10GE LAN - Control

**Network Packets (132 items)**

Packet No	Time	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	00:00:06.358747	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP PSC
0002	00:00:06.358784	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP PSC
0003	00:00:06.362212	34 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP PSC
0004	00:00:06.362258	34 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP PSC
0005	00:00:06.859305	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP BFD-CC
0006	00:00:06.859334	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP BFD-CC
0007	00:00:06.859341	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP BFD-CC
0008	00:00:06.859348	60 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP BFD-CC
0009	00:00:06.861800	50 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP BFD-CC
0010	00:00:06.861837	50 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP BFD-CC

Tree packet

**MPLS-TP BFD-CC MPLS, Label Stack: 2000:13, MPLS-TP BFD-CC**

BFD Control message

- 001 . .... = Protocol Version: 1
- ...0 0000 = Diagnostic Code: No Diagnostic (0x00)
- .... .01 = Session State: Down (0x01)
- + .00 1000 = Message Flags: 0x08
- Detect Time Multiplier: 3 (= 3000 ms Detection time)
- Message Length: 24 Bytes
- My Discriminator: 0x00000001
- Your Discriminator: 0x00000000

00:00:1A:08:E5:BF  
MPLS-TP BFD-CC Endpoint

5.859305 MPLS, Label Stack: 2000:13, MPLS-TP BFD-CC

5.859334 MPLS, Label Stack: 2001:13, MPLS-TP BFD-CC

5.859341 MPLS, Label Stack: 1000:13, MPLS-TP BFD-CC

5.859348 MPLS, Label Stack: 1001:13, MPLS-TP BFD-CC

7.859145 MPLS, Label Stack: 2000:13, MPLS-TP BFD-CC

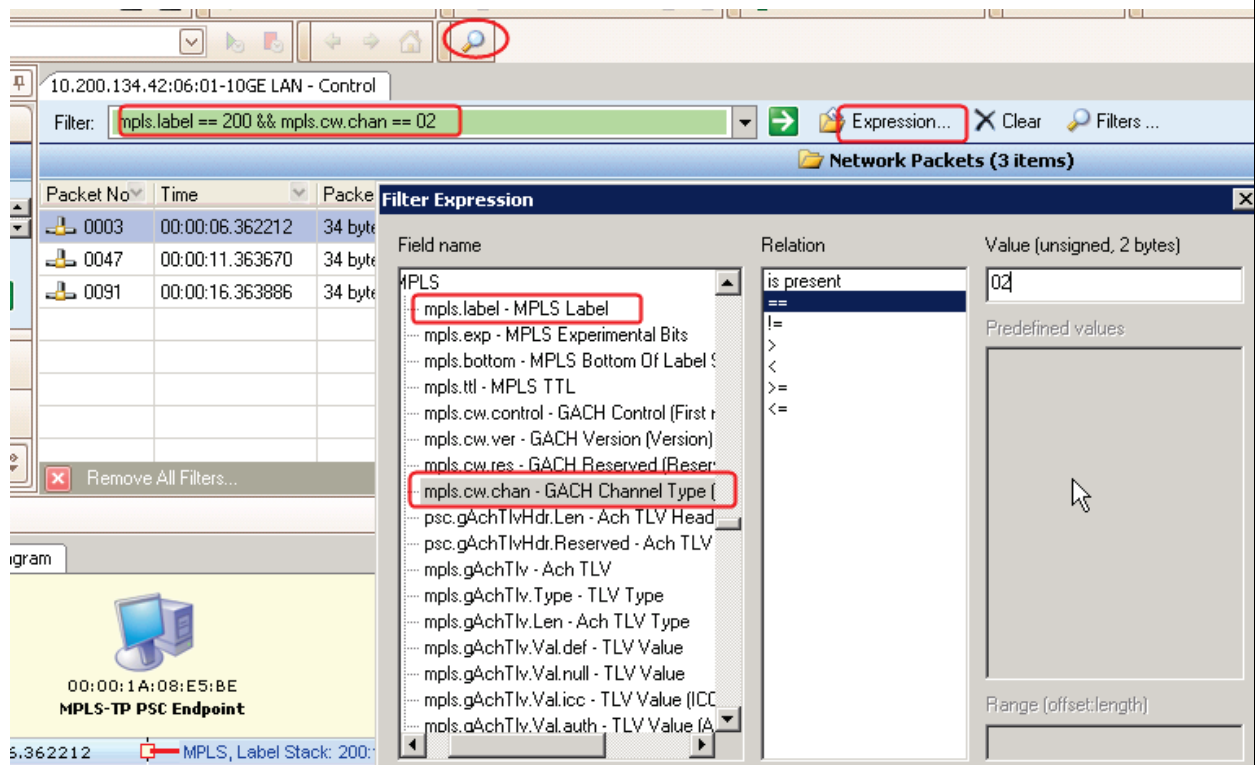
7.859170 MPLS, Label Stack: 2001:13, MPLS-TP BFD-CC

```

00000000 FF FF FF FF FF FF 00 00 1A 08 E5 BF 88 47 00 7D
00000010 0E 40 00 00 DF 01 10 00 00 07 20 48 03 18 00 00
00000020 00 01 00 00 00 00 00 0F 42 40 00 0F 42 40 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

## Test Scenario 1: Verify BFD functionality with G-ACh (and GAL) encapsulation over static MPLS-TP LSP or PW

10. In addition, use the IxAnalyzer advanced filter feature to narrow down specific messages for specific LSPs. In a large setup with many LSP or PW, this is extremely helpful.



## Test Variables

The following are possible test variables:

- IETF or Y.1731 choice of CCCV and APS
- Number of static LSPs and PWs
- LSP versus PW or a mix of both
- CCCV Interval from large to small
- Protection mode: 1:1 or 1+1, unidirectional or bidirectional



## Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

### Overview

G-ACh encapsulation for MPLS-TP PW and G-ACh plus GAL encapsulation for MPLS-TP LSP allow an in-band OAM operation along the path data plane traffic traverses. Just like the Continuity Check for failure detection, the OAM messages for alarm generation and failure propagation is another basic MPLS-TP interop test.

### Objective

To test basic interoperability of the DUT to ensure that either Y.1731 or IETF alarm and other OAM functions can operate seamlessly within G-ACh encapsulation for PW, or G-ACh plus GAL encapsulation for LSP.

### Setup

One or more Ixia test ports can be used to carry out this interoperability test. Ixia can be used to emulate either Ingress PE or Egress PE, or both.

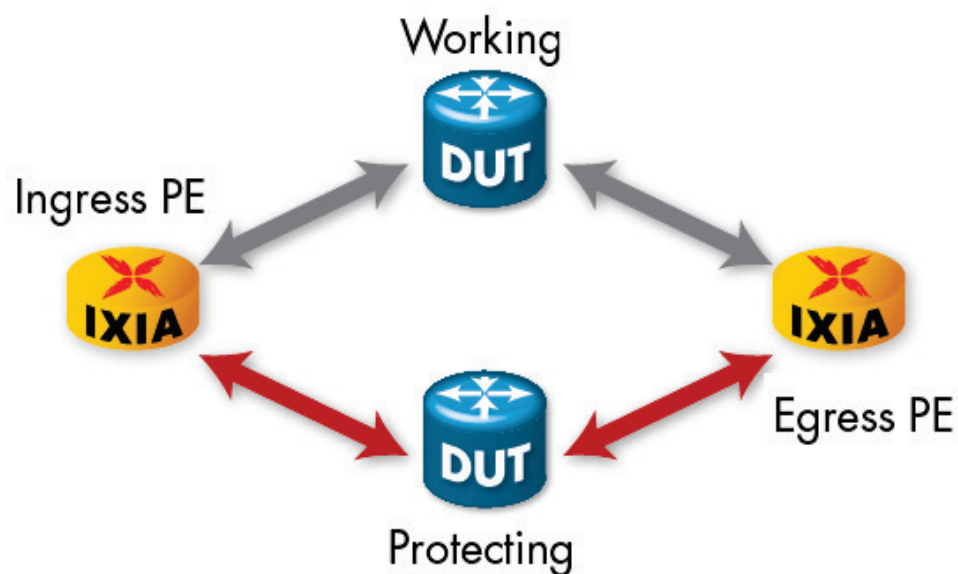


Figure 4 Test Setup for Testing MPLS-TP OAM Functions

## Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

### Step-by-Step Procedures by using IxNetwork

1. Continue from the previous test. Keep the protocol interfaces and the MPLS-TP routers, interfaces, and LSP/PW ranges. Change CCCV and APS types to use Y.1731.

Routers Interfaces LSP/PW Ranges							
To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field							
	Enable	Description	Type of Range	Range Role	Protect LSP/PW Range	CCCV Type	APS Type
1	<input checked="" type="checkbox"/>	IXIA.0001.0001.0001.0001	LSP	Working	IXIA.0001.0001.0001.0002	Y.1731	Y.1731
2	<input checked="" type="checkbox"/>	IXIA.0001.0001.0001.0002	LSP	Protect		Y.1731	Y.1731

2. In addition, change the MEG ID and MEP IDs to match that of DUT.

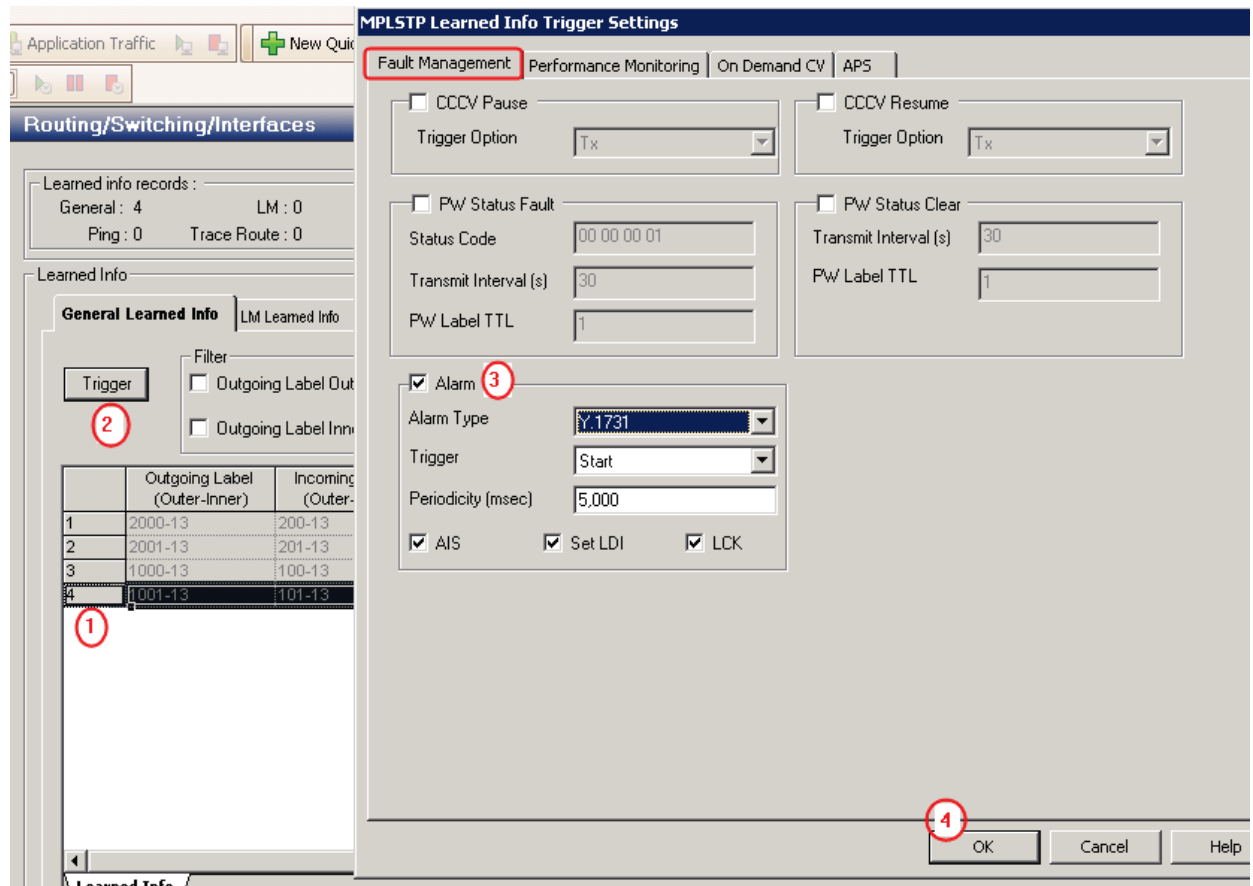
Routers Interfaces LSP/PW Ranges						
To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field						
	Interface	Enable	MEG ID Prefix	Src MEP ID	Dest MEP ID	MEG ID Integer Step
1	Connected - ProtocolInterface - 100.01 -	<input checked="" type="checkbox"/>	ixia-0001	10	30	0
2		<input checked="" type="checkbox"/>	ixia-0002	20	40	0

3. Start the MPLS-TP emulation and ensure that all Y.1731 CCM reach the UP state. This can be verified either from the aggregated CCCV stats or through the **Learned Info** pane.

Routing/Switching/Interfaces									
<p>Learned info records :</p> <p>General : 4    LM : 0    DM : 0</p> <p>Ping : 0    Trace Route : 0</p> <p>Refresh General Learned Info</p>									
<p>Learned Info</p> <p>General Learned Info    LM Learned Info    DM Learned Info    Ping Learned Info    Trace Route Learned Info</p> <p>Filter</p> <p>Trigger</p> <p>Outgoing Label Outer 0    Incoming label Outer 0    Type    Apply Filter</p> <p>Outgoing Label Inner 0    Incoming Label Inner 0    Role    Apply Filter</p>									
	Outgoing Label (Outer-Inner)	Incoming Label (Outer-Inner)	Type	Role	Continuity Check Local State	Continuity Check Remote State	APS Local Fault Path	APS Remote Fault Path	APS Local Path
1	2000-13	200-13	LSP	Protect	NA	Y1731 UP	None	NA	Working
2	2001-13	201-13	LSP	Protect	NA	Y1731 UP	None	NA	Working
3	1000-13	100-13	LSP	Working	NA	Y1731 UP	NA	NA	NA
4	1001-13	101-13	LSP	Working	NA	Y1731 UP	NA	NA	NA

Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

4. To inject Alarms to DUT, do the following:
  - a. Under the **Learned Info** pane, click to select the LSP/PW(s) that you want to inject alarms to.
  - b. Click **Trigger**.
  - c. Select the **Alarm** check box.
  - d. In the **Alarm Type** list, click **Y.1731**. Toggle the supported Alarms.
  - e. Click **Ok** to start sending the selected alarms periodically.
  - f. Click **Cancel** if you want to stop periodical alarms.



## Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

- To monitor Alarms from DUT, start the capture and use IxAnalyzer to decode the alarms from DUT.

**Network Packets (214 items)**

Packet No.	Time	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0095	00:00:11.085682	101 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP Y1731 CCM
0096	00:00:11.085689	101 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP Y1731 CCM
0097	00:00:11.110122	101 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 CCM
0098	00:00:11.110141	101 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 CCM
0099	00:00:11.110153	101 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 CCM
0100	00:00:11.110164	101 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 CCM
0101	00:00:11.980986	31 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 AIS
0102	00:00:11.981031	31 bytes	00:00:1A:08:E5:BE	00:00:1A:08:E5:BF			MPLS-TP Y1731 LCK
0103	00:00:12.086149	101 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP Y1731 CCM
0104	00:00:12.086169	101 bytes	00:00:1A:08:E5:BF	FF:FF:FF:FF:FF:FF			MPLS-TP Y1731 CCM

**Tree packet**

**MPLS-TP Y1731 AIS MPLS, Label Stack: 101:13, MPLS-TP Y1731(AIS)**

- CFM
  - MEG Level: 7
  - Version: 0
  - OpCode: Alarm Indication Signal (33)
  - Flags: 0x04 (AIS Period = 1 s)
  - First TLV Offset: 0
  - Alarm Indication Signal**
  - End TLV

**00:00:1A:08:E5:BE MPLS-TP Y1731 AIS Endpoint**

978847 - MPLS, Label Stack: 101:13, MPLS-TP Y

979086 - MPLS, Label Stack: 101:13, MPLS-TP Y

980986 - MPLS, Label Stack: 101:13, MPLS-TP Y

980228 - MPLS, Label Stack: 101:13, MPLS-TP Y

982142 - MPLS, Label Stack: 101:13, MPLS-TP Y

00000000 00 00 1A 08 E5 BF 00 00 1A 08 E5 BE 88 47 00 06 ^@.....

00000010 5E 40 00 00 DF 01 10 00 7F FA E0 21 04 00 00 .....@.....

Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

6. To send other OAM functions, such as Loss Measurement and Delay Measurement, click the **Performance Monitoring** tab within the trigger window.

The screenshot shows the 'MPLSTP Learned Info Trigger Settings' dialog box with the 'Performance Monitoring' tab selected. The 'DM Trigger' section is checked and expanded, showing settings for Delay Measurement. The 'LM Trigger' section is also checked and expanded, showing settings for Loss Measurement. Red circles highlight the checkmarks for both triggers, and a red rectangle highlights the 'Performance Monitoring' tab.

MPLSTP Learned Info Trigger Settings			
Fault Management		Performance Monitoring	On Demand CV   APS
<b>DM Trigger</b>			
DM Type	Y.1731	DM Interval (ms)	1,000
DM Iterations	10	Last DM Response Timeout (ms)	1,000
DM Mode	Response Expected	DM Time Format	NTP
DM Pad Len	0	<input type="checkbox"/> DM Request Padded reply	
DM Traffic Class	7		
<b>LM Trigger</b>			
LM Type	Y.1731	LM Interval (ms)	1,000
LM Iterations	10	Last LM Response Timeout (ms)	1,000
LM Mode	Response Expected	Counter Type	32 Bit
LM Initial Tx Value	0 : 1000	LM Tx Step	0 : 1000
LM Initial Rx Value	0 : 1000	LM Rx Step	0 : 1000
LM Traffic Class	7		

OK Cancel Help



Test Scenario 2: Verify Y.1731 and IETF Alarm OAM functions over static MPLS-TP LSP or PW with G-ACh (and GAL) encapsulation

7. To verify LM and DM response from DUT, click the **LM/DM Learned Info** tab and click **Refresh General Learned Info** to view the latest information.

The screenshot shows a web-based interface for monitoring network information. At the top, there's a section titled 'Learned info records:' with statistics for General (4), LM (1), DM (1), Ping (0), and Trace Route (0). A button labeled 'Refresh General Learned Info' is highlighted with a red rectangle. Below this is a tabbed interface with five tabs: 'General Learned Info', 'LM Learned Info' (which is selected and highlighted with a red rectangle), 'DM Learned Info', 'Ping Learned Info', and 'Trace Route Learned Info'. Under the 'LM Learned Info' tab, there is a table with the following data:

	Outgoing Label (Outer-Inner)	Incoming Label (Outer-Inner)	Type	LM Queries Sent	LM Responses Received	Last LM Response My Tx	Last LM Response
1	1001-13	101-13	LSP	10	0	0	0

## Test Variables

The following are possible test variables:

- Y.1731 or IETF
- Alarms and applicable OAM functions
- LSP or PW or a mix of both
- Number of static LSPs and PWs

## Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

### Overview

APS is the central piece of a successful implementation of MPLS-TP. While it is well understood in TDM-based transport technologies, it is fresh and new to packet-based transport, such as MPLS-TP. The critical part is that the switchover triggered by manual commands or by some kind of active alarms, from working path to protecting path, should be sub-50 ms in service disruption. This is easily said than done, especially in the case where hundreds or even thousands of working LSP/PW are switched over simultaneously and possibly with mixed type of triggers.

### Objective

To test the DUT ability, as ingress router, to perform linear APS in case of failure (LoC) and switch traffic from working path to protecting path, and to benchmark the APS performance by measuring the switchover time with respect to the total number of LSP/PWs under test, and various protection modes.

### Setup

A minimum of two test ports are required to perform this test. One test port will be used as traffic source, and the other port or ports are used to simulate LSP or PW tunnel end-points. DUT is the ingress PE of both working and protecting tunnel.

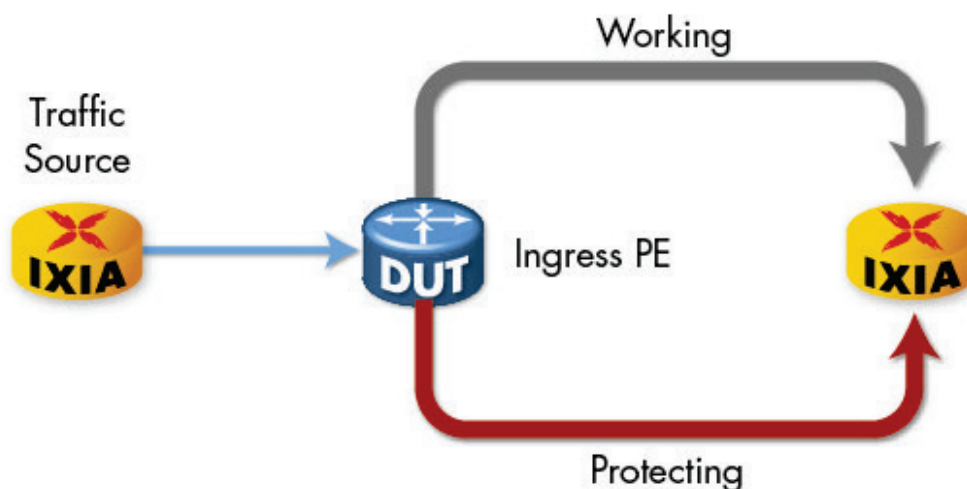
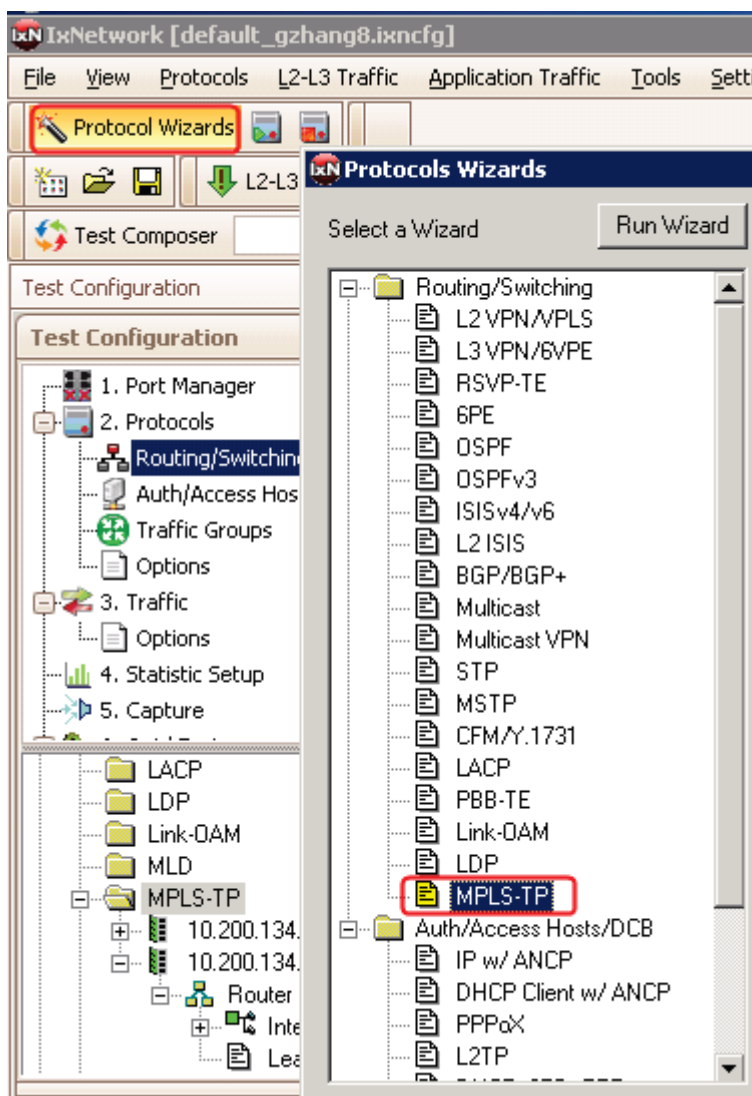


Figure 6 Test Setup for Testing Linear APS and Switchover Time

## Step-by-Step Procedures by using IxNetwork

1. Start the protocol wizard and click **MPLS-TP** to run the MPLS-TP wizard.



### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

- In the first page of the MPLS-TP wizard, configure the following:

DUT = Ingress

Protection Type = 1:1 Bidirectional

Traffic Src/Sink: first test port

Tunnel Head/Tail Port: second test port

	Tunnel Head/Tail Port	Traffic Src/Sink Port	Port Description
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.200.134.42:06:01-10GE LAN - LAN/W
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.200.134.42:06:02-10GE LAN - LAN/W

- In the second page of the wizard, configure the following:

Number of Routers Per Port: 1

Enable IP Address: selected

Router IP Address: enter value to match DUT's subnet

DUT MAC: leave default broadcast or enter DUT's MAC

☐ Enable VLAN

VLAN ID: 100 Increment By: 1

☐ Repeat VLAN Across Ports ☐ Use Same VLAN for All Emulated Routers

Number of Routers Per Port: 1

☒ Enable IP Address

Router IP Address: 20.20.20.2/24 DUT IP Address: 20.20.20.1

Increment Per Router: 0.0.0.1 Increment Per Port: 1.0.0.0

☐ Continuous Increment Across Ports

DUT MAC Addresses

	Port	Router	Interface	DUT MAC
1	10.200.134.4	Router - 1	Interface - 1	FF FF FF FF FF FF

### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

4. In the third page of the wizard, configure the following:

Static MPLS-TP LSP: selected

Number of LSPs per Router: 10

Working LSP Outgoing Label: 100

Working LSP Incoming Label: 1000

Protecting LSP Outgoing Label: 200

Protecting LSP Incoming Label: 2000

The rest of the parameters: keep the default values

Static LSPs

MPLS-TP Tunnel Type

- ☒ Static MPLS-TP LSP
- ☐ Static L2VPN PW
- ☐ Both

Static LSP Properties

Number of LSPs Per Router: 10

Working LSP Outgoing Label

Outgoing Label: 100

Increment Per LSP: 1

Increment Per Router: 1

Increment Per Port: 1

Working LSP Incoming Label

Incoming Label: 1,000

Increment Per LSP: 1

Increment Per Router: 1

Increment Per Port: 1

Protecting LSP Outgoing Label

Outgoing Label: 200

Increment Per LSP: 1

Increment Per Router: 1

Increment Per Port: 1

Protecting LSP Incoming Label

Incoming Label: 2,000

Increment Per LSP: 1

Increment Per Router: 1

Increment Per Port: 1

### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

5. In the fourth page of the wizard, configure the following:

Global Identifier Type: IETF

PSC Type: IETF

CC-CV Type: BFD CC

CC-CV Interval: Select from the list or enter a specific value

The rest of the parameters: keep the default values

The screenshot shows a configuration window titled "Protocol Behavior" with several sections for setting protocol parameters. The following table summarizes the visible settings:

Section	Parameter	Value
Global Identifier Type	IETF	Selected
	ICC	Not selected
PSC Type	IETF	Selected
	Y.1731	Not selected
CC-CV Type	BFD CC	Selected
	Y.1731	Not selected
CC-CV Interval	Interval	100 ms
	Unit	ms
On-demand CV Type	IETF	Selected
	Y.1731	Not selected
Alarm Type	IETF	Selected
	Y.1731	Not selected
DM Type	IETF	Selected
	Y.1731	Not selected
Periodic DM Mode	1-way	Not selected
	2-way	Selected
Periodic DM Time Format	IEEE	Selected
	NTP	Not selected
LM Type	IETF	Selected
	Y.1731	Not selected
Periodic LM Reply Mode	In Band	Selected
	No Reply	Not selected

### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

- The fifth page of the wizard is not applicable to IETF or BFD. If Y.1731 is used, ensure to enter the Src MEP ID and Dest MEP ID for both working LSP and Protecting LSP.

The screenshot shows the 'MEG Configuration' and 'MEP Configuration' sections of a wizard. The 'MEG Configuration' section has two columns: 'Working LSP/PW' and 'Protecting LSP/PW'. Each column has 'MEG ID Prefix' and 'MEG ID Integer Step' fields. The 'MEP Configuration' section also has two columns: 'Working LSP/PW' and 'Protecting LSP/PW'. Each column has four rows of fields: 'Src MEP ID' and 'Increment By', 'Dest MEP ID' and 'Increment By', 'Local Tunnel ID' and 'Increment By', and 'Remote Tunnel ID' and 'Increment By'. In the 'Working LSP/PW' column, the 'Src MEP ID' is 10 and 'Dest MEP ID' is 20. In the 'Protecting LSP/PW' column, the 'Src MEP ID' is 100 and 'Dest MEP ID' is 200. All 'Increment By' fields are set to 1. The 'Local Tunnel ID' and 'Remote Tunnel ID' fields are all set to 1.

MEG Configuration	
Working LSP/PW	Protecting LSP/PW
MEG ID Prefix: Ixia-Wrk-0001	MEG ID Prefix: Ixia-Prt-0001
MEG ID Integer Step: 1	MEG ID Integer Step: 1

MEP Configuration	
Working LSP/PW	Protecting LSP/PW
Src MEP ID: 10 Increment By: 1	Src MEP ID: 100 Increment By: 1
Dest MEP ID: 20 Increment By: 1	Dest MEP ID: 200 Increment By: 1
Local Tunnel ID: 1 Increment By: 1	Local Tunnel ID: 1 Increment By: 1
Remote Tunnel ID: 1 Increment By: 1	Remote Tunnel ID: 1 Increment By: 1

- In the sixth page, keep the default values and enter some IP or MAC for traffic purpose.

The screenshot shows the 'MPLS-TP IP Traffic Endpoint Configuration' section of a wizard. It has a 'End Point Type' dropdown menu set to 'IPv4' and an 'IP Hosts Per LSP' field set to 1. Below this are two columns: 'Left Traffic Endpoints' and 'Right Traffic Endpoints'. Each column has an 'IP Start' field and a 'Step' field. The 'Left Traffic Endpoints' column has 'IP Start' set to 2.2.2.2/24 and 'Step' set to 1. The 'Right Traffic Endpoints' column has 'IP Start' set to 1.1.1.1/24 and 'Step' set to 1.

MPLS-TP IP Traffic Endpoint Configuration	
End Point Type: IPv4	IP Hosts Per LSP: 1
Left Traffic Endpoints	Right Traffic Endpoints
IP Start: 2.2.2.2/24 Step: 1	IP Start: 1.1.1.1/24 Step: 1

### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

8. In the last page of the wizard, give the config some name and click **Generate and Overwrite All Protocol Configurations**.

FailOverPerfTest

- ☐ Save Wizard Config, But Do Not Generate on Ports
- ☐ Generate and Append to Existing Configuration
- ☐ Generate and Overwrite Existing Configuration
- ☒ Generate and Overwrite All Protocol Configurations  
(WARNING : This will clear the interface configurations also)

9. We have completed the control plane configuration so far. You can either start the control plane now or start it after the data plane is configured. MPLS-TP labels are static so data plane traffic can be configured without running the control plane first. Next few steps will focus on the traffic wizard that is used to configure the data plane. Before starting the traffic wizard, first select the **Packet Loss Duration** check box under **Traffic** -> **Options**. By default, this option is off. It is important to have this option enabled because it delivers per flow switchover time in ms accuracy.

Test Configuration

Test Configuration

- 1. Port Manager
- 2. Protocols
  - Routing/Switching/Interfaces
  - Auth/Access Hosts/DCB
  - Traffic Groups
  - Options
- 3. Traffic
  - Options**
- 4. Statistic Setup
- 5. Capture
- 6. QuickTests

Options

Global Settings | Statistics Configuration

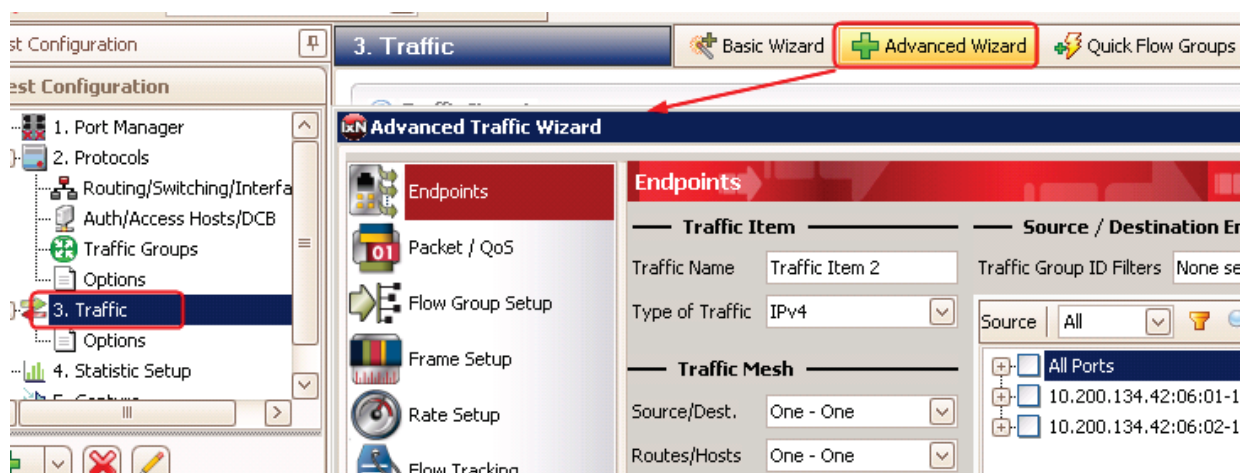
Available Sets of Statistics

C...	Statistics Set	Settings
<input type="checkbox"/>	Inter-arrival time/rate	
<input type="checkbox"/>	Sequence Checking	
<input type="checkbox"/>	CP/DP Convergence	
<input type="checkbox"/>	PRBS	
<input type="checkbox"/>	IPv4/TCP/UDP Checksum Err...	
<input checked="" type="checkbox"/>	Data integrity	
<input checked="" type="checkbox"/>	<b>Packet Loss Duration</b>	



### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

10. Start the traffic wizard.



11. In the first page of the Advanced Traffic Wizard, configure the following:

Traffic Name: type a string

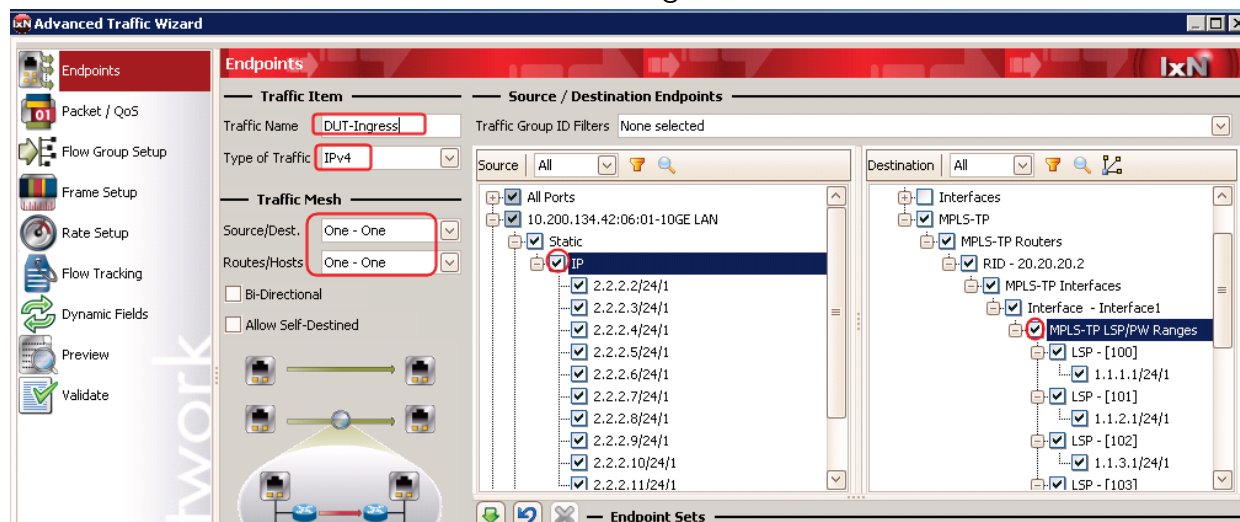
Type of Traffic: IPv4

Source/Dest Traffic Mesh: One-One

Routes/Hosts Traffic Mesh: One-One

Source End Points: all static IP

Destination End Points: all MPLS-TP LSP/PW Ranges



Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

12. Skip Packet/QoS and Flow Group Setup and enter appropriate frame size under Frame Setup.



### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

13. Enter some appropriate rate. Note that the rate will be evenly distributed to all flow groups by default.

**Advanced Traffic Wizard [Read Only]**

**Rate Setup**

☒ All Encapsulations ☐ Per Encapsulation

	Tx Port	Encapsulation	Transmission	Target Rate	Target
1	10.200.134.42:06:01-10GE LAN	Ethernet II,IPv4	Continuous	Packet rat...	Apply

All Encapsulations - Same settings will be applied to all (1) encapsulation(s)

**Traffic Item Transmission Mode**

☒ Interleaved  
☐ Sequential

The Interleaved Transmit mode will interleave the packets from each Flow Group when sending Traffic

**Flow Group Transmission Mode**

☒ Continuous  
☐ Fixed Packet Count  
☐ Fixed Iteration Count  
☐ Fixed Duration  
☐ Burst (Auto)  
☐ Burst (Custom)

How it will look on the wire: 1 2 3 1

**Rate**

☐ Line rate 20.00 %  
☒ Packet rate 10000.00 per second  
☐ Layer2 Bit Rate 1000.00 bps

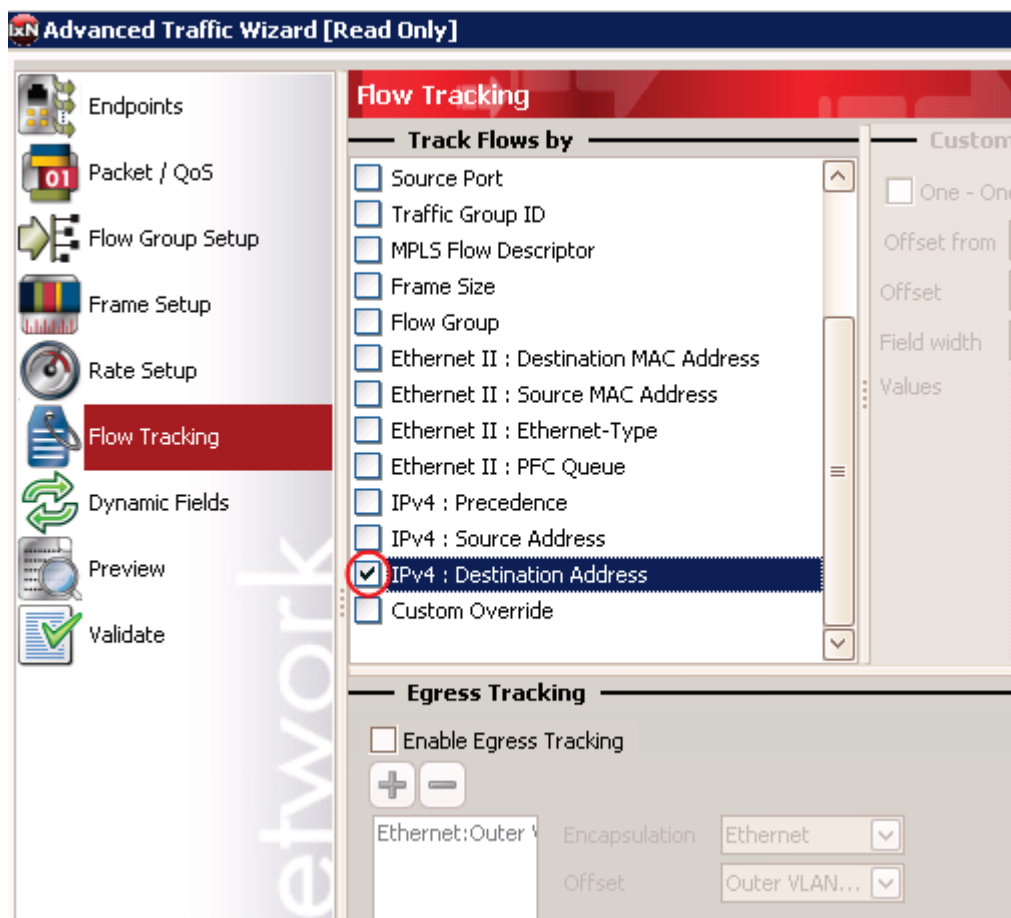
**Rate Distribution**

Ports:  
☒ Apply rate on all ports  
☐ Split rate evenly among ports

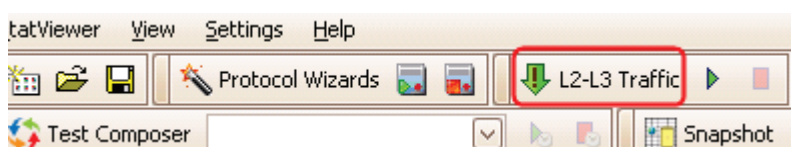
Flow Groups:  
☐ Apply port rate to all Flow Groups  
☒ Split port rate evenly among Flow Groups

### Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

14. For Flow Tracking, because the TX port will be native IP, tracking by either source IP or destination IP is good enough to deliver per-flow stats, including failover time.



15. Finish the traffic wizard and push the traffic definition to HW.



16. Start control plane (if you have not started it in previous steps) to ensure that all CCCV sessions are in the UP state.

MPLSTP Aggregated Statistics				
	Stat Name	CCCV Configured	CCCV Up	CCCV Down
1	10.200.134.42/Card06/Port02	20	20	0

## Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

17. Send data plane traffic and ensure that no packet drops occur before switchover.

Flow Statistics								
	Tx Port	Rx Port	v4 :Destination Address	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)
1	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.1.1	175,527	175,527	0	0.000	0.000
2	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.2.1	175,527	175,527	0	0.000	0.000
3	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.3.1	175,527	175,527	0	0.000	0.000
4	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.4.1	175,527	175,527	0	0.000	0.000
5	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.5.1	175,526	175,526	0	0.000	0.000
6	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.6.1	175,526	175,526	0	0.000	0.000
7	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.7.1	175,526	175,526	0	0.000	0.000
8	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.8.1	175,526	175,526	0	0.000	0.000
9	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.9.1	175,526	175,526	0	0.000	0.000
10	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.10.1	175,526	175,526	0	0.000	0.000

18. Inject errors from the emulated Egress PE to DUT. Select all 10 LSPs and force CCCV Pause on TX.

The screenshot shows the NCM interface with the 'Routing/Switching/Interfaces' configuration page. The 'Learned Info' section is expanded, showing a list of 10 LSPs (7-20) with their outgoing labels. The 'Trigger' button is highlighted. The 'MPLSTP Learned Info Trigger Settings' dialog is open, showing the 'Fault Management' tab. The 'CCCV Pause' checkbox is checked, and the 'Trigger Option' is set to 'Tx'. Other settings like 'Status Code', 'Transmit Interval (s)', 'PW Label TTL', 'Alarm Type', and 'Periodicity (msec)' are also visible.



## Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

19. Wait for a few seconds and go back to the statistics page to view the Packet Loss Duration on both the aggregated traffic item as well as the individual flow level.

The screenshot shows the 'Statistics' page in a network management interface. The left sidebar contains a tree view with categories like 'Views (Total: 10)', 'Custom Views', 'Defaults', 'Ports', 'Traffic', 'Protocols', and 'Configuration'. The main area displays a table of traffic statistics.

Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)	Tx Frame Rate	Rx Frame Rate	Rx Bytes	Tx Rate (Bps)	Rx Rate (Bps)
1 DUT-Ingress	7,155,264	7,155,264	0	0.000	0.000	10,000.000	10,000.000	457,936,896	640,000.000	640,000.000

Below the aggregated traffic table, there is a 'Flow Statistics' section with a table showing individual flows:

Tx Port	Rx Port	Destination Address	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)	Tx Frame Rate
1 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.1.1	715,527	715,527	0	0.000	0.000	
2 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.2.1	715,527	715,527	0	0.000	0.000	
3 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.3.1	715,527	715,527	0	0.000	0.000	
4 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.4.1	715,527	715,527	0	0.000	0.000	
5 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.5.1	715,526	715,526	0	0.000	0.000	
6 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.6.1	715,526	715,526	0	0.000	0.000	
7 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.7.1	715,526	715,526	0	0.000	0.000	
8 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.8.1	715,526	715,526	0	0.000	0.000	
9 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.9.1	715,526	715,526	0	0.000	0.000	
10 10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.10.1	715,526	715,526	0	0.000	0.000	

20. Increase the number of LSP/PW under test and repeat the preceding steps to get another set of data points. To increase the number of LSP/PW under test, you can either use the Protocol Wizard to enter the new number and overwrite the existing configuration or simply go to the GUI and make the changes. Ensure that you stop the protocol first and run it again after the change.

The screenshot shows the 'LSP/PW Ranges' configuration page. It has tabs for 'Routers', 'Interfaces', and 'LSP/PW Ranges'. Below the tabs, there is a text box: 'To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field'. Below this is a table with columns: Interface, Enable, Number of LSPs, Number of PWs per LSP, LSP Outgoing Label, LSP Incoming Label, and PW Out.

	Interface	Enable	Number of LSPs	Number of PWs per LSP	LSP Outgoing Label	LSP Incoming Label	PW Out
1	20.20.20.2/24 - 23.222.1 - 20.20.20.2 -	<input checked="" type="checkbox"/>			100	1,000	
2		<input checked="" type="checkbox"/>	1000		200	2,000	

21. Change the APS protection mode to 1+1 bidirectional and perform the same type of steps to collect performance data points for different protection modes. This can be done by simply changing the **Type of Protection Switching** value under **APS**. Stop and start the protocol again, if needed.

The screenshot shows the 'Routing/Switching/Interfaces' configuration page. It has tabs for 'Diagram', 'Ports', 'Routers', 'Interfaces', and 'LSP/PW Ranges'. Below the tabs, there is a text box: 'To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field'. Below this is a table with columns: Interface, Enable, APS Type, Type of Protection Switching, Revertive, and Wait To Revert Time (ms).

	Interface	Enable	APS Type	Type of Protection Switching	Revertive	Wait To Revert Time (ms)
1	20.20.20.2/24 - 23.221.1 - 20.20.20.2 -	<input checked="" type="checkbox"/>	IETF			
2		<input checked="" type="checkbox"/>	IETF	1+1 Bidirectional	<input checked="" type="checkbox"/>	300

A dropdown menu is open for the 'Type of Protection Switching' column, showing options: 1:1 Unidirectional, 1+1 Unidirectional, 1:1 Bidirectional, and 1+1 Bidirectional. The '1+1 Bidirectional' option is selected and highlighted.

## Test Scenario 3: Verify linear APS switchover time with numerous LSP/PWs and various protection modes

### Test Variables

The following are possible test variables:

- Number of test ports
- LSPs or PWs or a mix of both
- Number of static LSPs and PWs
- IETF or Y.1731 APS
- Protection Mode (1:1 or 1+1, Uni- or Bi- directional)
- LoC or other Alarms to cause auto-trigger on DUT
- Traffic rate and frame size

## Test Scenario 4: Verify manual APS command functionality

### Overview

APS is the central piece of a successful implementation of MPLS-TP. While it is well understood in TDM-based transport technologies, it is fresh and new to packet-based transport, such as MPLS-TP. The critical part is that the switchover triggered by manual commands or by some kind of active alarms, from working path to protecting path, should be sub-50 ms in service disruption. Manual switch is intended for administrative purposes. It is critical to ensure that DUT, as egress PE, responds correctly to all the administrative commands. The following manual commands are available today: Clear, Exercise, Forced Switch, Freeze, Lockout, Manual Switch to Protect, and Manual Switch to Working. A brief explanation of each command is as follows:

- Clear: Clears previously issued Freeze, Lockout, Forced Switch, Exercise, or Manual switch command.
- Exercise: Exercises the APS protocol but not the traffic.
- Forced Switch: Forces far end to select traffic from protecting path instead of working path.
- Freeze: Freezes the state of the protection group. Until the freeze is cleared, additional manual commands are rejected.
- Lockout: Prevents far end from selecting traffic over protecting path. Further local end switch commands, either manual or auto triggered based on Signal Failure (SF) or Signal Degradation (SD), will be rejected. This effectively disables the protection mechanism at the local end. In bidirectional switching, remote entity APS operation continues as usual to prevent failures.
- Manual switch to Protect or Manual Switch to Working: In the absence of or a failure of PSC, forces far end to select traffic from protecting path or working path respectively.

### Objective

To test DUT's ability, as egress router, to accept manual APS commands, and then to respond correctly to the commands. All supported manual commands should be tested.



## Setup

A minimum of two test ports are required to perform this test. The first test port will be used to emulate Ingress router and issue manual switch commands, and in the meantime as traffic generator. The second port will be used as traffic sink to analyze and detect where the traffic is coming from: protecting path or working path. DUT must behave according to the standard when interpreting those manual switching commands.

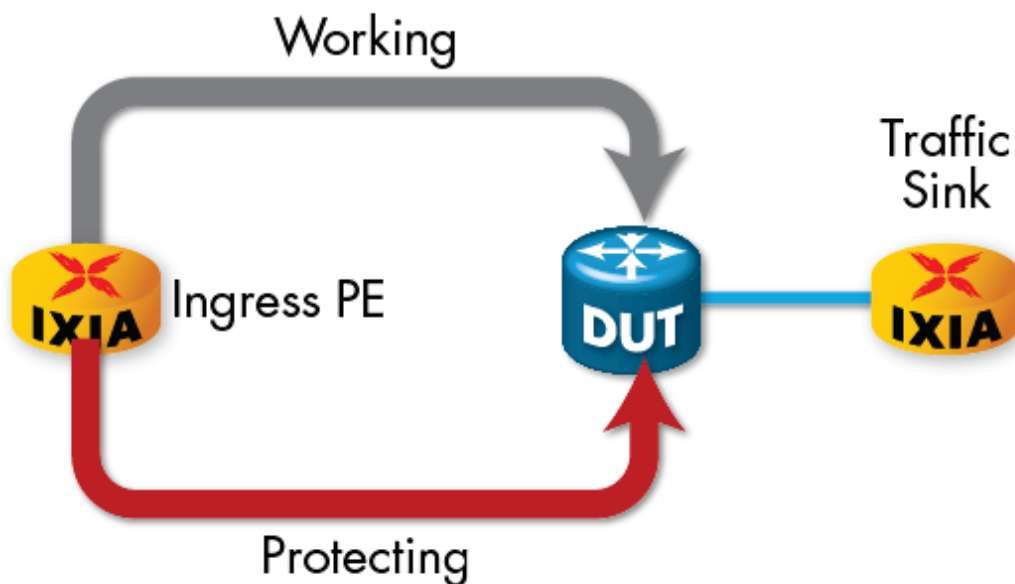


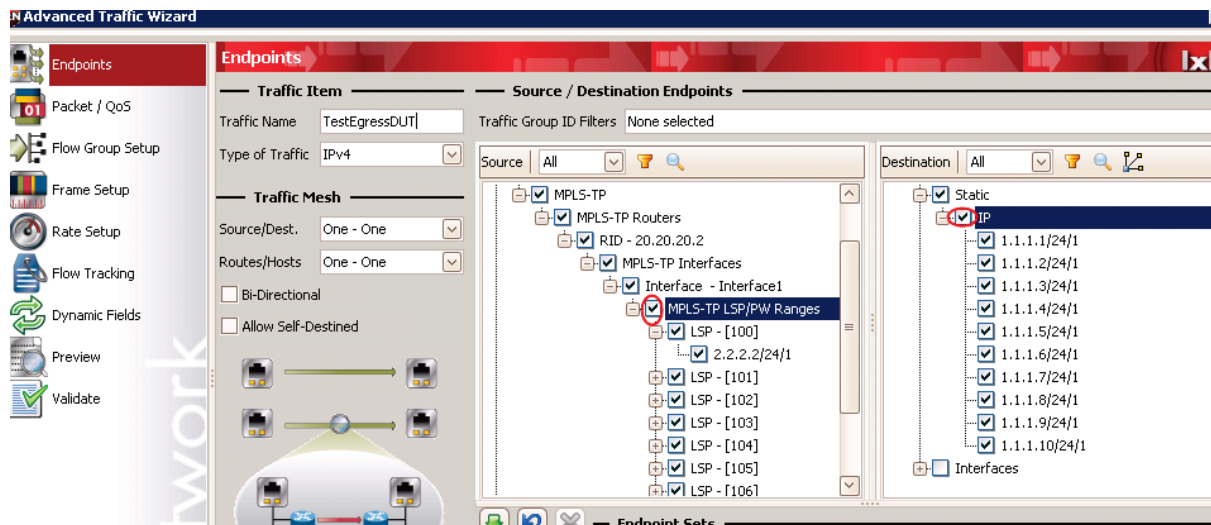
Figure 7 Test Setup for Testing Manual APS Commands

## Step-by-Step Procedures by using IxNetwork

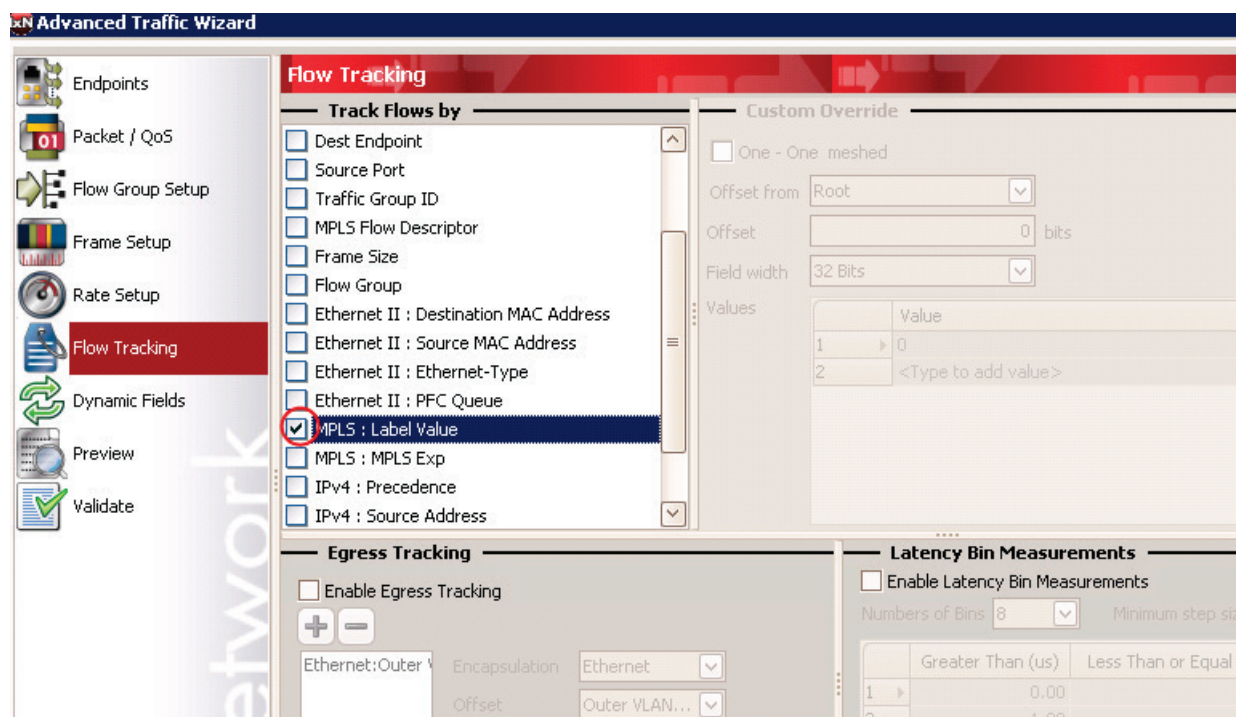
1. Use the MPLS-TP Protocol Wizard to configure the setup with DUT=Egress mode. Refer to the previous test on how to operate the protocol wizard. Detailed steps are skipped here for brevity.
2. Select the APS mode to be 1+1 bidirectional. This is to facilitate traffic analysis at the traffic sink port.

## Test Scenario 4: Verify manual APS command functionality

- Start the Advanced traffic wizard. Select all MPLS-TP LSP ranges on the first port and all Static IP end points.



- Skip all other pages except Flow Tracking. Select **MPLS : Label Value** as the tracking option.



## Test Scenario 4: Verify manual APS command functionality

- Finish the traffic wizard. Start protocol and ensure that all CCCV sessions are in the UP state. Next, start traffic. Ensure that there is no traffic loss on the working path while 100 percent loss on the protecting path, before issuing manual commands to test the DUT's ability to respond to individual commands.

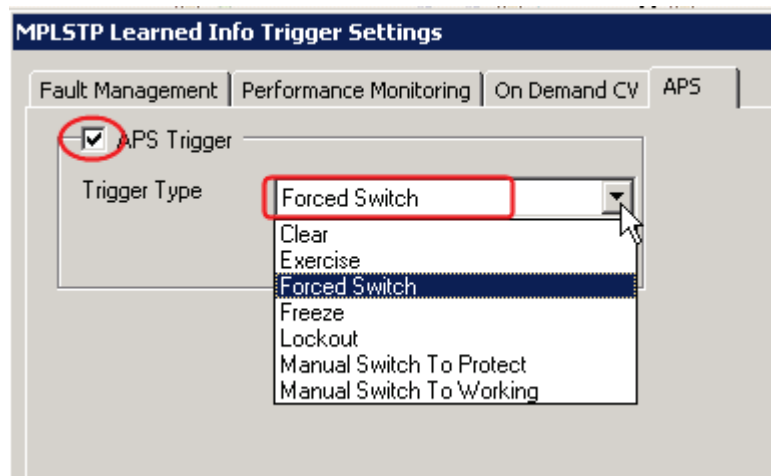
Flow Statistics

Home Formulas

Autoscroll AutoUpdate Enabled Favorites Select a Profile ... Customize

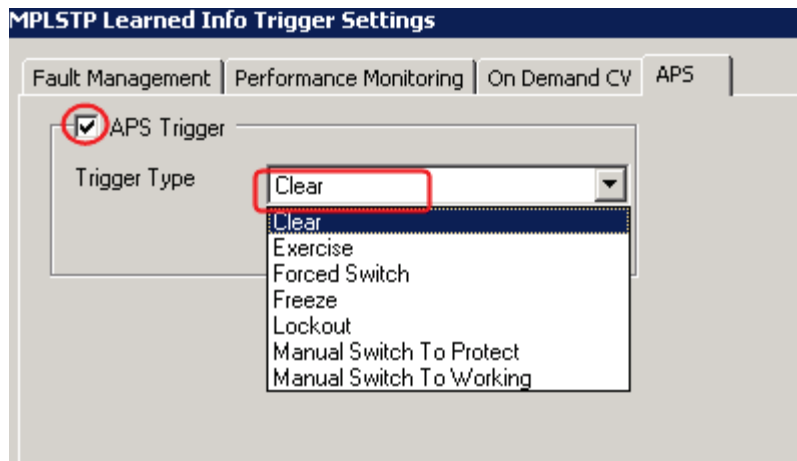
	Tx Port	Rx Port	Traffic Item	MPLS:Label Value	Tx Frames	Rx Expected Frames	Rx Frames	Frames Delta
1	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	100	26,753	26,753	26,753	0
2	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	101	26,752	26,752	26,752	0
3	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	102	26,752	26,752	26,752	0
4	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	103	26,752	26,752	26,752	0
5	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	104	26,752	26,752	26,752	0
6	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	105	26,752	26,752	26,752	0
7	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	106	26,752	26,752	26,752	0
8	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	107	26,752	26,752	26,752	0
9	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	108	26,752	26,752	26,752	0
10	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	109	26,752	26,752	26,752	0
11	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	200	26,752	26,752	0	26,752
12	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	201	26,752	26,752	0	26,752
13	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	202	26,752	26,752	0	26,752
14	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	203	26,752	26,752	0	26,752
15	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	204	26,752	26,752	0	26,752
16	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	205	26,752	26,752	0	26,752
17	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	206	26,752	26,752	0	26,752
18	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	207	26,752	26,752	0	26,752
19	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	208	26,752	26,752	0	26,752
20	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	209	26,752	26,752	0	26,752

- To test a Forced Switch, select the LSPs you want to perform a Forced Switch on, and then select to issue a Forced Switch command.

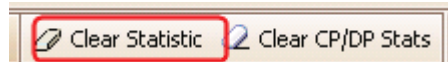


To verify if the DUT is performing the right action, go to traffic flow stats. Those LSPs that have been forced switch will have non-zero Loss over working path while RX frames on the corresponding protecting path will show RX frames with rate matching the sending rate.

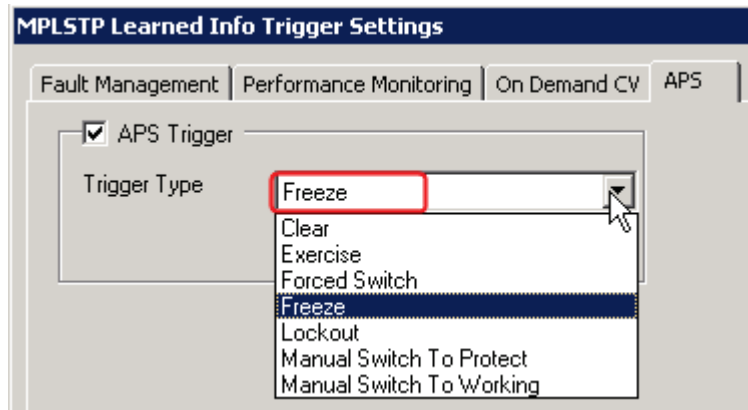
7. To verify Clear, click **Clear** in the **Trigger Type** list.



To verify if DUT performs the Clear action, go to flow stats and click '**Clear Statistic**' first, and then observe if traffic is flowing on all working LSP again (no loss).



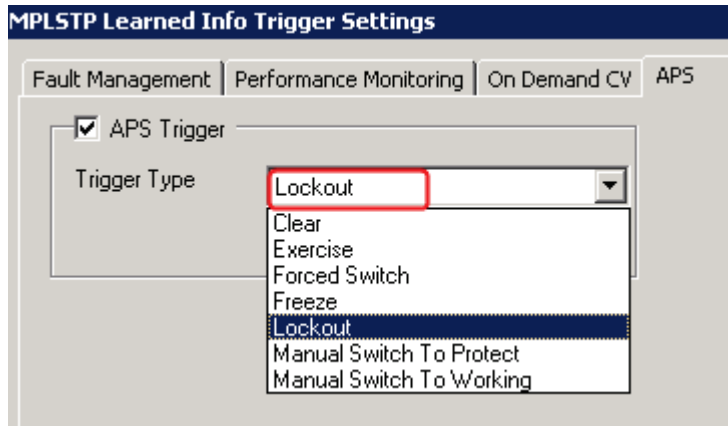
8. To verify Freeze, ensure that the protection state is in clear state. Next, issue a **Freeze** command from tester.



To see if the DUT is in 'Freeze' state, perform another 'Forced Switch' command, and then go to the flow stats page to observe if traffic is flowing over the protecting path or working path. The expected behavior is that traffic should stay on the working path because the DUT is in 'Freeze' state and further switching commands are ignored.

## Test Scenario 4: Verify manual APS command functionality

9. To test the Lockout operation, ensure that DUT is in clear state. This can be done by simply issuing a 'Clear' command from tester. Next, issue a Lockout command.



To verify whether or not the DUT is in 'Lockout' state, first try to issue a 'Forced Switch' from headend (tester) and observe from the flow stats page whether or not traffic is continuing to flow on working path. This is to say whether or not the 'Forced Switch' command is being rejected (as it should). Next, cause DUT to cease sending of CC tx towards the headend (tester). This will trigger the tester (ingress PE) to perform auto trigger switchover based on LoC alarm. Verify from the flow statistics page and observe whether or not the traffic still flows over working path. The correct behavior is that DUT should also reject any auto triggered switchover signal.

10. Manual Switch to Protect and Manual Switch to Working work like the name indicates and will leave for the user for exercise with no further details.

### Test Variables

The following are possible test variables:

- LSPs or PWs or a mix of both
- Number of static LSPs and PWs
- IETF or Y.1731 APS
- Protection Mode (1:1 or 1+1, Uni- or Bi- directional)

## Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

### Overview

After an MPLS-TP device passed the basic interoperability test, the G-ACh/GAL encapsulated control messages for CC, CV (LSP ping and traceroute), Alarms (AIS, LDI, LCK), LM, DM, and PSC (1:1, 1+1, Unidirectional, Bidirectional), and also have acceptable APS performance numbers (for example, < 50 ms switchover time), the next immediate pending question is how does the device scale?

One of the challenges in the implementation of MPLS-TP is the number of LSP or PWs that can run Y.1731 CCM or BFD CC at the fastest pace. The interval of 3.33 ms is critical for overall switchover performance to meet or exceed 50 ms total service disruption time.

### Objective

This test is to find out the maximum number of MPLS-TP LSP or PW that the DUT can establish and sustain when either the Y.1731 CCM or BFD CC is running at 3.33 ms interval.

### Setup

One or more Ixia test ports can be used to carry out this performance test.

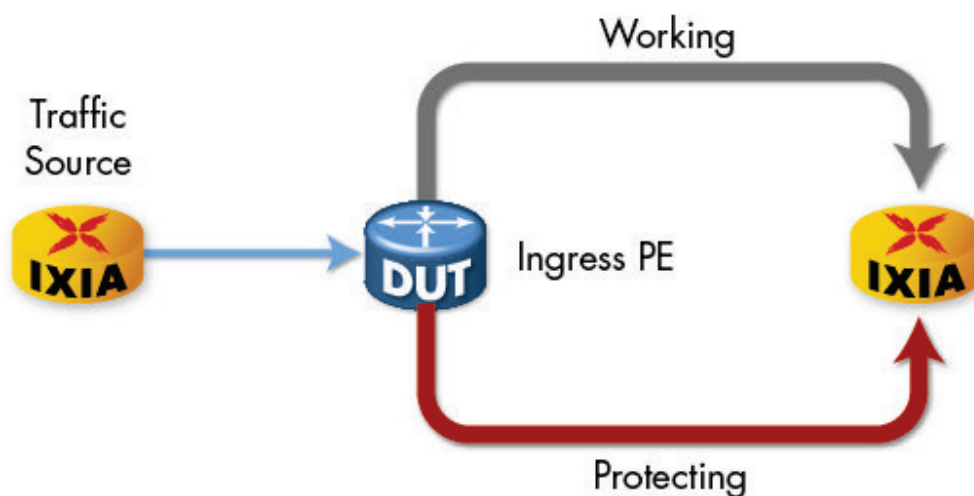


Figure 8 Test Setup for Testing MPLS-TP Scalability at 3.33 ms Interval

## Step-by-Step Procedures by using IxNetwork

1. Use the protocol wizard to configure the setup. Refer to Test Scenario 3 for detailed steps on how to configure each wizard page.
2. Click DUT = Ingress. Start with a comfortable number of LSP/PW, for example, 100. Ensure that the CC-CV interval is set as 3.33 ms.

The screenshot displays three configuration pages from the IxNetwork protocol wizard. The first page, 'Mode', shows 'DUT = Ingress' selected with a red circle, and 'Protection Type' set to '1:1 Bidirectional' in a dropdown menu, also highlighted with a red box. The second page, 'Select Port(s) for Wizard Configuration', contains a table with two rows. Row 1 has 'Tunnel Head/Tail Port' checked and 'Traffic Src/Sink Port' checked. Row 2 has 'Tunnel Head/Tail Port' checked and 'Traffic Src/Sink Port' unchecked. The third page, 'Static LSPs', shows 'Static MPLS-TP LSP' selected under 'MPLS-TP Tunnel Type', and 'Number of LSPs Per Router' set to '100' in a text box, highlighted with a red box. The fourth page, 'Protocol Behavior', shows 'Global Identifier Type' set to 'ICC', 'PSC Type' set to 'IETF', 'CC-CV Type' set to 'BFD CC', and 'On-demand CV Type' set to 'IETF'. The 'CC-CV Interval' is set to '3.33' ms, with a dropdown menu open showing a list of values including 10, 100, 1000, 10000, 3.33 (highlighted with a red box), 60000, and 600000. The 'Alarm Type' is set to 'IETF'.

Mode

☒ DUT = Ingress  
☐ DUT = Egress

Protection Type  
1:1 Bidirectional

Select Port(s) for Wizard Configuration

	Tunnel Head/Tail Port	Traffic Src/Sink Port	Port Description
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10.200.134.42:06:01-10GE LAN - LAN/W
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.200.134.42:06:02-10GE LAN - LAN/W

Static LSPs

MPLS-TP Tunnel Type  
☒ Static MPLS-TP LSP  
☐ Static L2VPN PW  
☐ Both

Static LSP Properties  
Number of LSPs Per Router 100

Protocol Behavior

Global Identifier Type  
☐ IETF  
☒ ICC

PSC Type  
☒ IETF  
☐ Y.1731

CC-CV Type  
☒ BFD CC  
☐ Y.1731

On-demand CV Type  
☒ IETF  
☐ Y.1731

DM Type

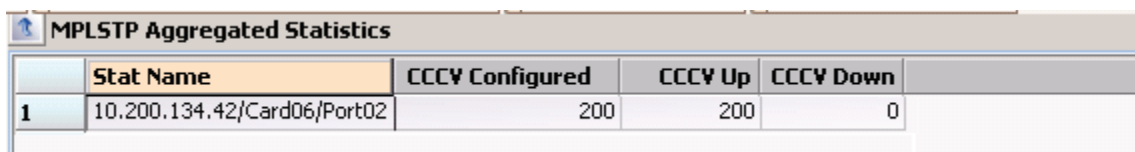
CC-CV Interval 3.33 ms

Alarm Type  
☒ IETF  
☐ Y.1731



Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

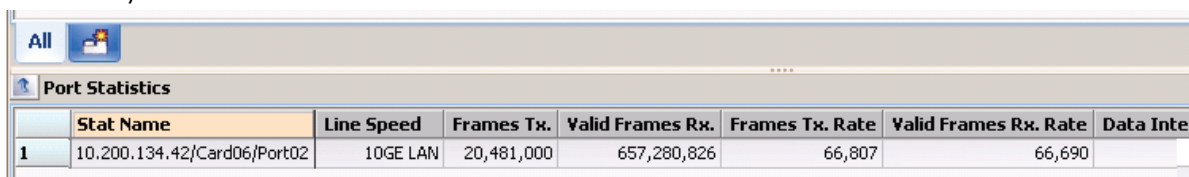
3. Start the control plane CCCV sessions. Ensure that all 200 sessions (100 working and 100 protecting) are up.



The screenshot shows a table titled "MPLSTP Aggregated Statistics". It has five columns: "Stat Name", "CCCV Configured", "CCCV Up", "CCCV Down", and an unlabeled column. The first row shows the configuration for 10.200.134.42/Card06/Port02 with 200 configured sessions, 200 up sessions, and 0 down sessions.

	Stat Name	CCCV Configured	CCCV Up	CCCV Down	
1	10.200.134.42/Card06/Port02	200	200	0	

One quick way to check whether or not each session is running at 3.33 ms is by opening the Port Statistics. The next diagram shows about 66,000 packets per second as both TX and RX rate. Because there are 200 sessions, each is sending CC message at 3.33 ms (3 packets every 10 ms so 1 second is equivalent to 300 messages per session). So a total of 200 sessions will generate about 60,000 packets per second. Remember that there is PSC control packet that is running on the Protecting LSPs only. The frequency for PSC packet is about 60 packets for every session and the total 100 sessions will contribute about 6000 packets per second. So the port stats confirmed that each working and protection LSPs is indeed running at continuity check at 3.33 ms.



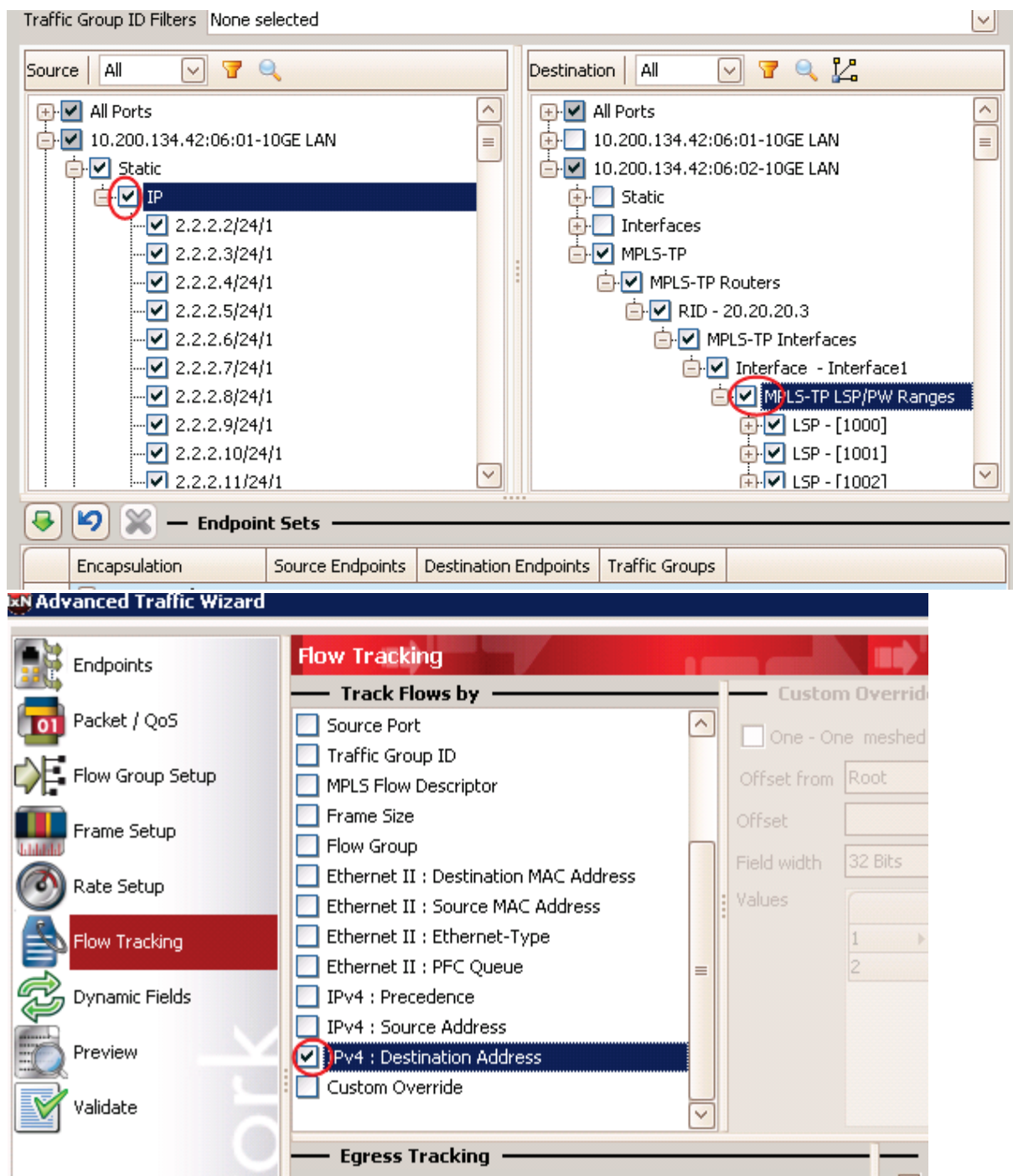
The screenshot shows a table titled "Port Statistics". It has eight columns: "Stat Name", "Line Speed", "Frames Tx.", "Valid Frames Rx.", "Frames Tx. Rate", "Valid Frames Rx. Rate", and "Data Inte.". The first row shows statistics for 10.200.134.42/Card06/Port02, including a line speed of 10GE LAN, 20,481,000 frames transmitted, 657,280,826 valid frames received, and rates of 66,807 and 66,690 respectively.

	Stat Name	Line Speed	Frames Tx.	Valid Frames Rx.	Frames Tx. Rate	Valid Frames Rx. Rate	Data Inte.
1	10.200.134.42/Card06/Port02	10GE LAN	20,481,000	657,280,826	66,807	66,690	



Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

- After the control plane is up and works as expected, use the traffic wizard to configure traffic. Select the static IP end point defined at the Traffic Source port and select all MPLS-TP LSP ranges in a one-one mapping. Select the Dest IP address as the tracking option. This will deliver per LSP performance when failover takes place.



## Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

5. Ensure that no traffic loss before failover conditions are injected. Navigate to the Learned Info section and select all Working session to inject the 'CCCV TX Pause' error. This should cause DUT to switch traffic on all working LSPs to Protecting LSPs.

The screenshot displays the Network Configuration Manager (NCM) interface. The left pane shows the 'Configuration' tree with 'Routing/Switching/Interfaces' selected. The 'Learned Info' section is highlighted. The main pane shows the 'MPLSTP Learned Info Trigger Settings' configuration. The 'Fault Management' tab is active, and the 'CCCV Pause' trigger option is selected. The 'Learned Info' table lists various LSPs and PWs, with rows 101 through 108 highlighted in red.

	Outgoing Label (Outer-Inner)	Incoming Label (Outer-Inner)	
95	2094-13	294-13	L
96	2095-13	295-13	L
97	2096-13	296-13	L
98	2097-13	297-13	L
99	2098-13	298-13	L
100	2099-13	299-13	L
101	1000-13	100-13	L
102	1001-13	101-13	L
103	1002-13	102-13	L
104	1003-13	103-13	L
105	1004-13	104-13	L
106	1005-13	105-13	L
107	1006-13	106-13	L
108	1007-13	107-13	L

## Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

- Observe the Packet Loss Duration due to switchover for all 100 LSPs. Ensure that they are within an acceptable range before increasing the number of LSPs under test.

Flow Statistics

ome Formulas

Autoscroll AutoUpdate Enabled Favorites Select a Profile ... Customize Traffic...

Tx Port	Rx Port	Destination Address	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)	T
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.1.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.2.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.3.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.4.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.5.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.6.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.7.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.8.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.9.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.10.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.11.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.12.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.13.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.14.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.15.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.16.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.17.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.18.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.19.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.20.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.21.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.22.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.23.1	7,555	7,555	0	0.000	0.000	
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.24.1	7,555	7,555	0	0.000	0.000	

Page 1 of 2 (Total rows: 100)

- To increase the number of LSPs, navigate to the **LSP/PW Ranges -> Static Label Range** tab. Change the Number of LSPs to a higher number and repeat the test.

Routing/Switching/Interfaces

Start Stop

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Interface	Enable	Number of LSPs	Number of PWs per LSP	LSP Outgoing Label	LSP Incoming Label	PW Outgoing Label
1	20.20.20.2/24 - 23.222 - 1 - 20.20.20.3 -	<input checked="" type="checkbox"/>			1,000	100	
2		<input checked="" type="checkbox"/>	120		2,000	200	

General **Static Label Range** ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

## Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

- The same test procedure is applicable to PW test. Just change the Type of Range to PW and enter appropriate LSP as well as PW label values.

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Interface	Enable	Description	Type of Range	Range Role	Protect LSP/PW Range
1	20.20.20.2/24 - 23.222.1 - 20.20.20.3 -	<input checked="" type="checkbox"/>	IXIA.0002.0001.0001.0001	PW	Working	IXIA.0002.0001.0001.0002
2		<input checked="" type="checkbox"/>	IXIA.0002.0001.0001.0002	PW	Protect	

**General** Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

---

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Enable	Number of LSPs	Number of PWs per LSP	LSP Outgoing Label	LSP Incoming Label	PW Outgoing Label	PW Incoming Label	LSP Out
1	<input checked="" type="checkbox"/>			1,000	100	5,555	3,333	
2	<input checked="" type="checkbox"/>	100	1	2,000	200	6,666	4,444	

**General** **Static Label Range** ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

## Test Variables

The following are possible test variables:

- Number of test ports
- Number of static LSPs and PWs
- LSP or PW or a mix of both
- Protection mode (1:1, 1+1, Unidirectional, Bidirectional)



## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs

### Overview

MPLS-TP alone will not fulfill the end-to-end service requirement in a real network with many MPLS services already deployed. Most likely, MPLS-TP will need to work together with MPLS PW to provide end-to-end services. In addition to facing all the implementation and testing challenges that we have talked about so far, the DUT will need special ability to bridge the two disparate segments. This will need to happen not only on data plane but also on the control plane including end-to-end OAM operation. Additionally, PW status will need to be translated between the MPLS-TP segment and MPLS segment.

### Objective

This test is designed to test DUT ability to bridge multiple segments of an end-to-end PW with portions as MPLS-TP PW and others as regular MPLS PW. Both control plane and data plane need to be verified for a successful end-to-end MPLS-TP PW.

### Setup

Two or more Ixia test ports are required to carry out this functional test. One port is used to emulate ingress MPLS-TP node with both working and protecting tunnels configured, and the other port is used to emulate regular MPLS L2VPN PWs. Both control plane and data plane are verified to ensure true end-to-end service.

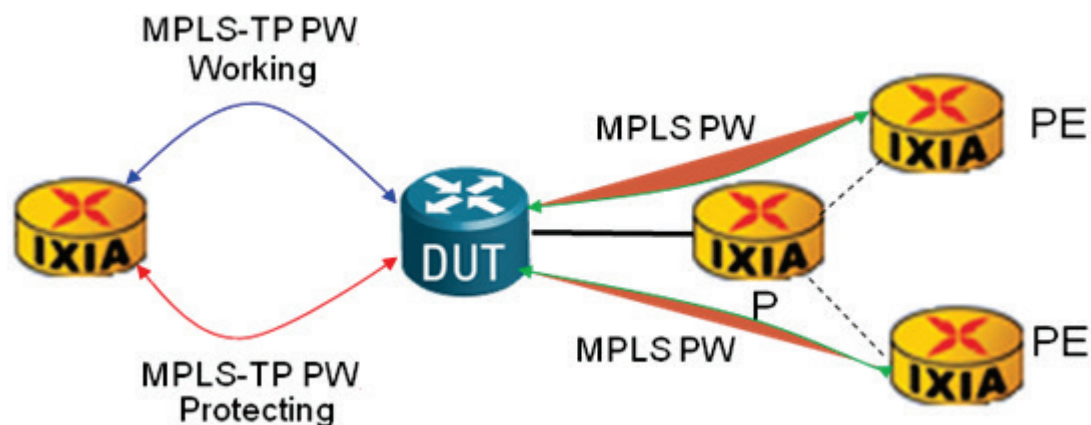


Figure 9 Test Setup for Testing IP/MPLS and MPLS-TP Coexistence

## Step-by-Step Procedures by using IxNetwork

1. Use either the manual method (see steps in Test Scenario 1) or the protocol wizard (see steps in Test Scenario 3) to configure the MPLS-TP port with a few PWs. Choose IETF as CCCV mode. Set the PW labels incoming and outgoing that match the DUT. In addition, select the CCCV interval to be 1000 ms. Start with 10 PWs.

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Interface	Enable	Description	Type of Range	Range Role	Protect LSP/PW Range	CCCV Type
1	20.20.20.2/24 - 23.221 - 1 - 20.20.20.2 -	<input checked="" type="checkbox"/>	IXIA.0001.0003.0001.0001	PW	Working	IXIA.0001.0003.0001.0002	BFD CC
2		<input checked="" type="checkbox"/>	IXIA.0001.0003.0001.0002	PW	Protect		BFD CC

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Enable	Number of LSPs	Number of PWs per LSP	LSP Outgoing Label	LSP Incoming Label	PW Outgoing Label	PW Incoming Label	LSP Outgoing
1	<input checked="" type="checkbox"/>			100	1,000	3,333	5,555	
2	<input checked="" type="checkbox"/>	10	1	200	2,000	4,444	6,666	

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Interface	Enable	CCCV Type	CCCV Interval (ms)	CCCV Traffic Class	Support Slow Start
1	20.20.20.2/24 - 23.221 - 1 - 20.20.20.2 -	<input checked="" type="checkbox"/>	BFD CC	1000	7	<input type="checkbox"/>
2		<input checked="" type="checkbox"/>	BFD CC	1000	7	<input type="checkbox"/>

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply Static MAC Range Static IP Range All

## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs

2. Use the L2VPN/VPLS wizard to configure the MPLS P/PE emulation port. Select 'LDP Extended Martini' as the L2VPN Signaling Protocol. Emulate 1 P and 2 PE routers each with 5 Ethernet PWs (EoMPLS VC).

The screenshot displays the L2VPN/VPLS wizard configuration interface, divided into three main sections: Enable P Routers, PE Router(s), and L2 Interfaces.

**Enable P Routers:**

- ☒ Enable P Routers
- Number of P Routers: 1
- Starting Subnet Between P and PE: 11.1.1.0/24
- IGP Protocol: OSPF (Options button)
- MPLS Protocol: LDP (Options button)
- L2 VPN Signaling Protocol: LDP Extended-Martini (highlighted with a red box)
- P Router IP Address: 20.20.20.2/24
- DUT IP Address: 20.20.20.1

**PE Router(s):**

- Number of PE Routers Connected to the P Router: 2 (circled in red)
- AS Number: 100
- Emulated PE Loopback Address: 2.2.2.2/32 (highlighted with a red box)
- Increment Per Router: 0.0.0.1
- Increment Per Port: 0.1.0.0
- ☐ Continuous Increment Across Ports
- DUT Loopback IP Address: 1.1.1.1/32
- Increment Per Router: 0.0.0.0
- Increment Per Port: (empty field)

**L2 Interfaces:**

- VPNs Traffic ID Name Prefix: L2VPN - 1 (Auto Prefix checkbox is checked)
- VC Pack Type: All VCs in one VC Range
- VC Interface Type: Ethernet (highlighted with a red box)
- Enable VPLS: ☐
- Note: To enable "Enable VPLS", select Ethernet or VLAN as Interface Type
- Number of VC/VPN IDs Per PE: 5 (circled in red)
- First VC/VPN ID: 10,000 (highlighted with a red box)
- Increment VC/VPN ID By: 1
- MTU: 1,500



## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs

- Start control plane for both test ports. Ensure that the MPLS-TP port has 20 CCCV sessions UP, and the MPLS port has 1 OSPF full session, 1 basic LDP session, and 2 t-LDP sessions up. The EoMPLS VC status is also UP.
- Inject MPLS-TP PW status from the MPLS-TP port and capture and analyze the response on the MPLS side.

**MPLSTP Learned Info Trigger Settings**

Fault Management | Performance Monitoring | On Demand CV | APS

☐ CCCV Pause  
Trigger Option: Tx

☒ PW Status Fault  
Status Code: 00 00 00 01  
Transmit Interval (s): 30  
PW Label TTL: 1

☐ CCCV Resume  
Trigger Option: Tx

☐ PW Status Clear  
Transmit Interval (s): 30  
PW Label TTL: 1

☐ Alarm  
Alarm Type: IETF  
Trigger: Start  
Periodicity (msec): 5,000  
☒ AIS ☒ Set LDI ☐ LCK

- Inject L2VPN PW Status code from the MPLS port and capture and analyze the response from the MPLS-TP port.

Routers | Interf... | Target... | Adv F... | Req F... | Filter... | L2 Int... | **L2 VC...** | MAC/... | Traffic... | L2 VC... | Multic... | Multic... | Multic... | Multic... | Multic...

To change number of VC Ranges, select 'L2 Interfaces' tab, and enter number in 'Number of VC Ranges' field

	Enable	Enable PW Status	Send PW Status Notification	PW Status Code	PW Status Code (in Hex)	Down Start (in sec)	Down Interval (in sec)	Up Interval (in sec)	Repeat Count
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PW not forwarding	0x1	30	60	30	1
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PW not forwarding	0x1	30	60	30	1

VC Ranges | Generalized Id FEC (0x81) VPLS | **PW Status** | ATM | CEM | IP | TDM | All

- If VCCV-BFD is supported on the MPLS PW, we also recommended you to see if VCCV-BFD on the MPLS side will interop with BFD CC session on the MPLS-TP side.

## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs

7. To generate traffic and verify end-to-end traffic delivery:

a. Define static MAC hosts behind MPLS-TP PW ranges.

Routers Interfaces **LSP/PW Ranges**

To change number of LSP/PW Range, select 'Interfaces' tab, and enter number in 'Number of LSP/PW Ranges' field

	Interface	Enable	MAC per PW	Repeat MAC	MAC Address	Enable VLAN	VLAN Count	VLAN ID (Outer,...,Inr
1	20.20.20.2/24 - 23:221 - 1 - 20.20.20.2 -	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	00 00 00 00 11 22	<input type="checkbox"/>		
2		<input checked="" type="checkbox"/>						

General Static Label Range ICC MEP/MEG IDs IP MEP/MEG IDs CCCV APS Triggered Reply **Static MAC Range** Static IP Range All

b. Start the traffic wizard and select Ethernet/VALN as Type of Traffic. Pick up the static MAC address from MPLS-TP port and the MAC address behind each L2VPN PW VC. Enable tracking on MPLS Flow Descriptor. Turn on the Dynamic Label Change optioin.

**Endpoints**

Traffic Item Traffic Item 1

Traffic Group ID Filters None selected

Type of Traffic **Ethernet/VLAN**

**Traffic Mesh**

Source/Dest. One - One

Routes/Hosts One - One

☐ Bi-Directional

☐ Allow Self-Destined

Source All

Destination All

Source Endpoints:

- All Ports
- 10.200.134.42:06:01-10GE LAN
- MPLS-TP
- MPLS-TP Routers
- RID - 20.20.20.2
- MPLS-TP Interfaces
- Interface - Interface1
- MPLS-TP LSP/PW Ranges**
- PW - [100:3333]
- PW - [101:3333]
- PW - [102:3333]
- PW - [103:3333]
- PW - [104:3333]
- PW - [105:3333]

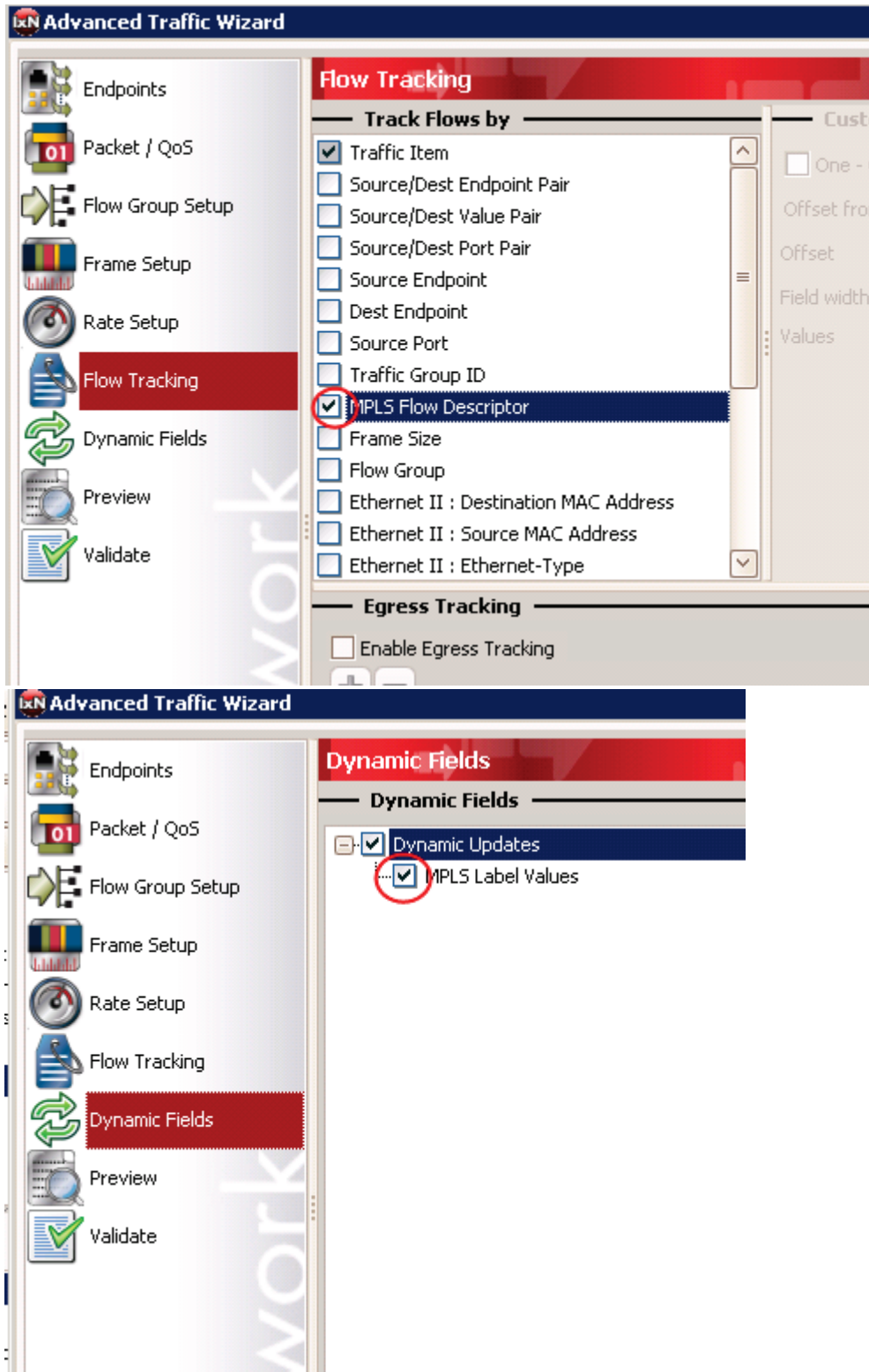
Destination Endpoints:

- All Ports
- 10.200.134.42:06:01-10GE LAN
- 10.200.134.42:06:02-10GE LAN
- LDP**
- RID - 2.2.2.2
- L2 VC FEC'S
- LDP L2 Interfaces
- LDP L2 Interface - 1
- L2 VC Range - 1.1.1.1/3...
- VCID: 10 Cnt: 50 Ma...
- RID - 2.2.2.3
- L2 VC FEC'S
- LDP L2 Interfaces
- LDP L2 Interface - 1

Endpoint Sets

Encapsulation	Source Endpoints	Destination Endpoints	Traffic Groups
*	Name: EndpointSet-1		

## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs



## Test Scenario 6: Verify coexistence of MPLS-TP PWs with MPLS PWs

- Both the aggregated Traffic Item stats as well as the per-LSP stats will give you a clear indication if the traffic has been delivered end-to-end. Optionally, test the MPLS-TP APS (see previous test scenarios for ideas) to see if it has any impact on MPLS side.

**Traffic Item Statistics**

Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)	Tx Frame Rate	Rx Frame Rate	Rx Bytes
1 Traffic Item 1	834,763	834,763	0	0.000	0.000	10,000.000	10,000.000	73,459,144

**Flow Statistics**

	Tx Port	Rx Port	MPLS Flow Descriptor	MPLS Current Label Value (Outer, Inner)	Tx Fr
1	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 100 ) -Protecting ( 4444 - 200 )	100, 3333	
2	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 101 ) -Protecting ( 4444 - 201 )	101, 3333	
3	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 102 ) -Protecting ( 4444 - 202 )	102, 3333	
4	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 103 ) -Protecting ( 4444 - 203 )	103, 3333	
5	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 104 ) -Protecting ( 4444 - 204 )	104, 3333	
6	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 105 ) -Protecting ( 4444 - 205 )	105, 3333	
7	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 106 ) -Protecting ( 4444 - 206 )	106, 3333	
8	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 107 ) -Protecting ( 4444 - 207 )	107, 3333	
9	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 108 ) -Protecting ( 4444 - 208 )	108, 3333	
10	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	ing ( 3333 - 109 ) -Protecting ( 4444 - 209 )	109, 3333	

## Test Variables

The following are possible test variables:

- Number of test ports
- Number of static MPLS-TP PWs and MPLS PWs
- IETF APS
- BFD TX/RX Interval
- Other PW status related alarms
- Traffic rate and frame size



## Contact Ixia

**Corporate Headquarters**  
Ixia Worldwide Headquarters  
26601 W. Agoura Rd.  
Calabasas, CA 91302  
USA  
+1 877 FOR IXIA (877 367 4942)  
+1 818 871 1800 (International)  
(FAX) +1 818 871 1805  
[sales@ixiacom.com](mailto:sales@ixiacom.com)

**Web site:** [www.ixiacom.com](http://www.ixiacom.com)  
**General:** [info@ixiacom.com](mailto:info@ixiacom.com)  
**Investor Relations:** [ir@ixiacom.com](mailto:ir@ixiacom.com)  
**Training:** [training@ixiacom.com](mailto:training@ixiacom.com)  
**Support:** [support@ixiacom.com](mailto:support@ixiacom.com)  
+1 877 367 4942  
+1 818 871 1800 Option 1 (outside USA)  
online support form:  
<http://www.ixiacom.com/support/inquiry/>

**EMEA Ixia Europe Limited**  
One Globeside, Fieldhouse Lane  
Marlow, SL7 1HZ  
United Kingdom  
+44 1628 405750  
FAX +44 1628 405790  
[salesemea@ixiacom.com](mailto:salesemea@ixiacom.com)

**Support:** [eurosupport@ixiacom.com](mailto:eurosupport@ixiacom.com)  
+44 1628 405797  
online support form:  
[http://www.ixiacom.com/support/inquiry/  
?location=emea](http://www.ixiacom.com/support/inquiry/?location=emea)

**Asia Pacific**  
210 Middle Road  
#08-01 IOI Plaza  
Singapore 188994  
+65 6332 0126  
[Support-Field-Asia-Pacific@ixiacom.com](mailto:Support-Field-Asia-Pacific@ixiacom.com)

**Support:** [Support-Field-Asia-Pacific@ixiacom.com](mailto:Support-Field-Asia-Pacific@ixiacom.com)  
+1 818 871 1800 (Option 1)  
online support form:  
<http://www.ixiacom.com/support/inquiry/>

**Japan Ixia KK**  
Aioi Sampo Shinjuku Building, 16th Floor  
3-25-3 Yoyogi Shibuya-Ku  
Tokyo 151-0053  
Japan  
+81 3 5365 4690  
(FAX) +81 3 3299 6263  
[ixiajapan@ixiacom.com](mailto:ixiajapan@ixiacom.com)

**Support:** [support@ixiacom.com](mailto:support@ixiacom.com)  
+81 3 5365 4690  
online support form:  
<http://www.ixiacom.com/support/inquiry/>

**Ixia India**  
UMIYA Business Bay  
Tower – I, 7th Floor, Cessna Business Park  
Outer ring road (Marathalli- Sarjapur ring road)  
Kadubeesanahalli Village, Vartur Hobli  
Bangalore 560 037  
India  
+91 80 42862600

**Support:** [support-india@ixiacom.com](mailto:support-india@ixiacom.com)  
+91 80 32918500  
online support form:  
[http://www.ixiacom.com/support/inquiry/  
?location=india](http://www.ixiacom.com/support/inquiry/?location=india)

