Black Book

Edition 7

MPLS-TP

http://www.ixiacom.com/blackbook

November 2010

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.

Your feedback is greatly appreciated!

Contents

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:

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

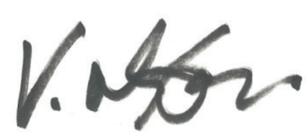
Volume 16 – Ultra Low Latency (ULL) Testing

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)

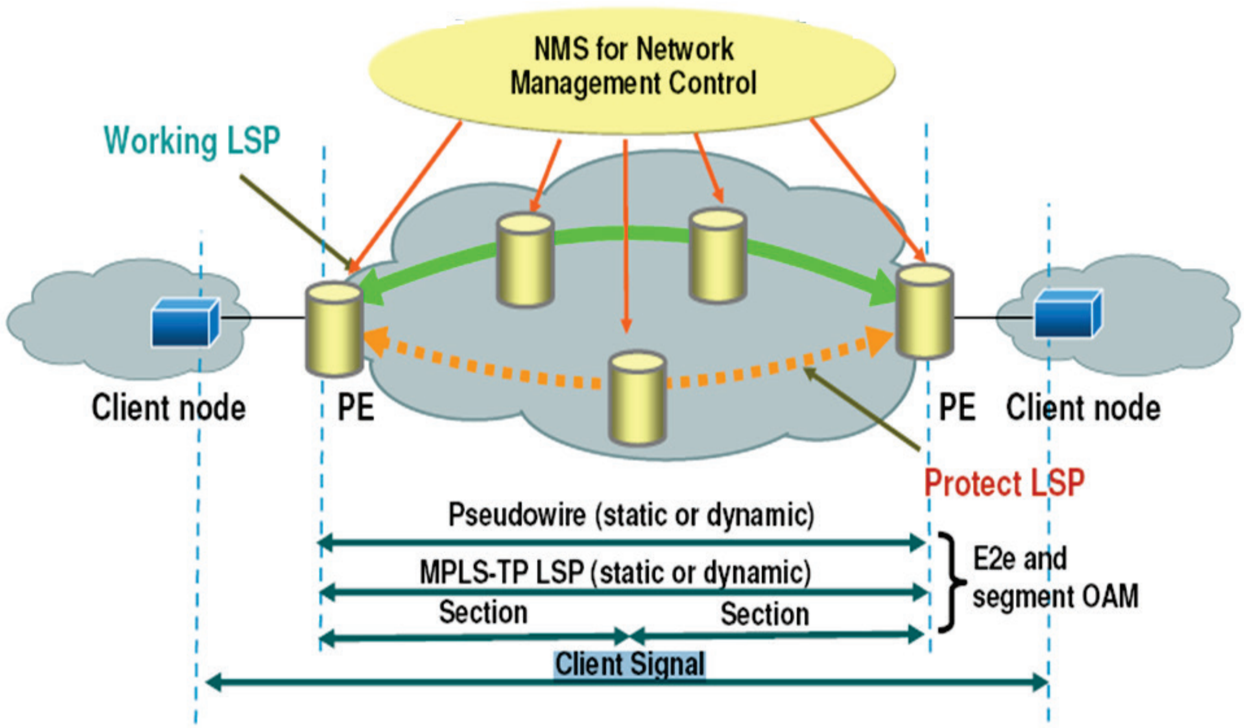


Figure 1 MPLS-TP Architecture: Direct Inheritance from PWE3 but with Added Functions in OAM, Protection, and Static Configuration

- 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)

- 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

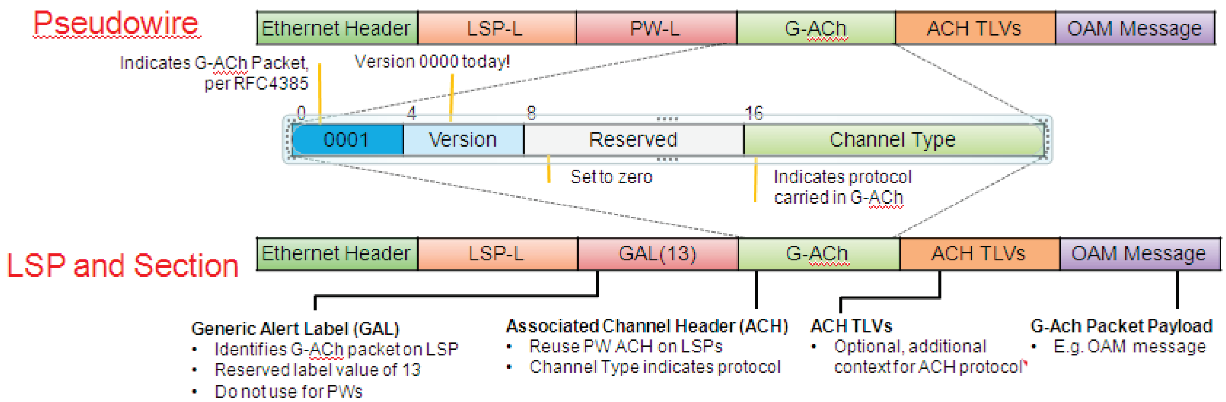


Figure 2 G-ACh and GAL Encapsulation for MPLS-TP PW and LSP

- 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 pesudowire 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).

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.

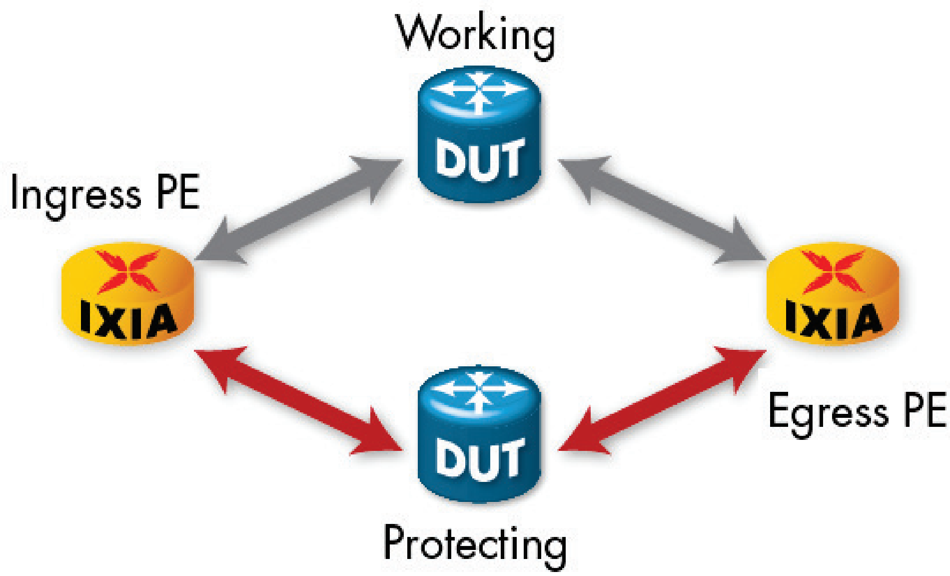


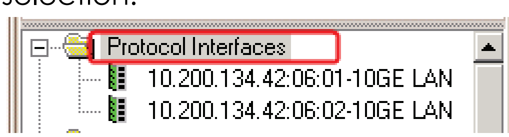
Figure 3 Test Setup for Testing BFD Interop with G-ACh and GAL Encapsulation

Step-by-Step Procedures by using IxNetwork

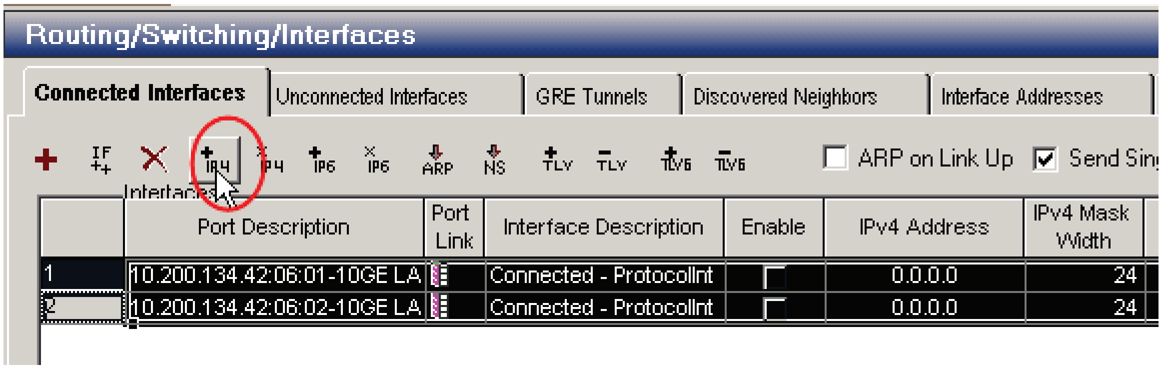
Note: You can configure the test by either using the MPLS-TP wizard or performing the steps manually. As an example, the following steps show the manual approach. Other tests later will show the use of the wizard.

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.

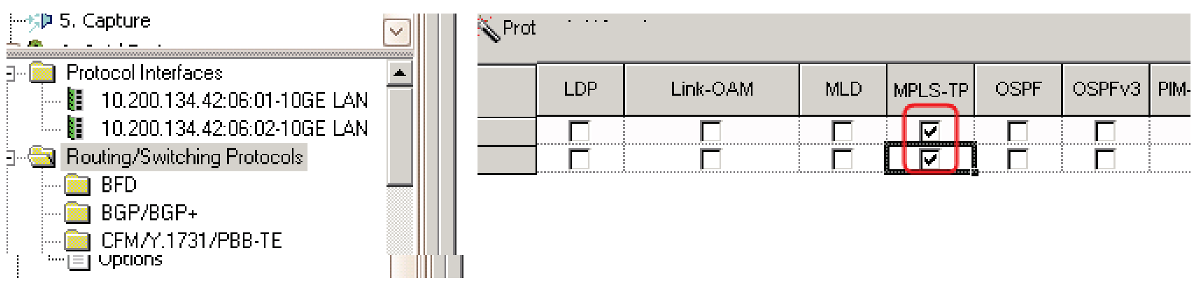


b. Click to highlight the test port(s) and add an IP address to the protocol interfaces. Change the IP address, as appropriate, and enable the protocol interfaces.

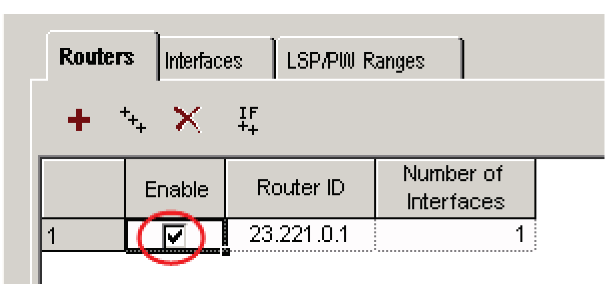


c. Select the Discovered Neighbors and note down the learned MAC address. This will be used by MPLS-TP config later on.

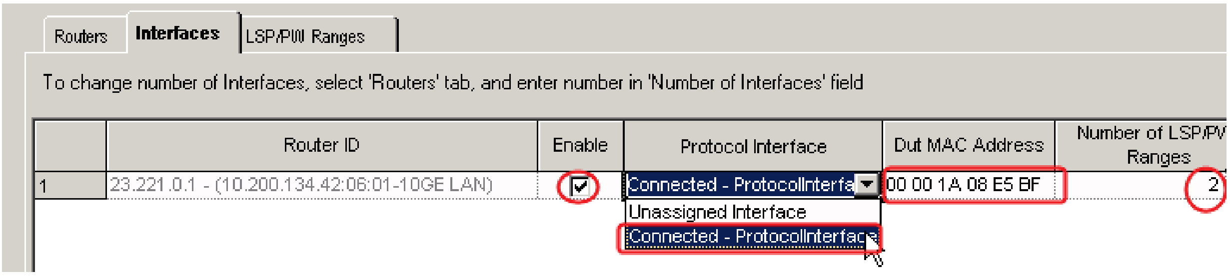
2. Click the Routing/Switching Protocols folder and select the MPLS-TP check boxes.



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.

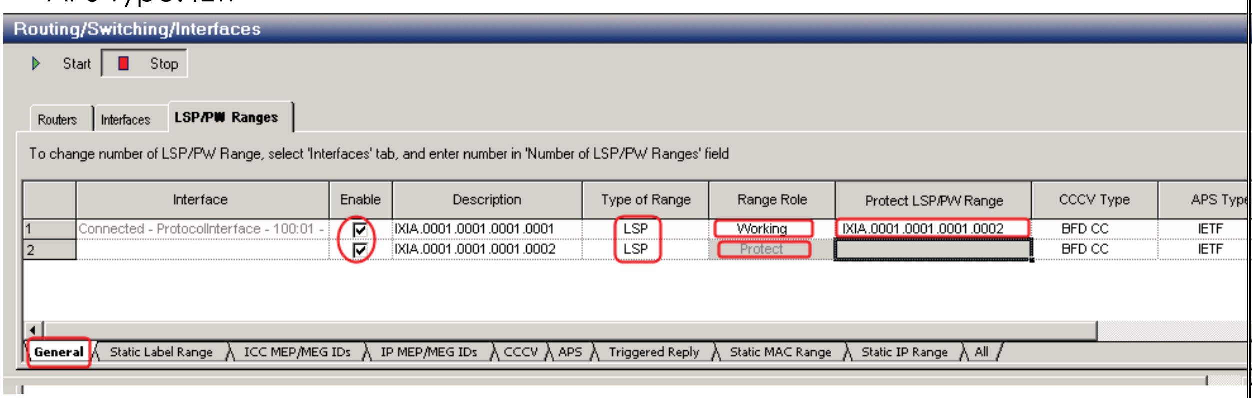


4. Configure the Interface to bind the protocol interface created in step 1, and enter the DUT MAC address, which is also noted in step 1. Enable the interface by selecting the check box and enter the number of LSP/PW Ranges as 2.

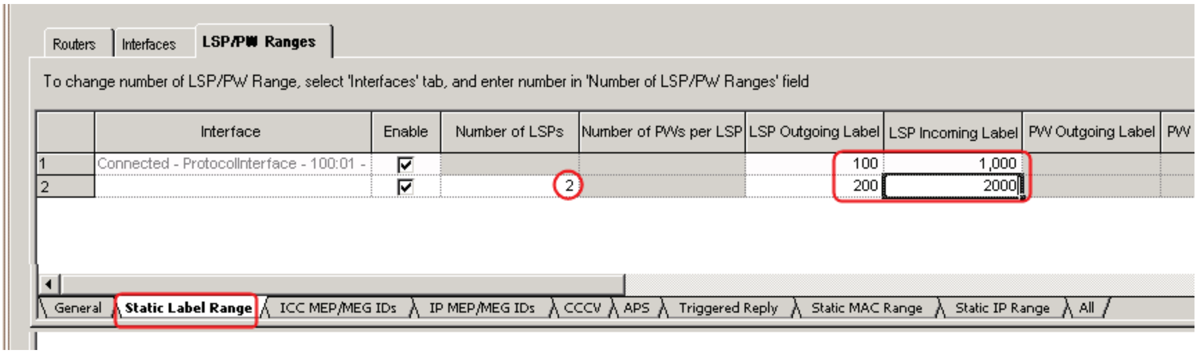


5. Configure the LSP/PW Ranges as follows:

   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

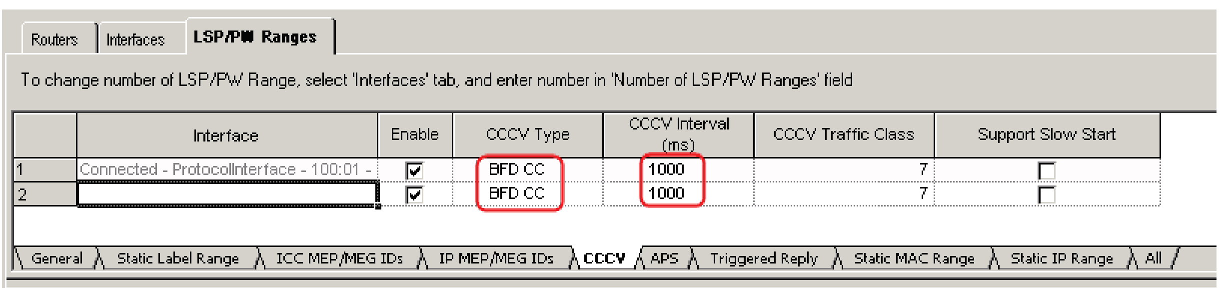


b. Static Label Range tab:
Number of LSPs: 2
LSP Outgoing Label: 100 for working and 200 for protect
LSP Incoming Label: 1000 for working and 2000 for protect

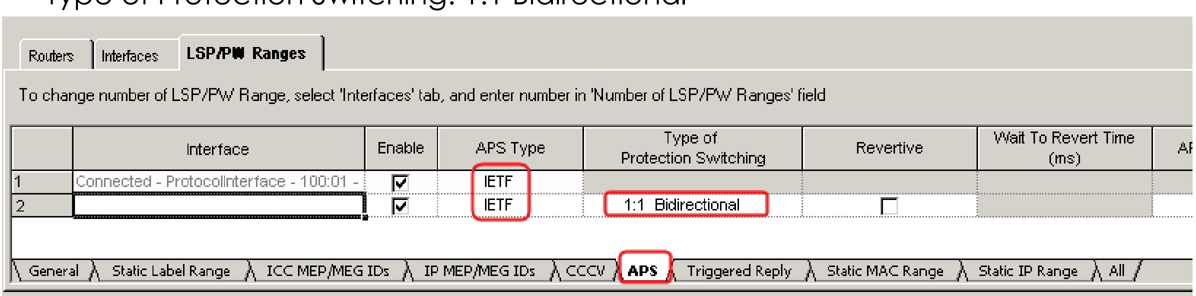


c. The next two tabs called ICC MEP/MEG IDs and IP MEP/MEG IDs are for Y.1731. We will skip them for this test as this test is using BFD as the failure detection mechanism.

d. CCCV tab:
CCCV Type: BFD CC
CCCV Interval: 1000 ms



d. APS tab:
APS Type: IETF
Type of Protection Switching: 1:1 Bidirectional

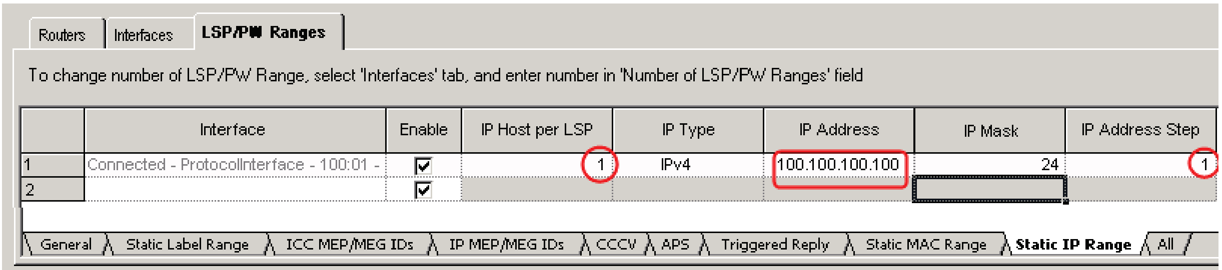


e. Optionally, configure Static MAC or IP for traffic generation and verification.

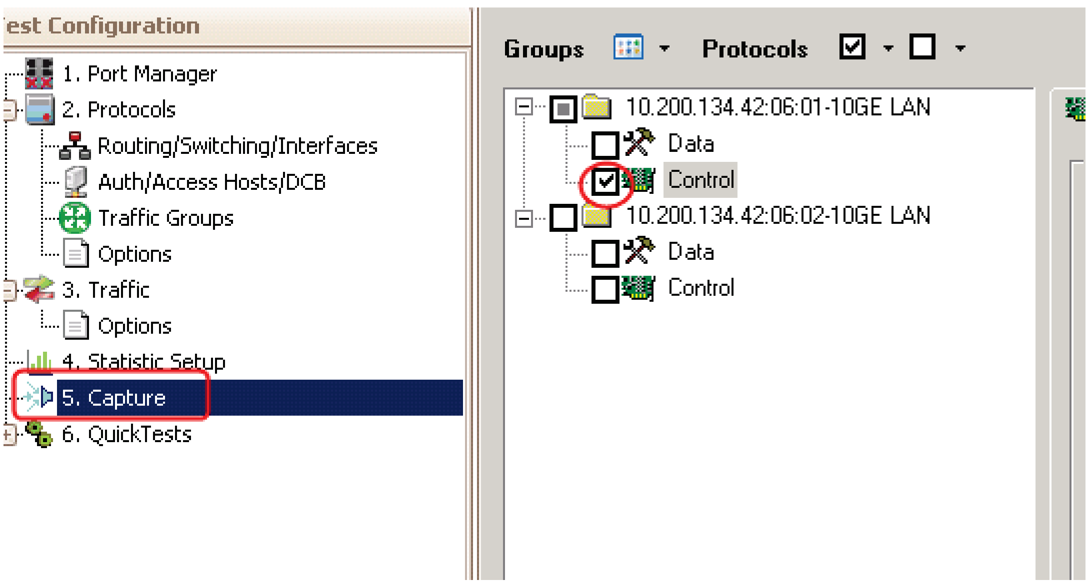
Static IP Range tab:

IP Host per LSP: 1

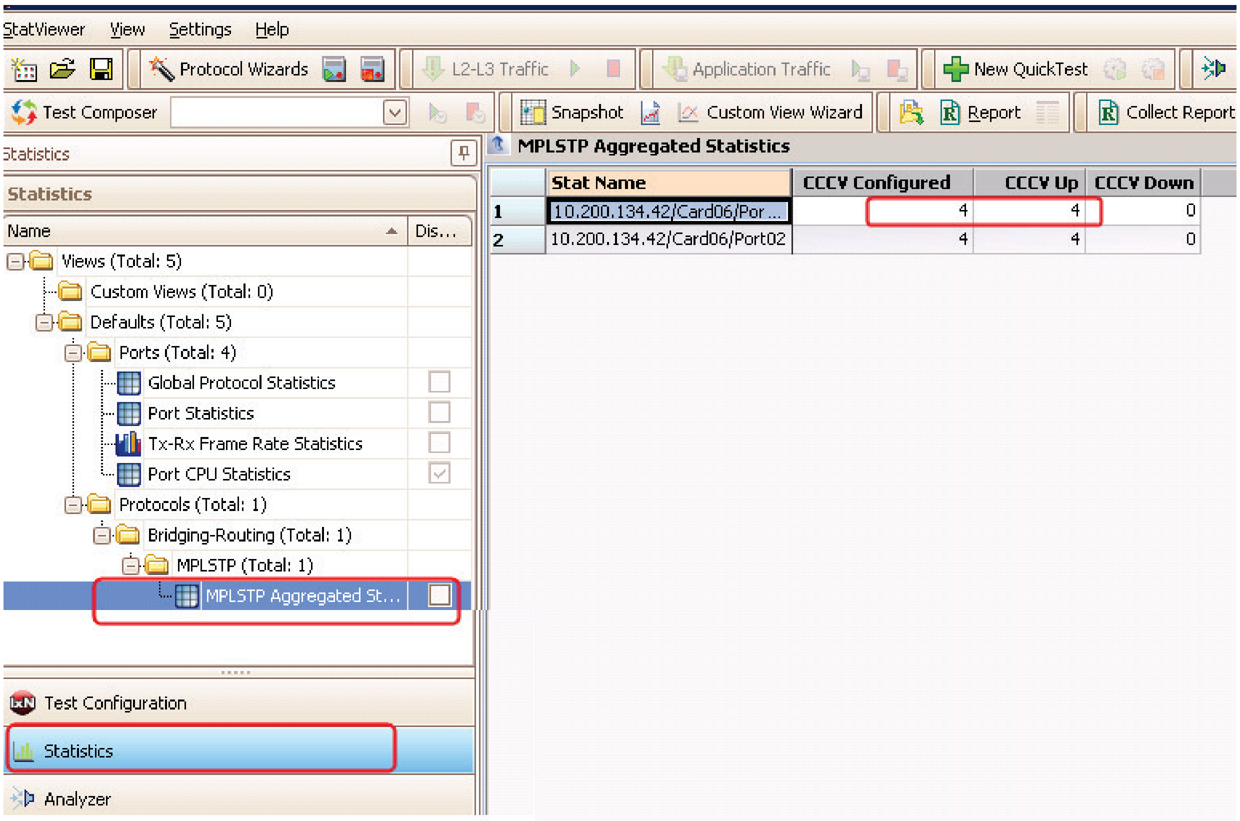
IP Address: 100.100.100.100



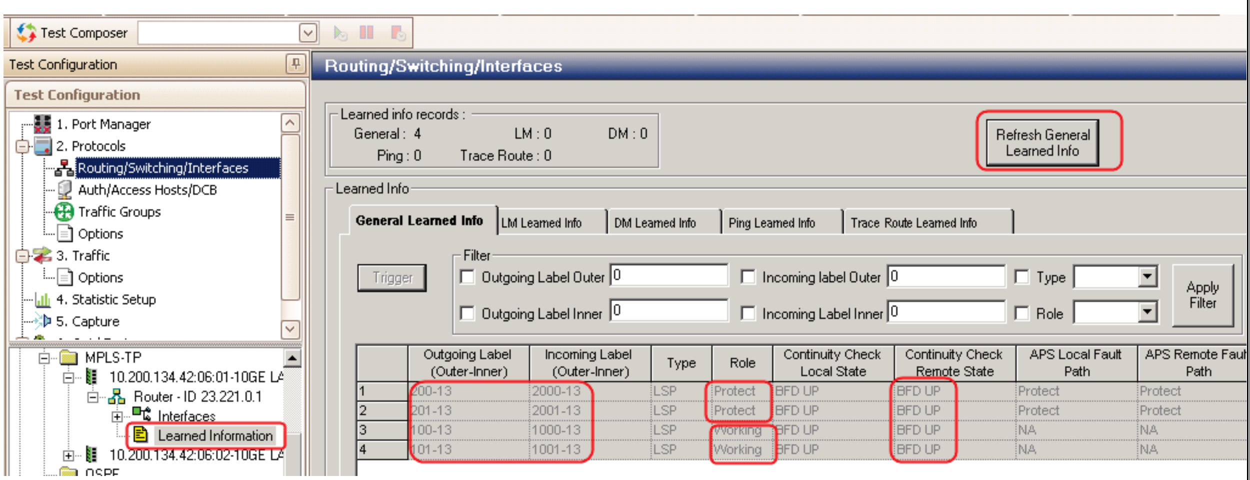
6. Optionally, enable and turn on Capture before starting the protocol.



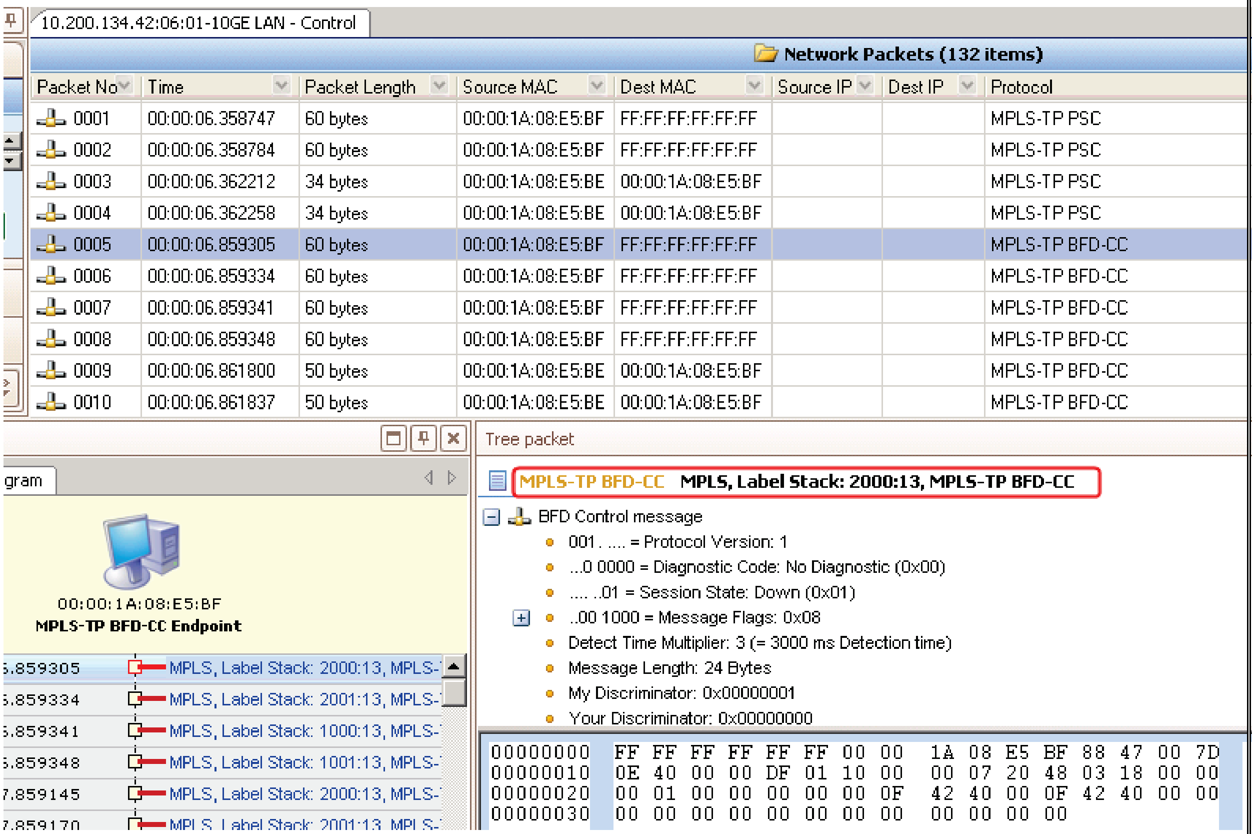
7. Start the protocol. Next, click the **Statistics** tab, and then click **MPLSTP Aggregated Stats**. It displays the total number of CCCV sessions configured as well as the Up/Down sessions. In this example, we have 4 sessions because there are two protect LSPs protecting two working LSPs.



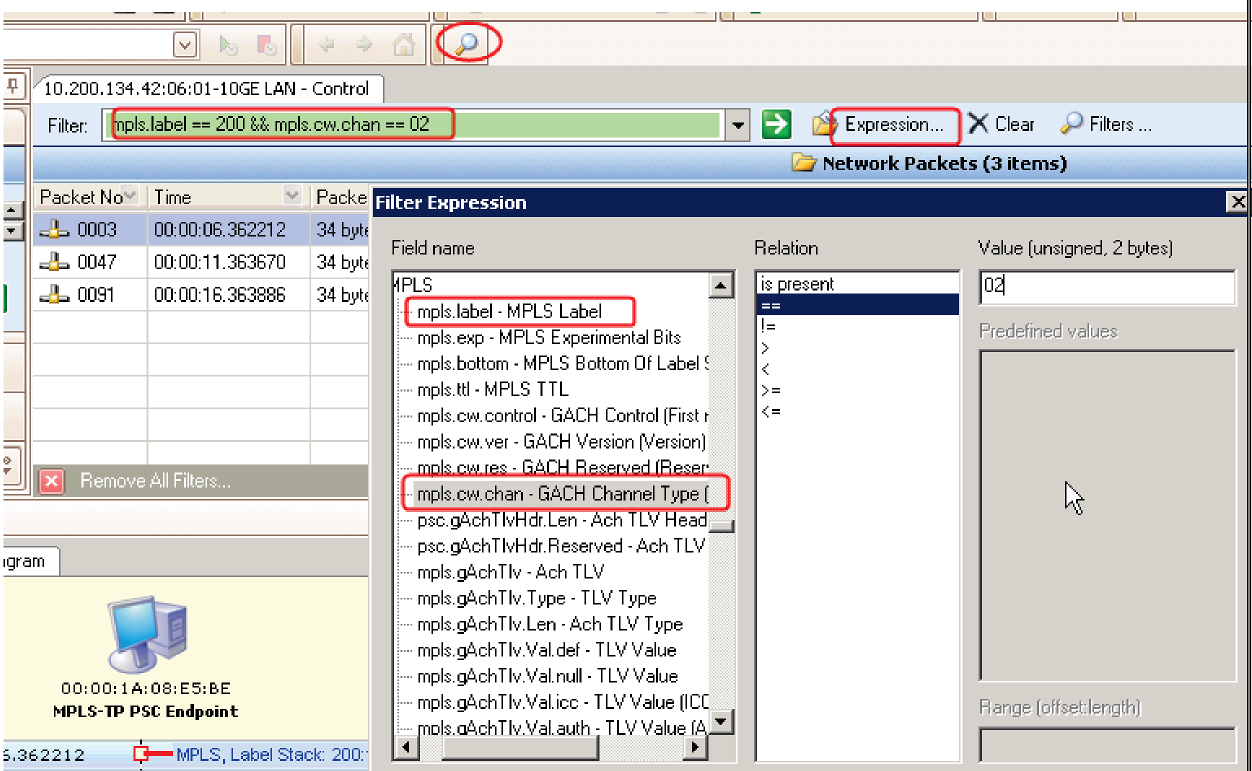
8. The other place to verify if all BFD sessions are up or not is to navigate to the **MPLS-TP** -> **Learned Information** folder and click **Refresh General Learned Info**. It displays clearly each BFD session status and its incoming and outgoing labels.



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. 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.

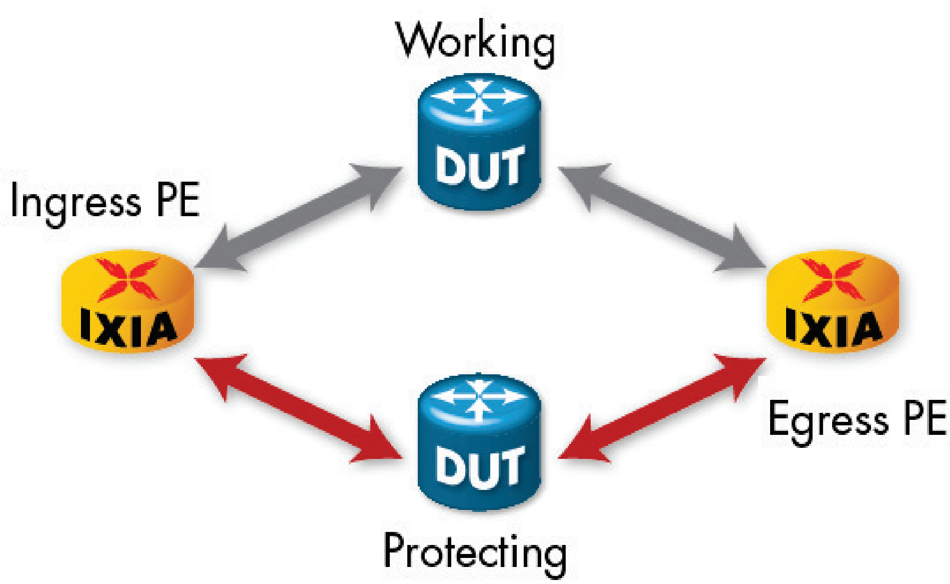
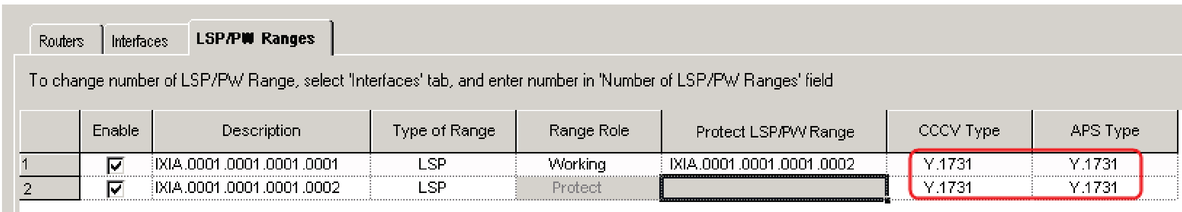


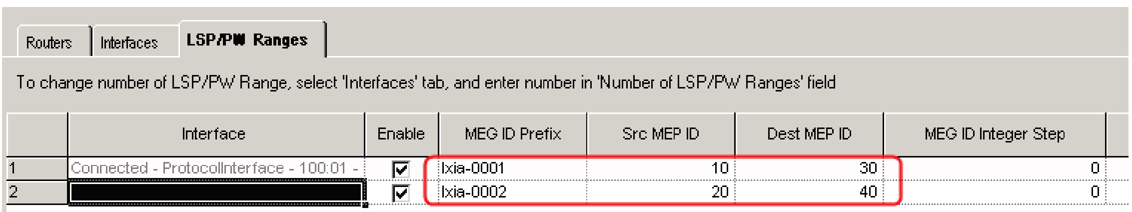
Figure 4 Test Setup for Testing MPLS-TP OAM Fuctions

Step-by-Step Procedures by using IxNetwork

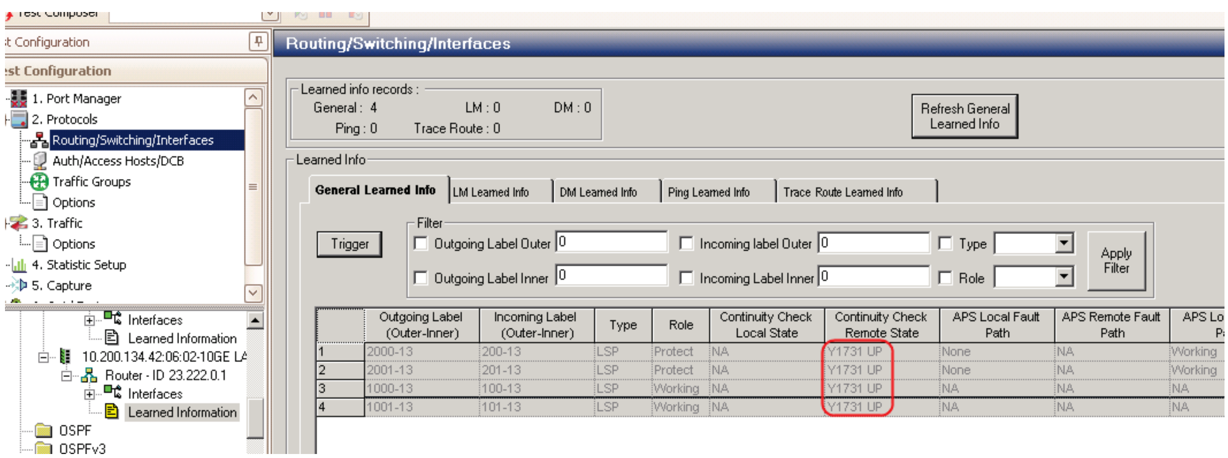
1. Continue from the previous test. Keep the protocol interfaces and the MPLS-TP routers, interfaces, and LSP/PW ranges. Change CCCV and APS types to use Y.1731.



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

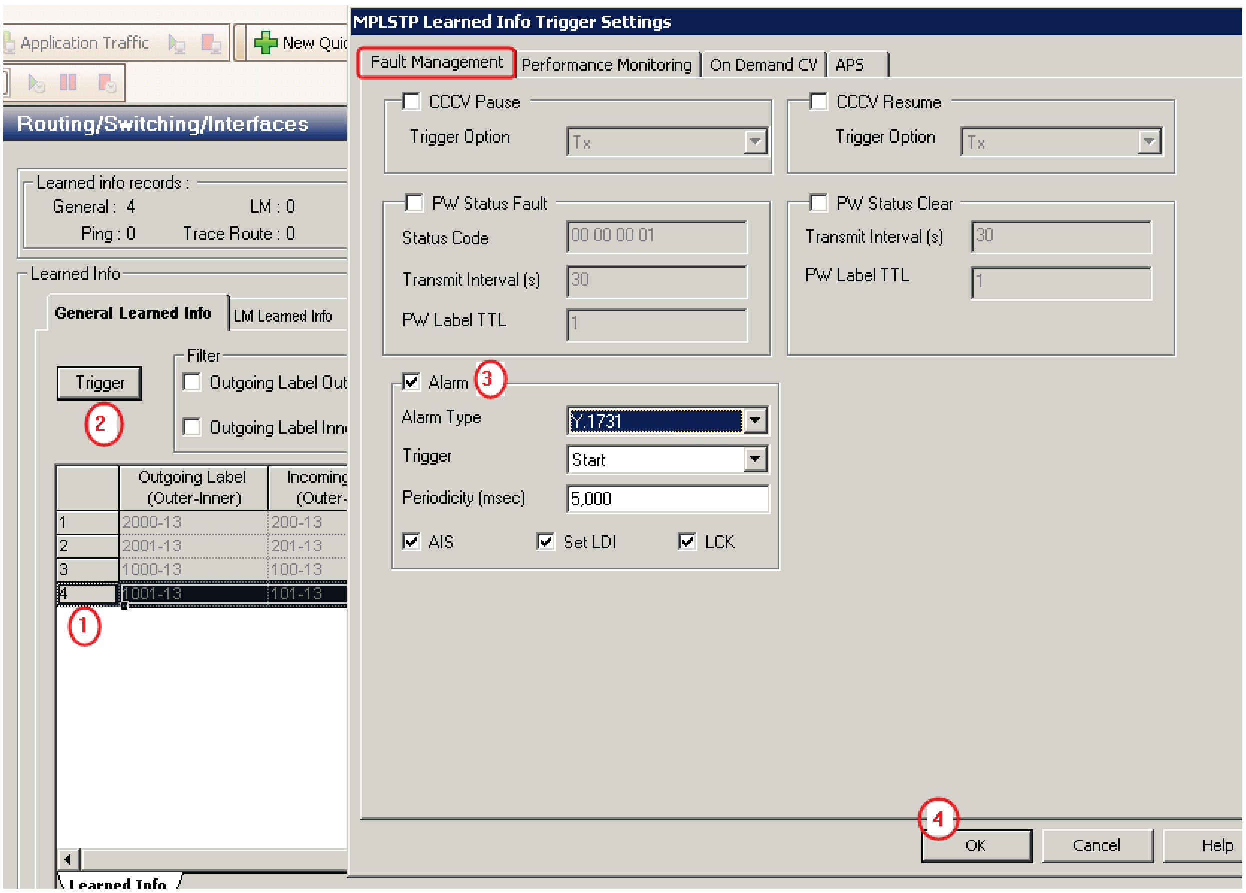


3. Start the MPLS-TP emulation and ensure that all Y.1731 CCM reach the UP state. This can be verified either from the aggregated CCCV stats or through the **Learned Info** pane.

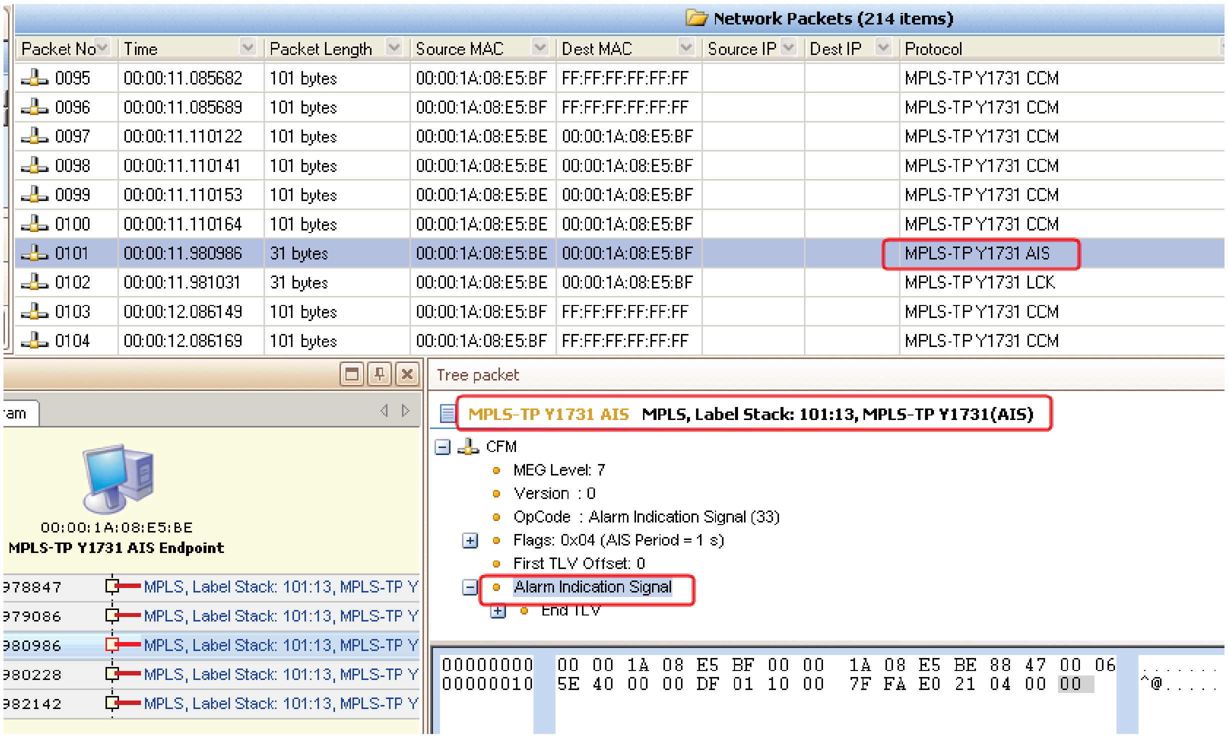


4. To inject Alarms to DUT, do the following:

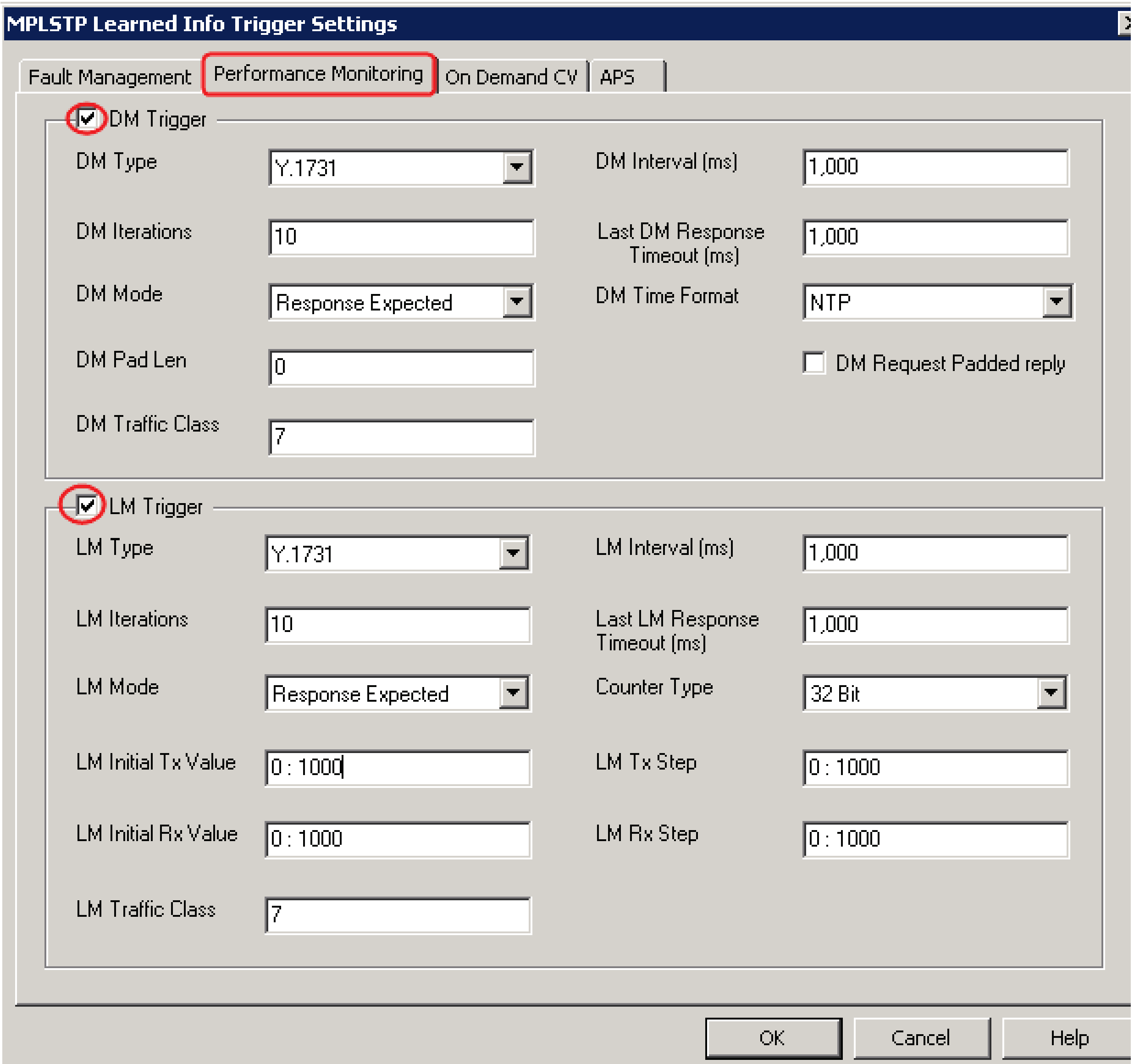
   a. Under the **Learned Info** pane, click to select the LSP/PW(s) that you want to inject alarms to.
   b. Click **Trigger**.
   c. Select the **Alarm** check box.
   d. In the **Alarm Type** list, click **Y.1731**. Toggle the supported Alarms.
   e. Click **Ok** to start sending the selected alarms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



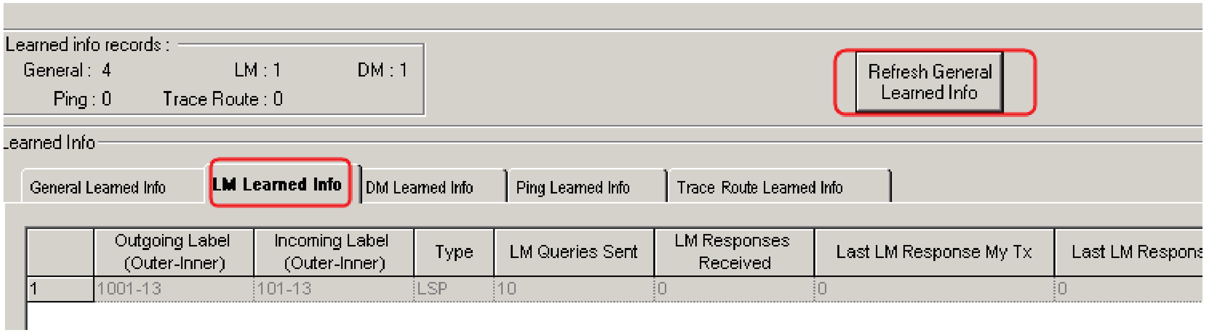
5. To monitor Alarms from DUT, start the capture and use IxAnalyzer to decode the alarms from DUT.



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



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.



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.

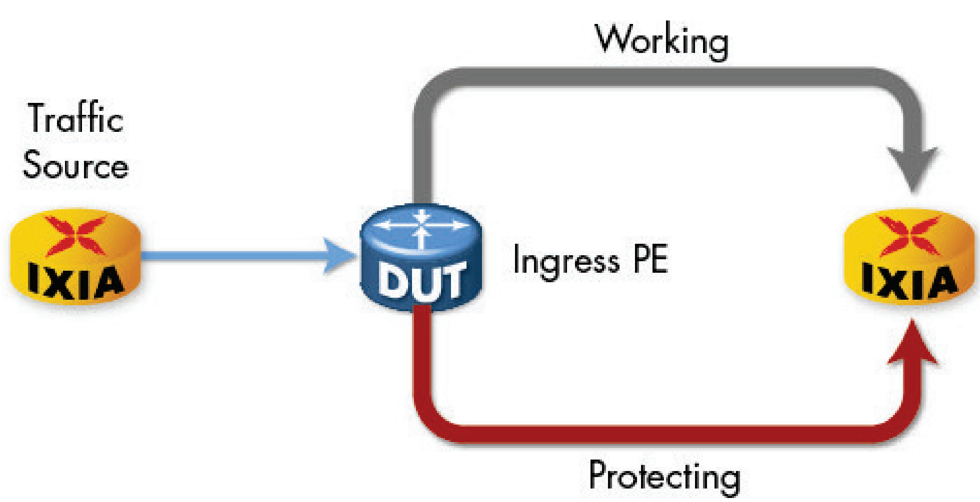
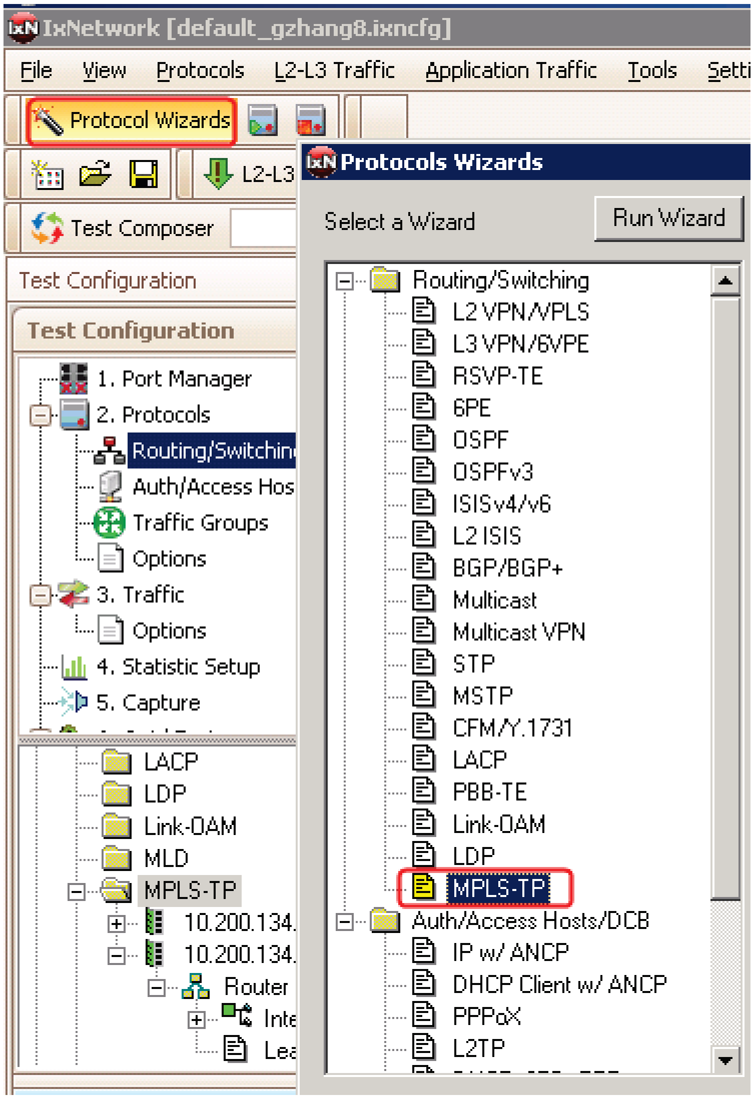


Figure 6 Test Setup for Testing Linear APS and Switchover Time

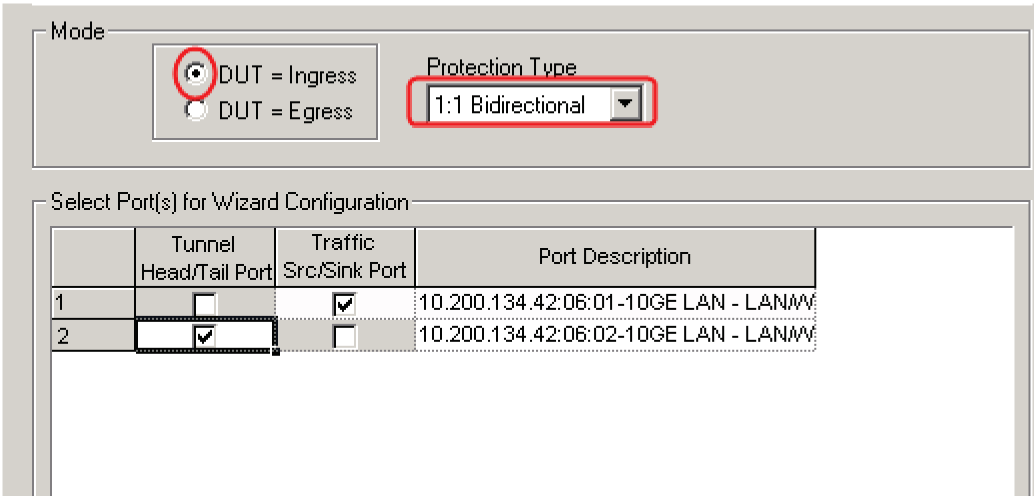
Step-by-Step Procedures by using IxNetwork

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



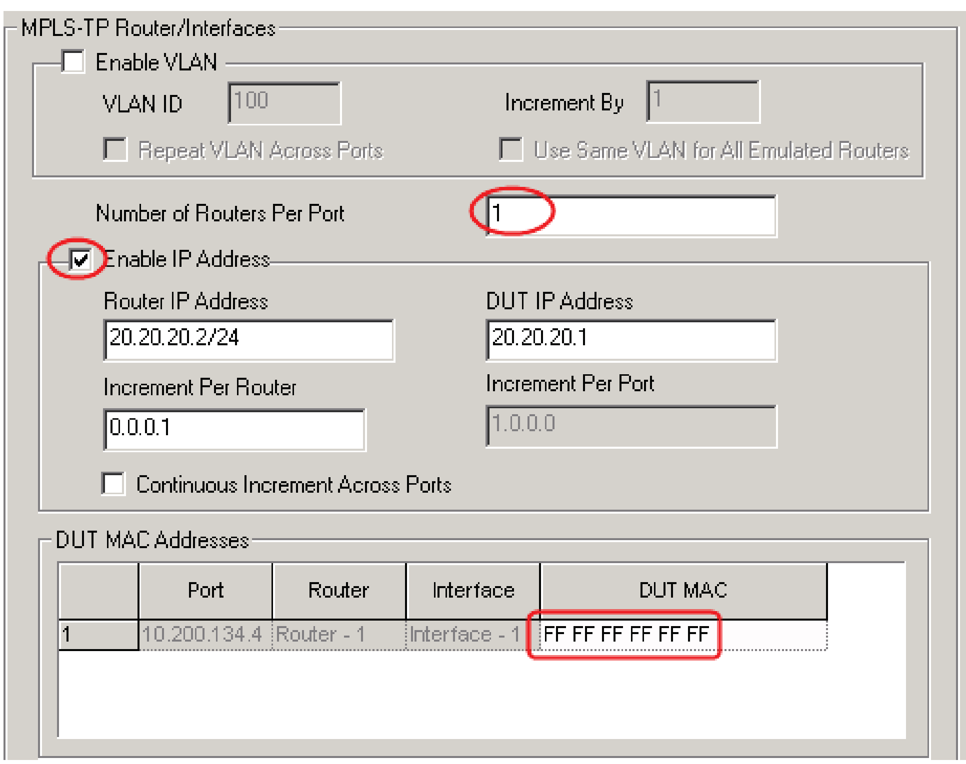
2. In the first page of the MPLS-TP wizard, configure the following:

   DUT = Ingress
   Protection Type = 1:1 Bidirectional
   Traffic Src/Sink: first test port
   Tunnel Head/Tail Port: second test port



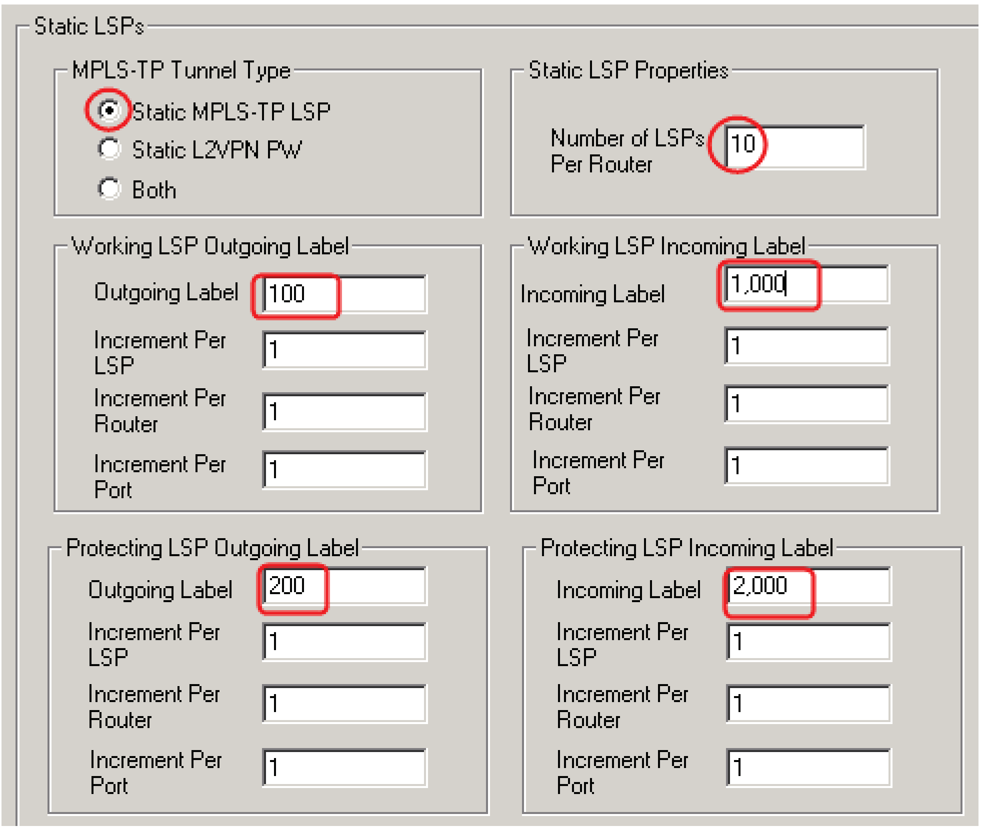
3. In the second page of the wizard, configure the following:

   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



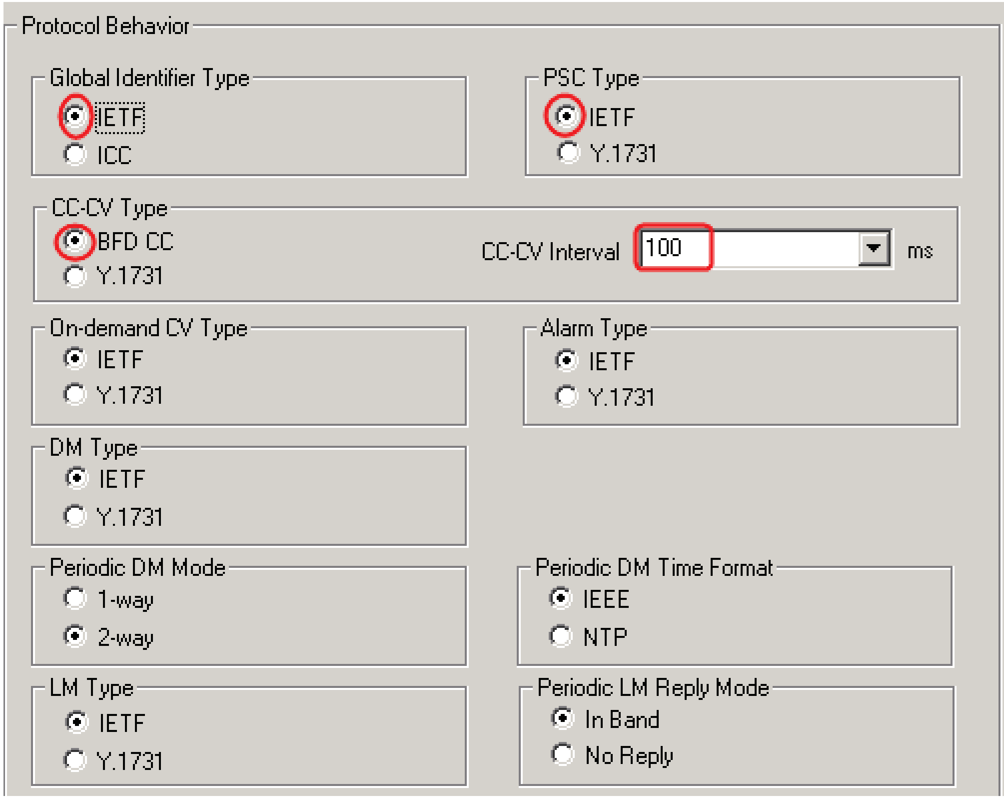
4. In the third page of the wizard, configure the following:

   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

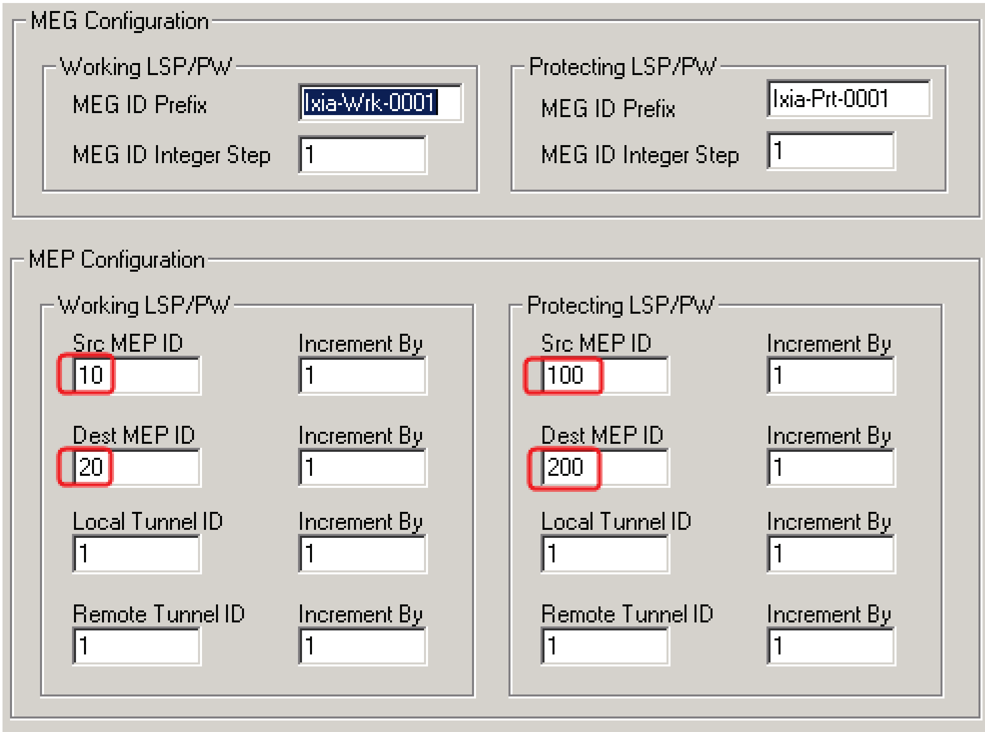


5. In the fourth page of the wizard, configure the following:

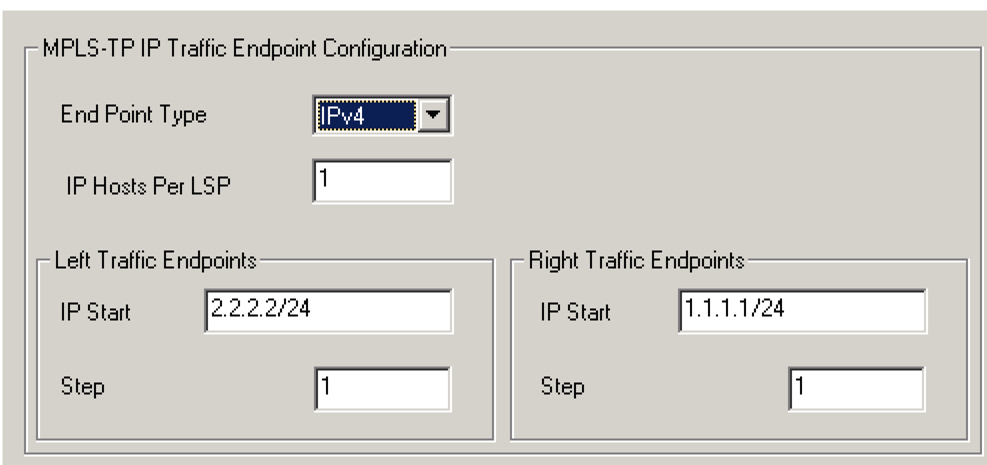
   Global Identifier Type: IETF
   PSC Type: IETF
   CC-CV Type: BFD CC
   CC-CV Interval: Select from the list or enter a specific value
   The rest of the parameters: keep the default values



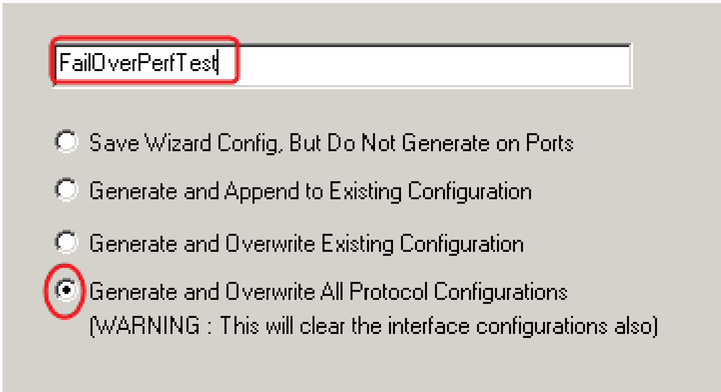
6. The fifth page of the wizard is not applicable to IEFT or BFD. If Y.1731 is used, ensure to enter the Src MEP ID and Dest MEP ID for both working LSP and Protecting LSP.



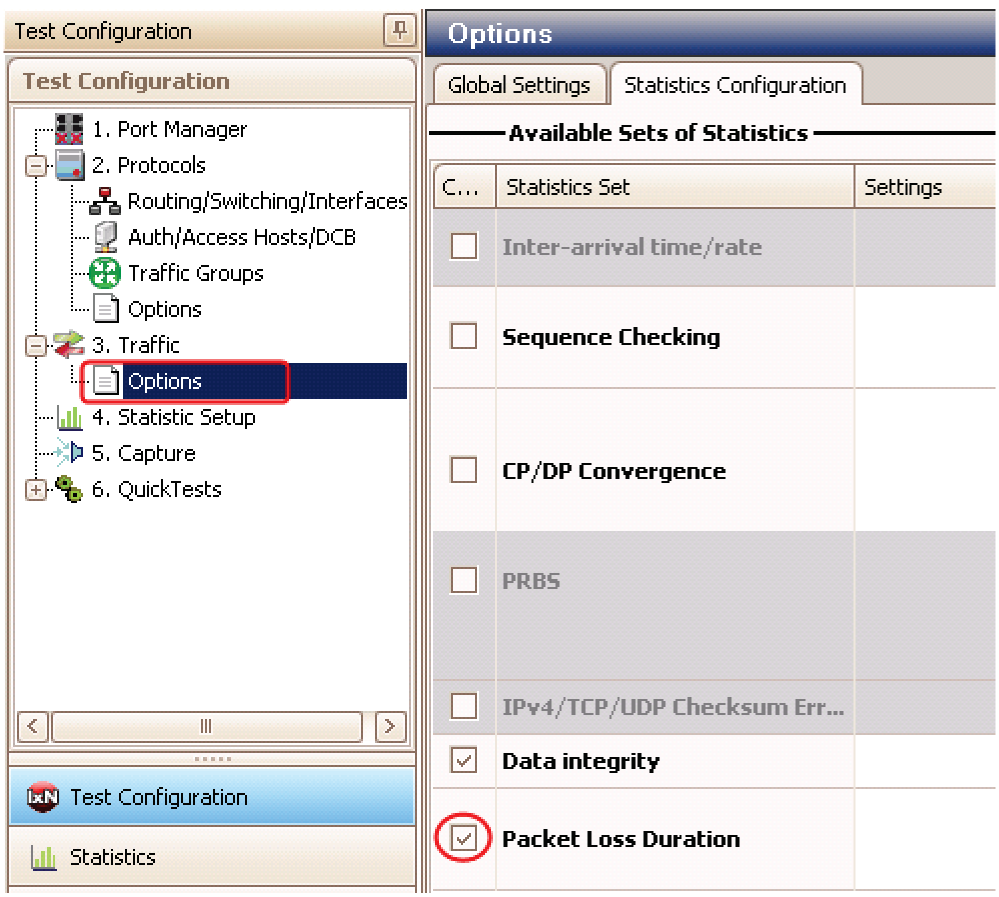
7. In the sixth page, keep the default values and enter some IP or MAC for traffic purpose.



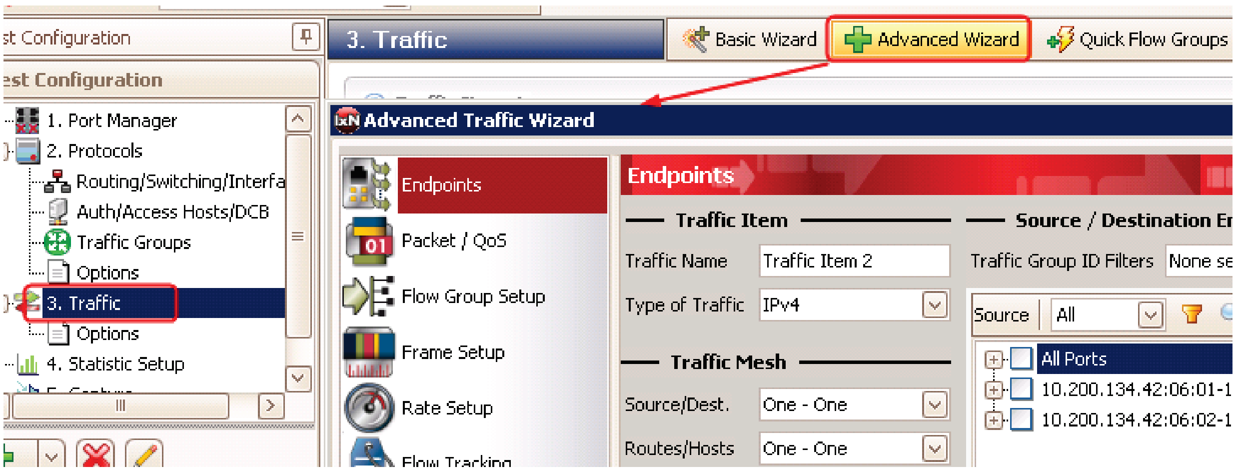
8. In the last page of the wizard, give the config some name and click **Generate and Overwrite All Protocol Configurations**.



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.

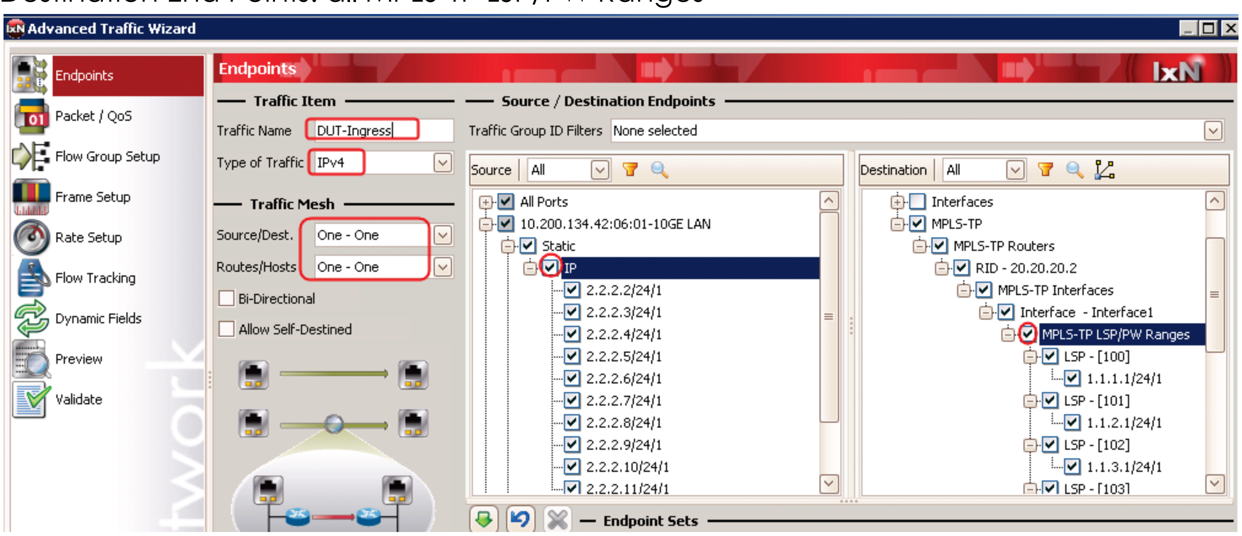


10. Start the traffic wizard.

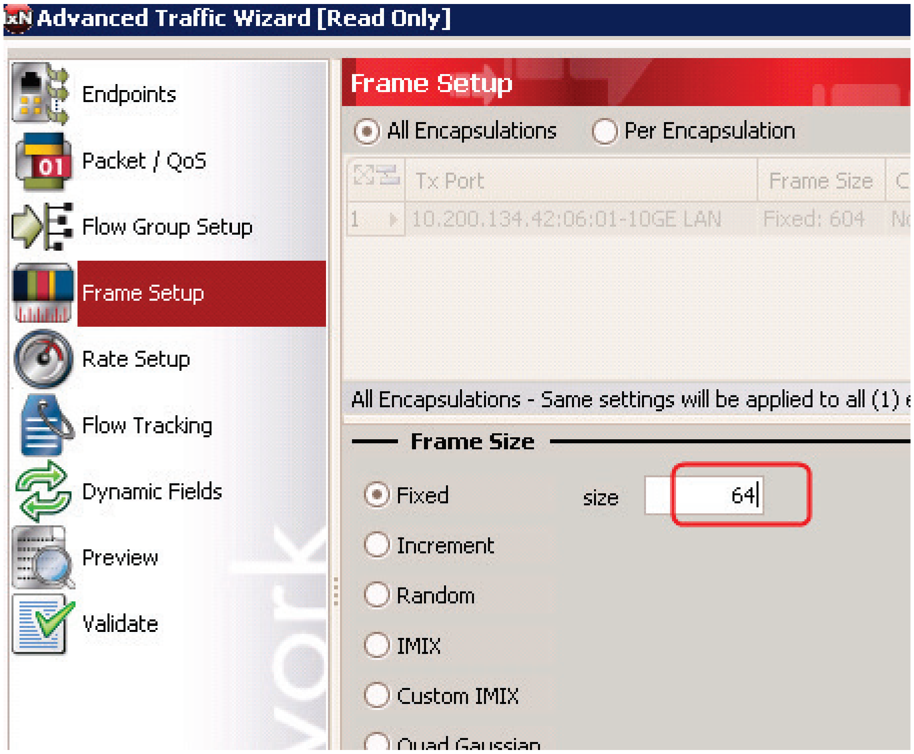


11. In the first page of the Advanced Traffic Wizard, configure the following:

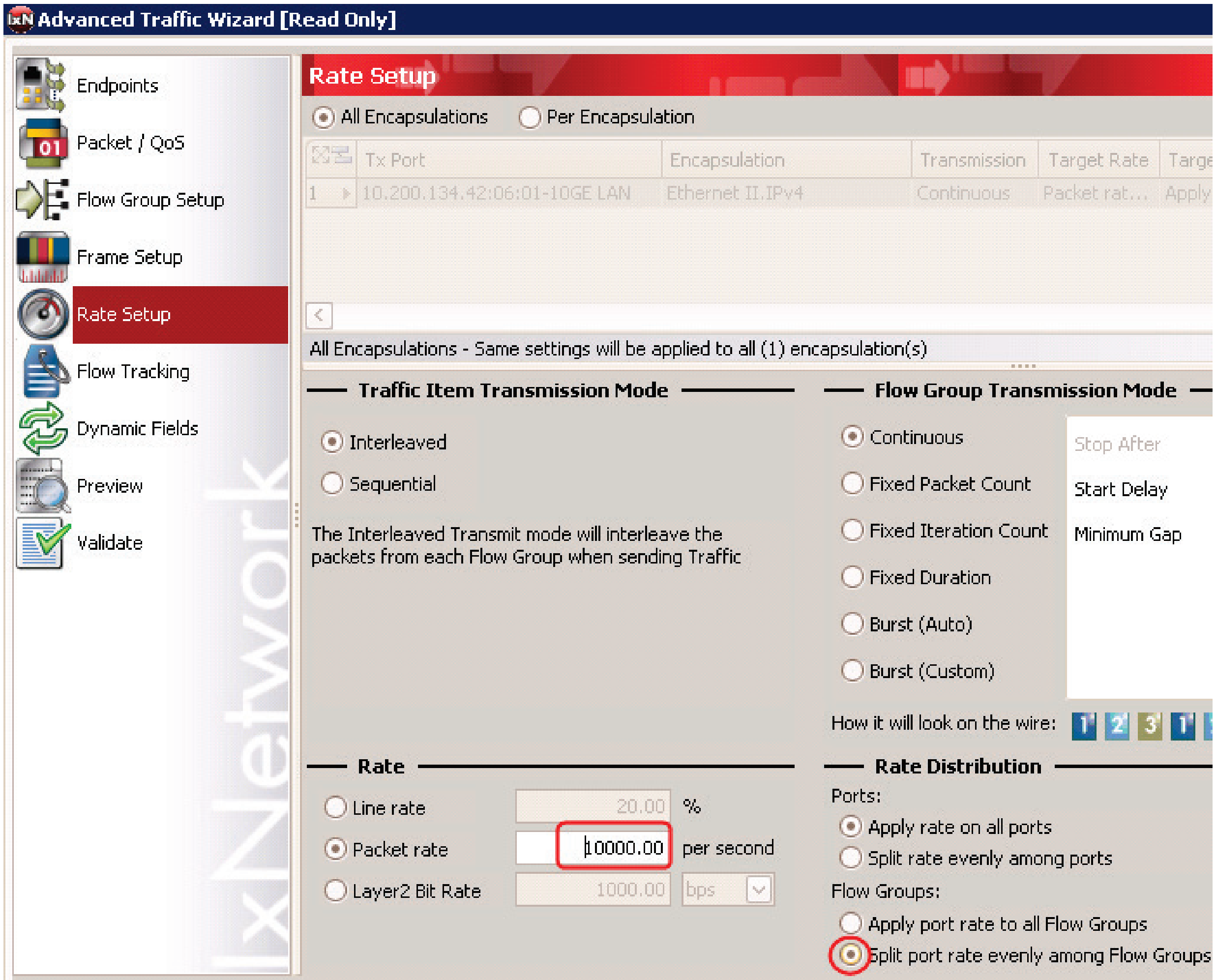
Traffic Name: type a string
Type of Traffic: IPv4
Source/Dest Traffic Mesh: One-One
Routes/Hosts Traffic Mesh: One-One
Source End Points: all static IP
Destination End Points: all MPLS-TP LSP/PW Ranges



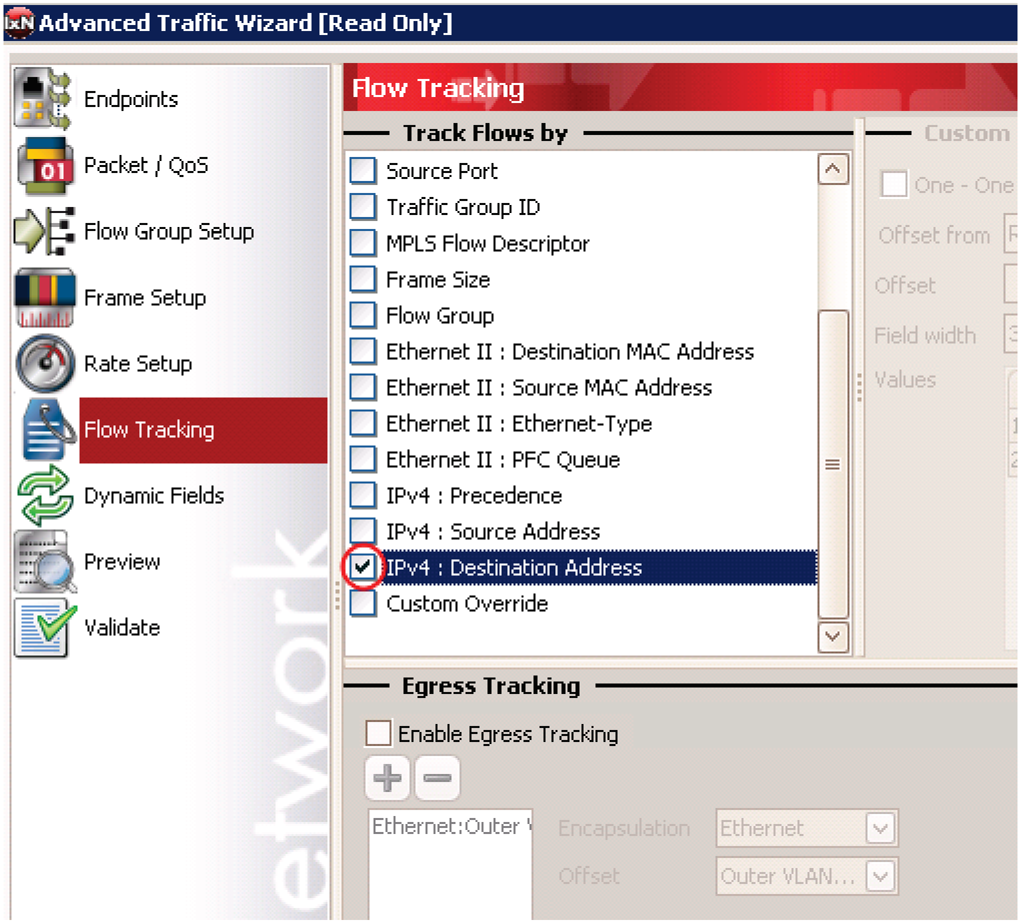
12. Skip Packet/QoS and Flow Group Setup and enter appropriate frame size under Frame Setup.



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

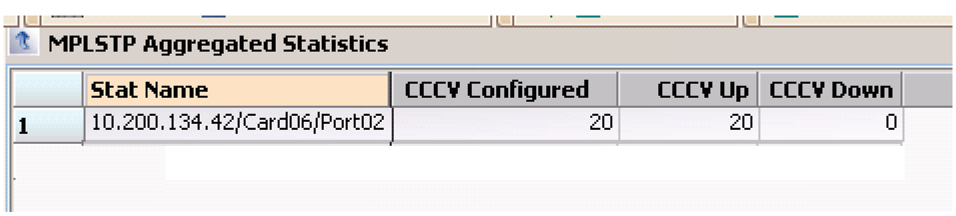


14. For Flow Tracking, because the TX port will be native IP, tracking by either source IP or destination IP is good enough to deliver per-flow stats, including failover time.



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.

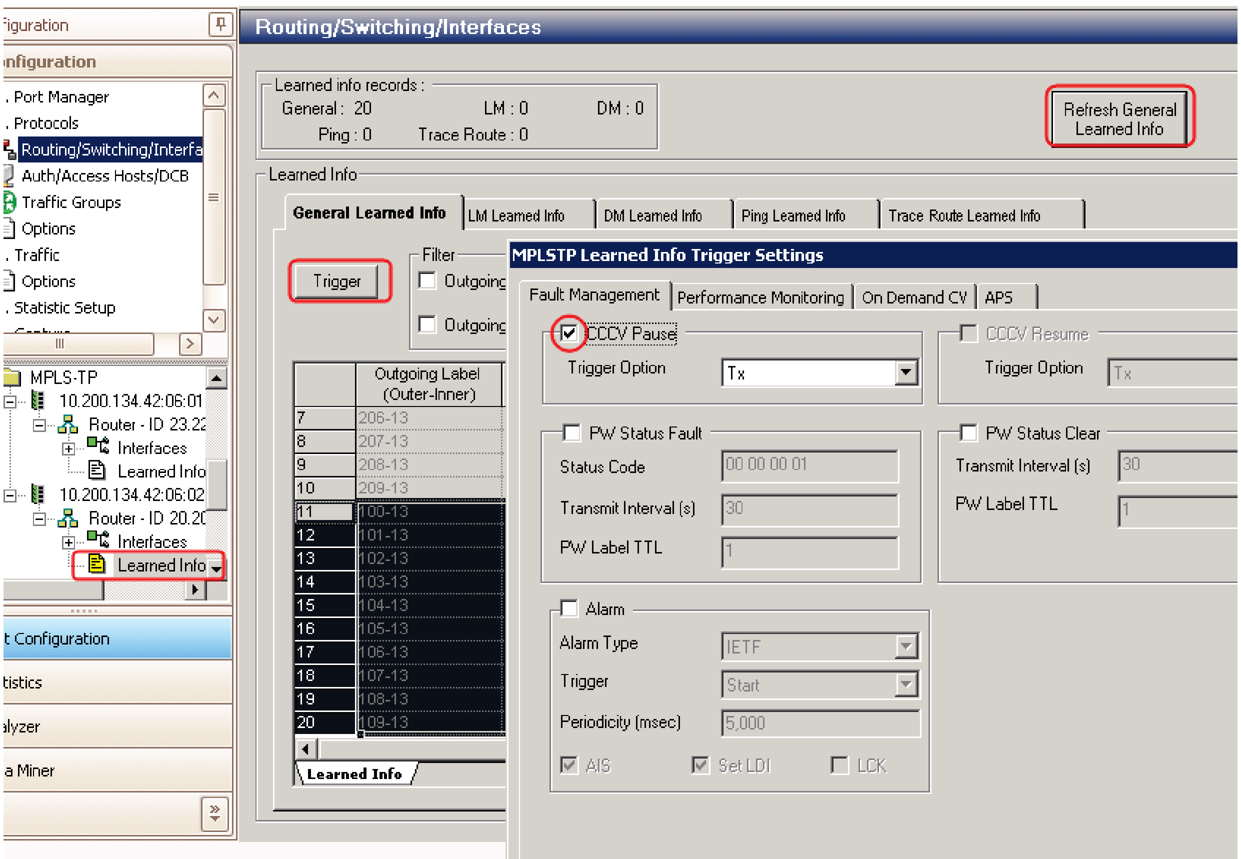


17. Send data plane traffic and ensure that no packet drops occur before switchover.

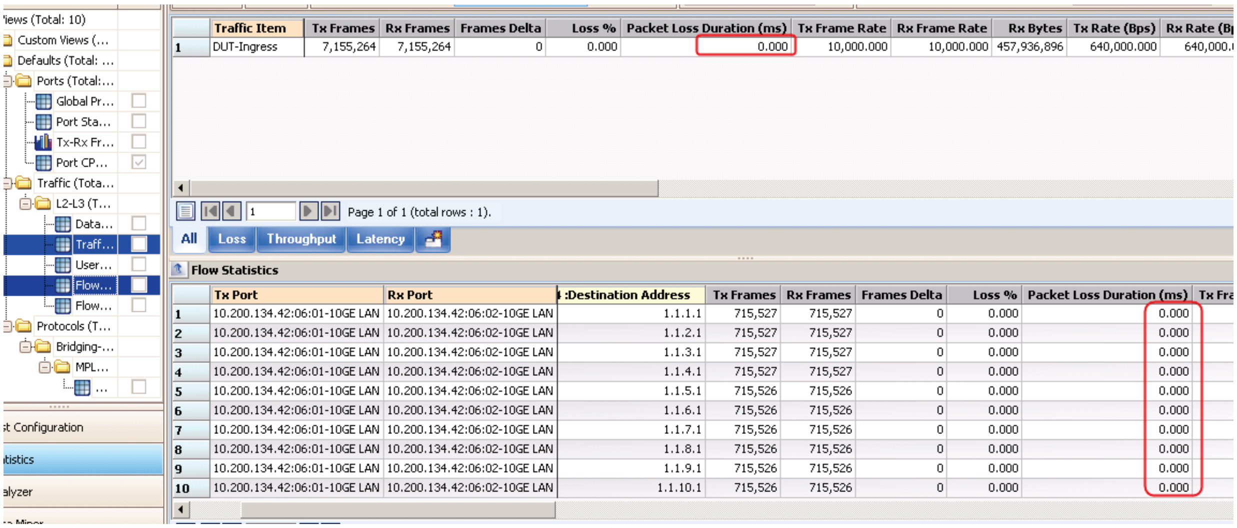
Flow Statistics

	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

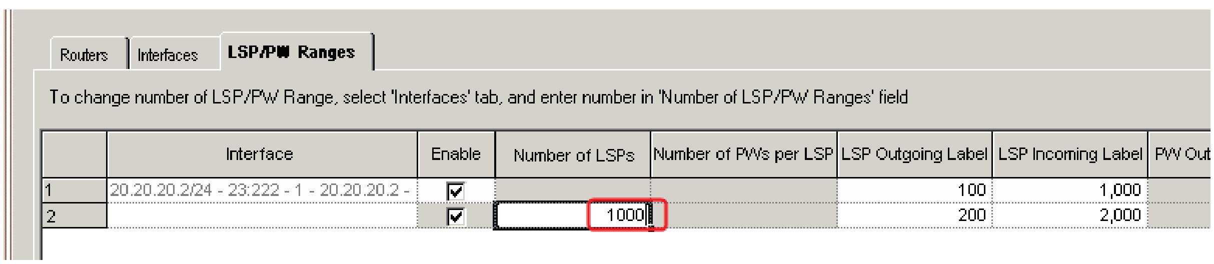
18. Inject errors from the emulated Egress PE to DUT. Select all 10 LSPs and force CCCV Pause on TX.



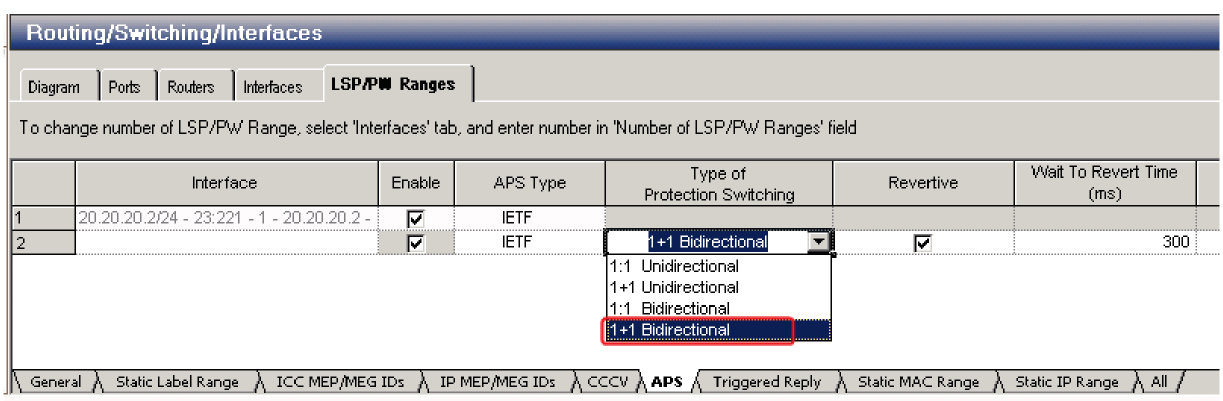
19. Wait for a few seconds and go back to the statistics page to view the Packet Loss Duration on both the aggregated traffic item as well as the individual flow level.



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.



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.



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.

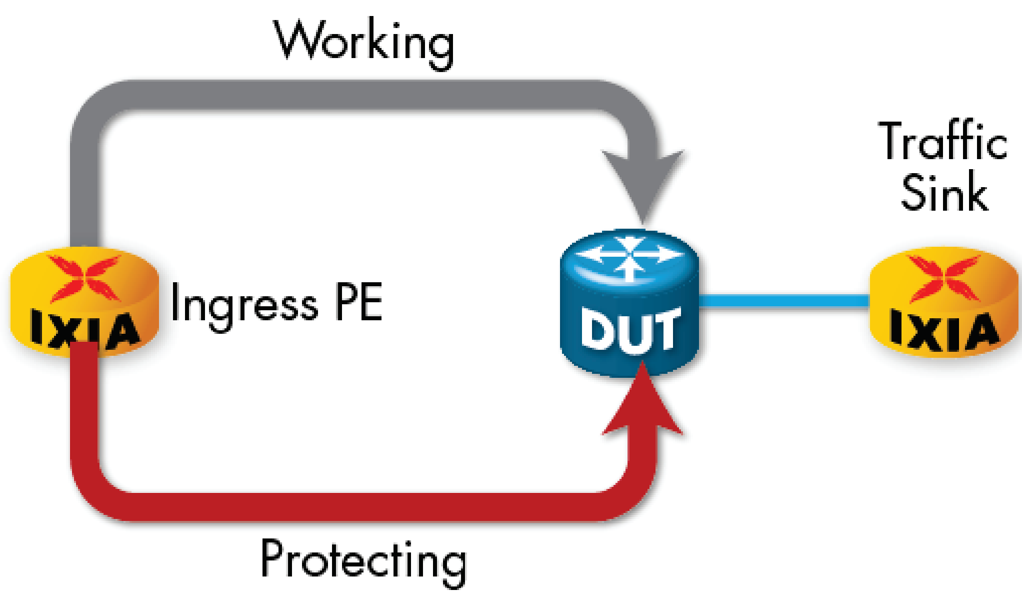


Figure 7 Test Setup for Testing Manual APS Commands

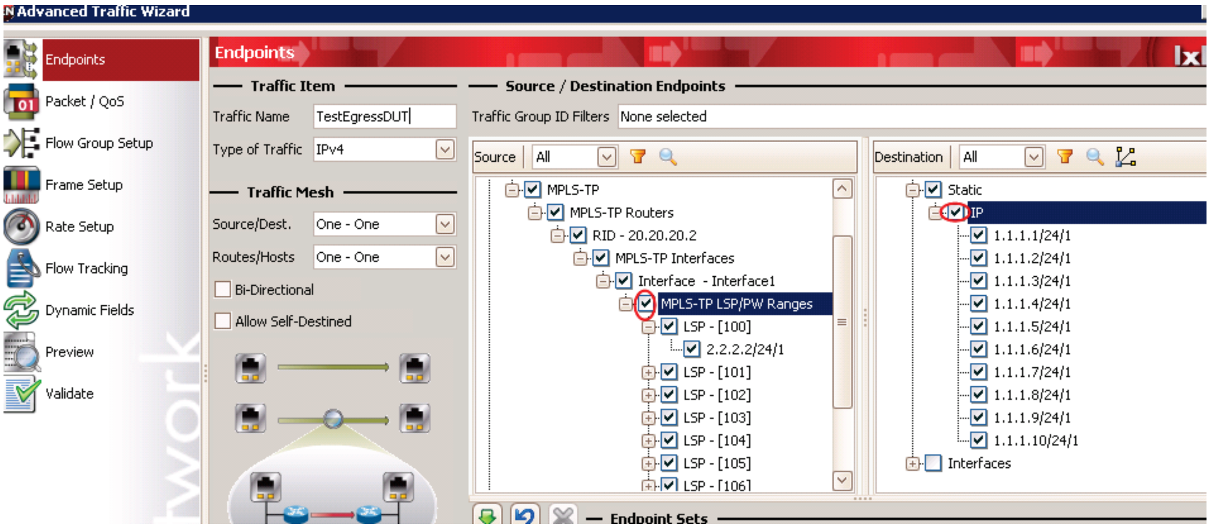
Step-by-Step Procedures by using IxNetwork

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.

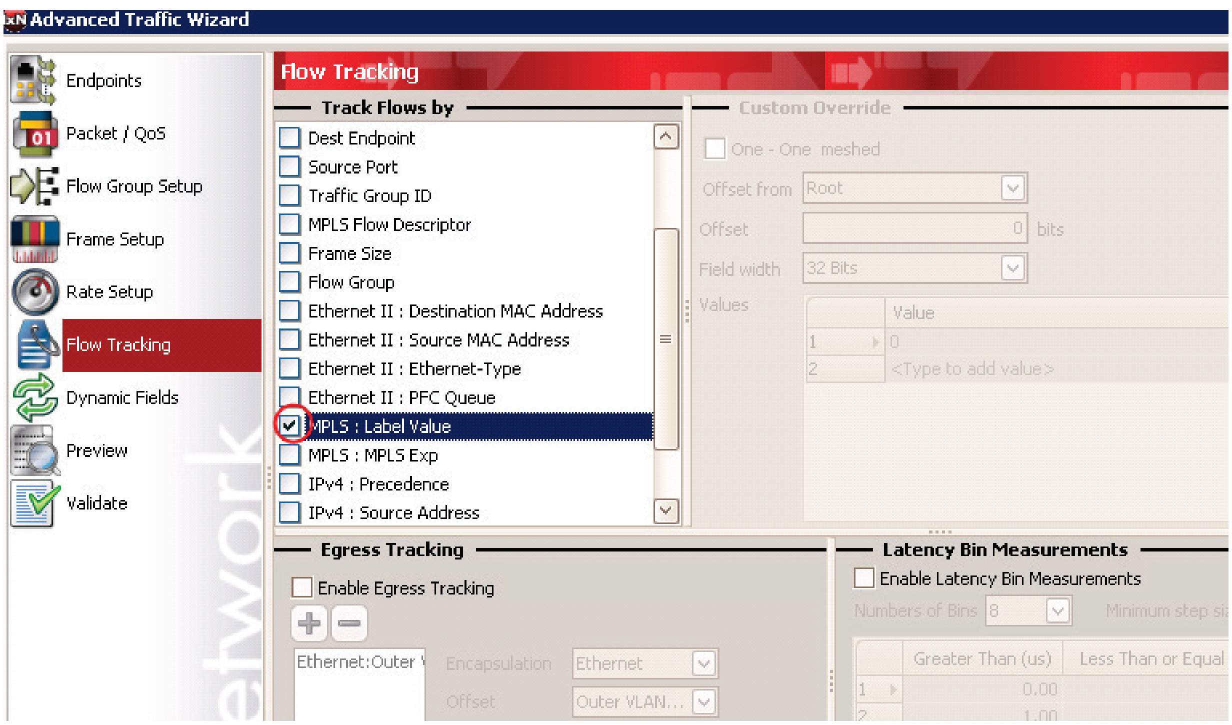
2. Select the APS mode to be 1+1 bidirectional. This is to facilitate traffic analysis at the traffic sink port.

Test Scenario 4: Verify manual APS command functionality

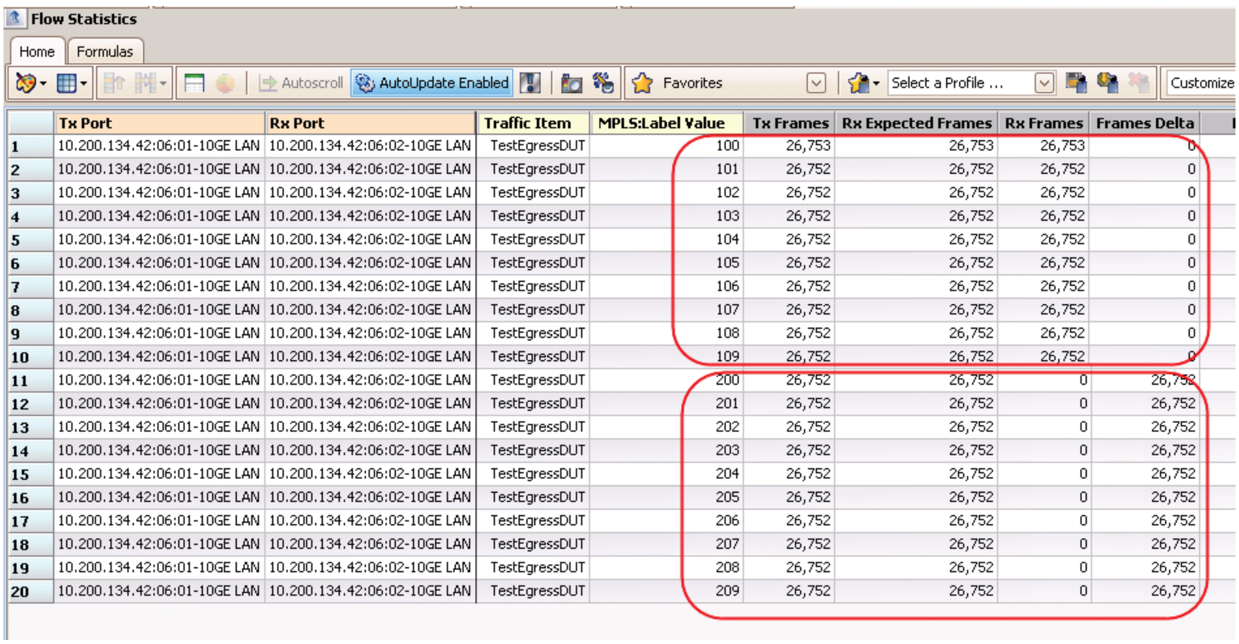
3. Start the Advanced traffic wizard. Select all MPLS-TP LSP ranges on the first port and all Static IP end points.



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

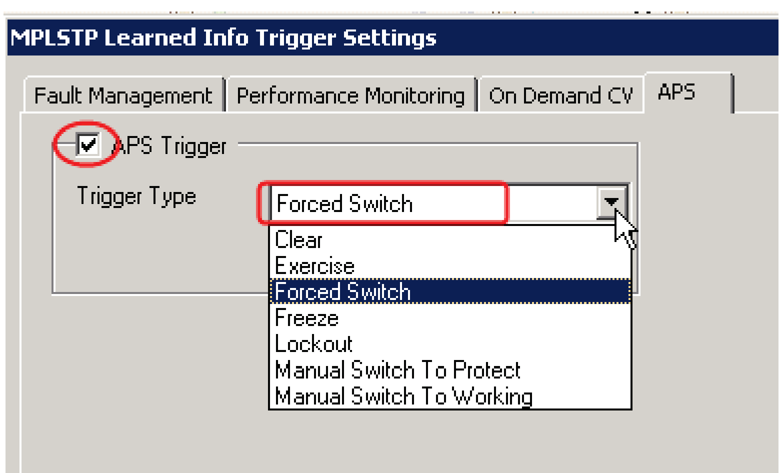


5. Finish the traffic wizard. Start protocol and ensure that all CCCV sessions are in the UP state. Next, start traffic. Ensure that there is no traffic loss on the working path while 100 percent loss on the protecting path, before issuing manual commands to test the DUT's ability to respond to individual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



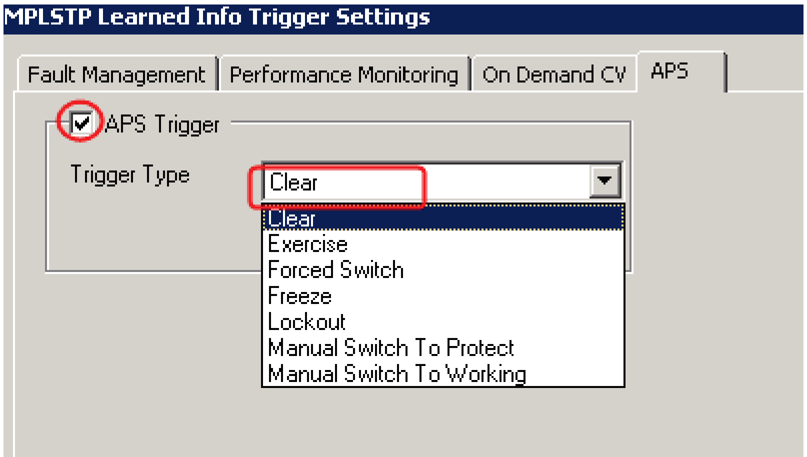
	Tx Port	Rx Port	Traffic Item	MPLS:Label Value	Tx Frames	Rx Expected Frames	Rx Frames	Frames Delta
1	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	100	26,753	26,753	26,753	0
2	10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	TestEgressDUT	101	26,752	26,752	26,752	0
3	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

6. 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.

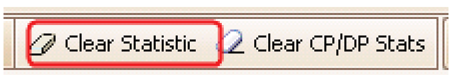


To verify if the DUT is performing the right action, go to traffic flow stats. Those LSPs that have been forced switch will have non-zero Loss over working path while RX frames on the corresponding protecting path will show RX frames with rate matching the sending rate.

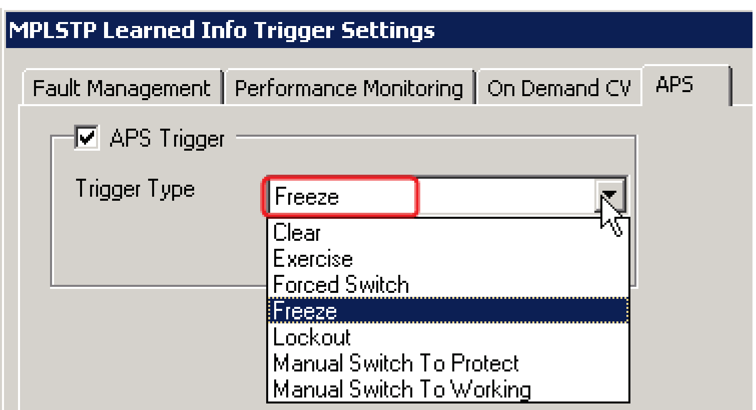
7. To verify Clear, click **Clear** in the **Trigger Type** list.



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).

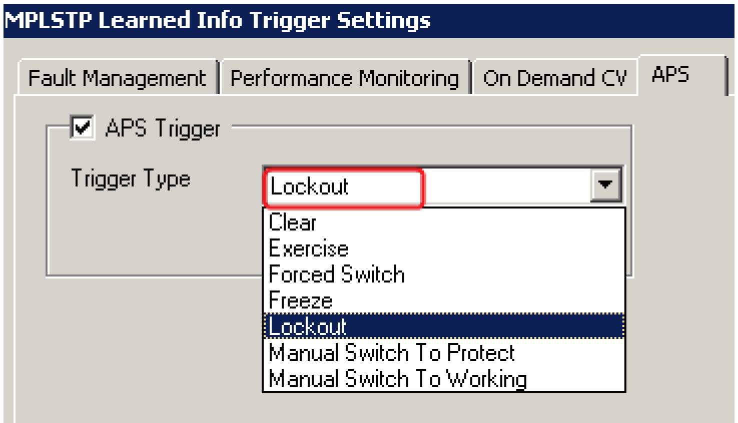


8. To verify Freeze, ensure that the protection state is in clear state. Next, issue a **Freeze** command from tester.



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.

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 ether 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.

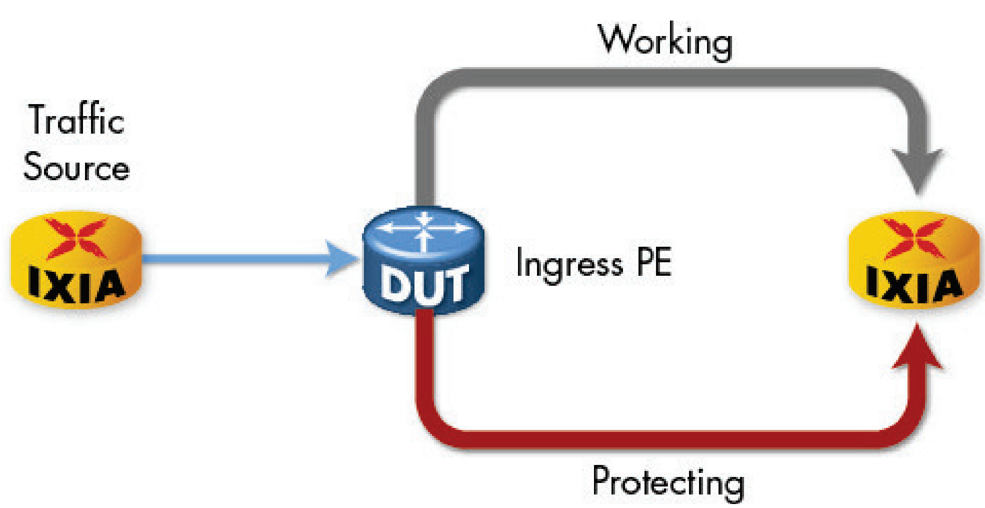
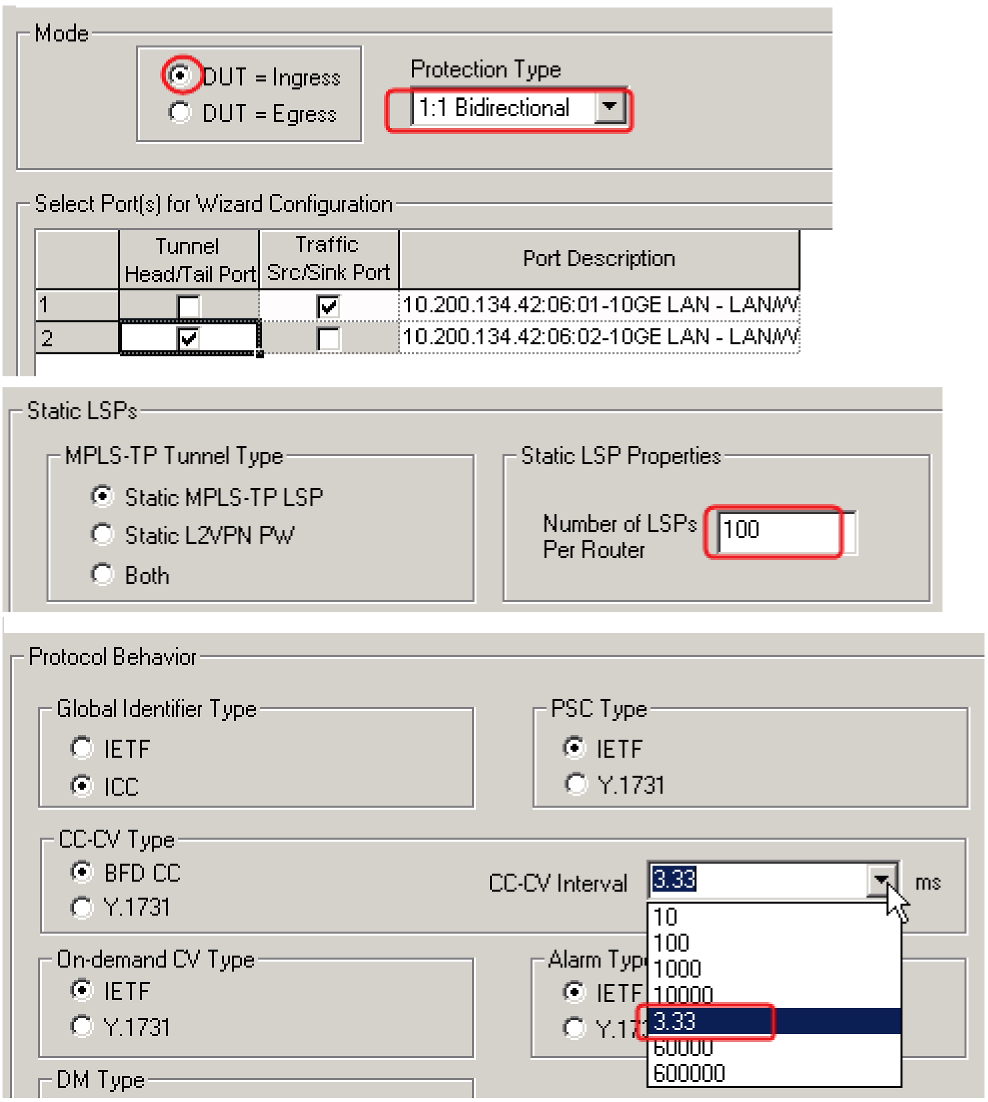


Figure 8 Test Setup for Testing MPLS-TP Scalability at 3.33 ms Interval

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.



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

MPLSTP Aggregated Statistics

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

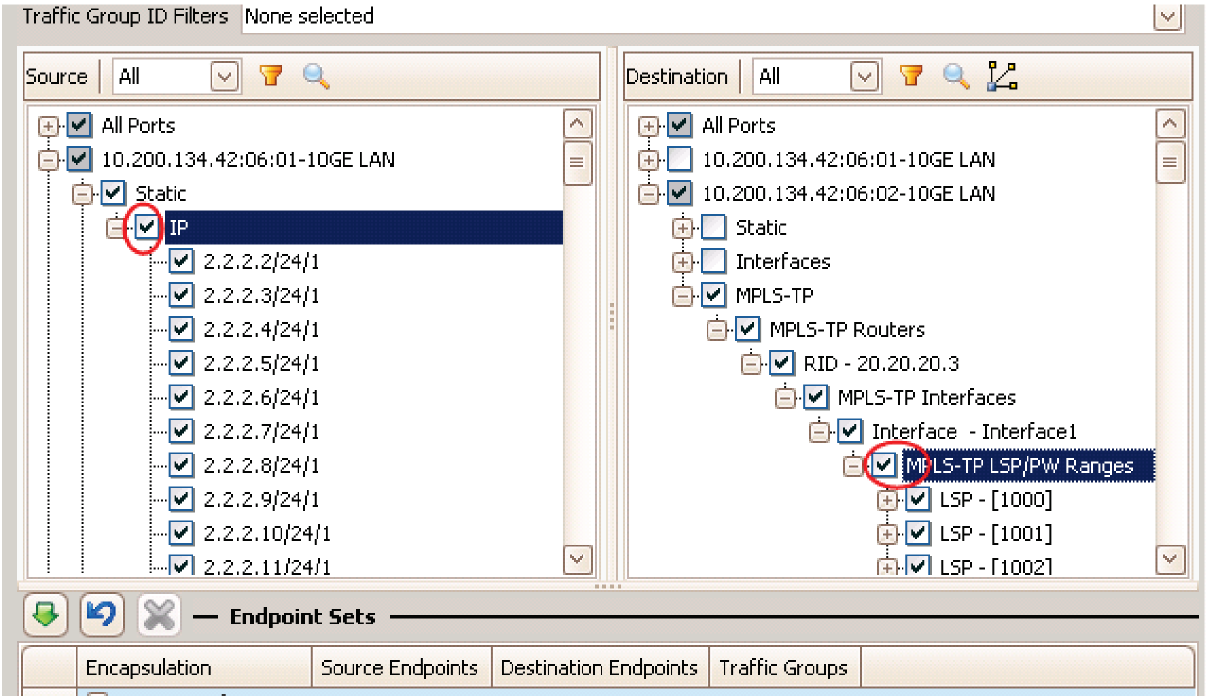
One quick way to check whether or not each session is running at 3.33 ms is by opening the Port Statistics. The next diagram shows about 66,000 packets per second as both TX and RX rate. Because there are 200 sessions, each is sending CC message at 3.33 ms (3 packets every 10 ms so 1 second is equivalent 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.

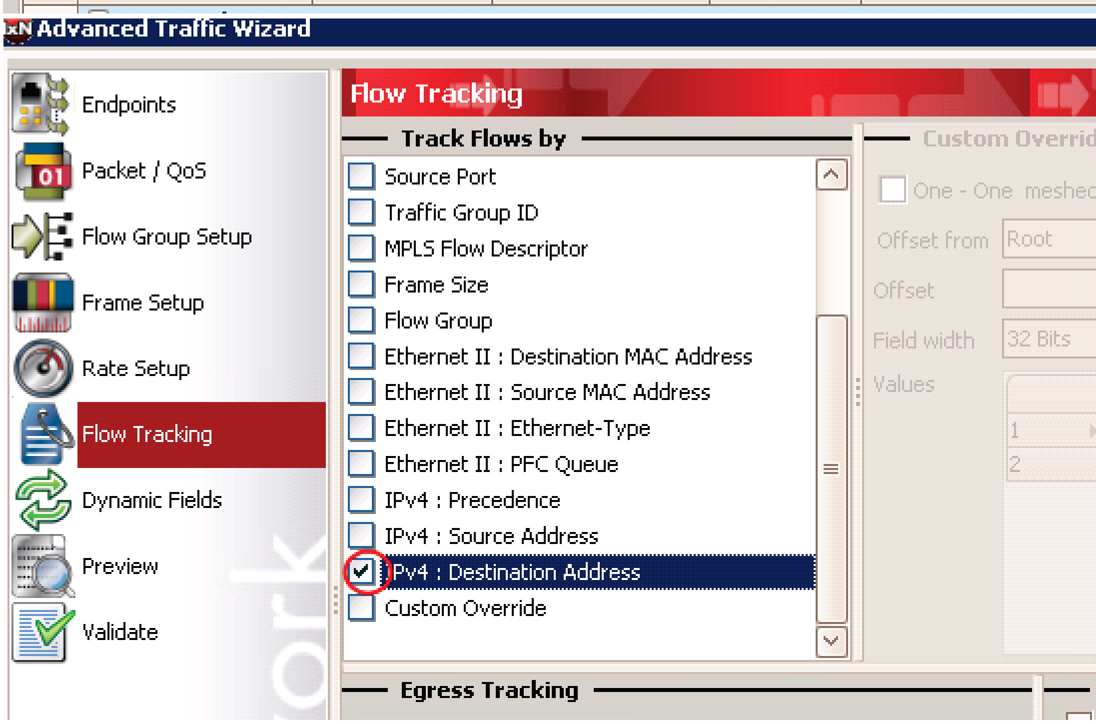
All

Port Statistics

	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	

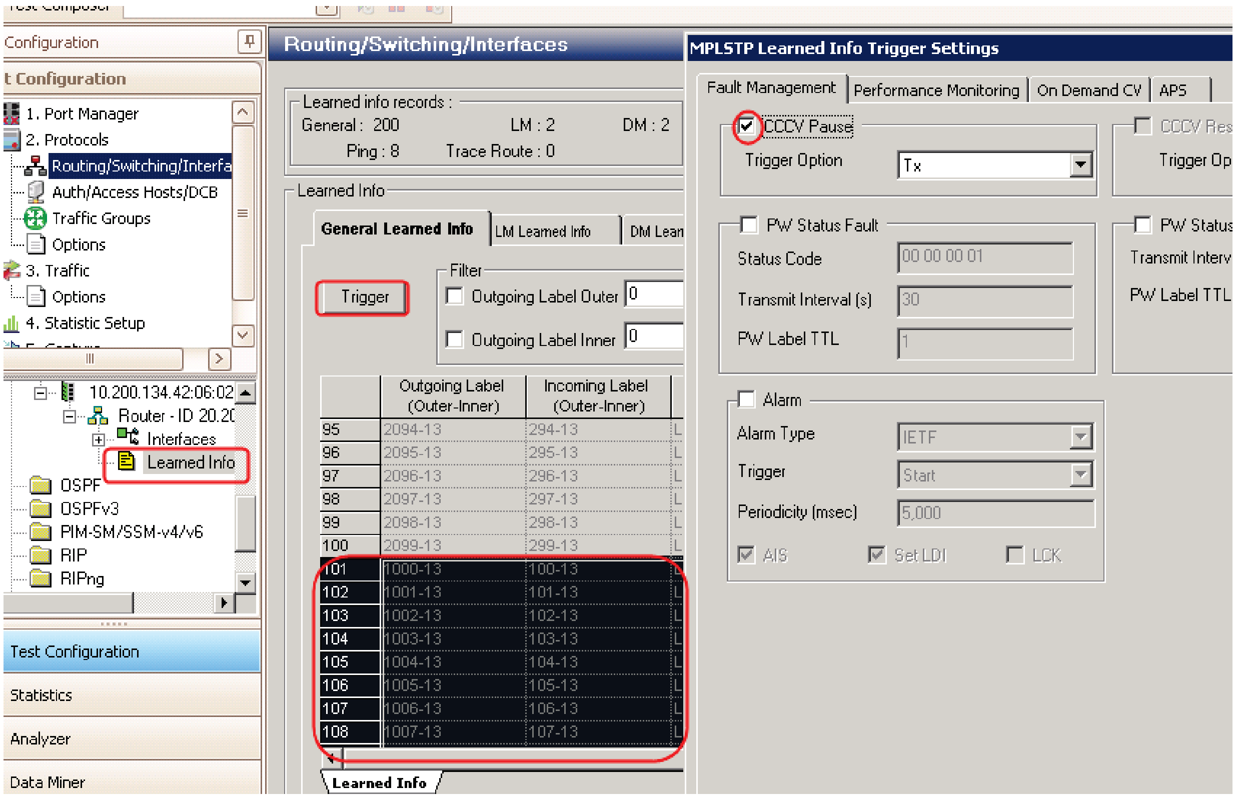
4. After the control plane is up and works as expected, use the traffic wizard to configure traffic. Select the static IP end point defined at the Traffic Source port and select all MPLS-TP LSP ranges in a one-one mapping. Select the Dest IP address as the tracking option. This will deliver per LSP performance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



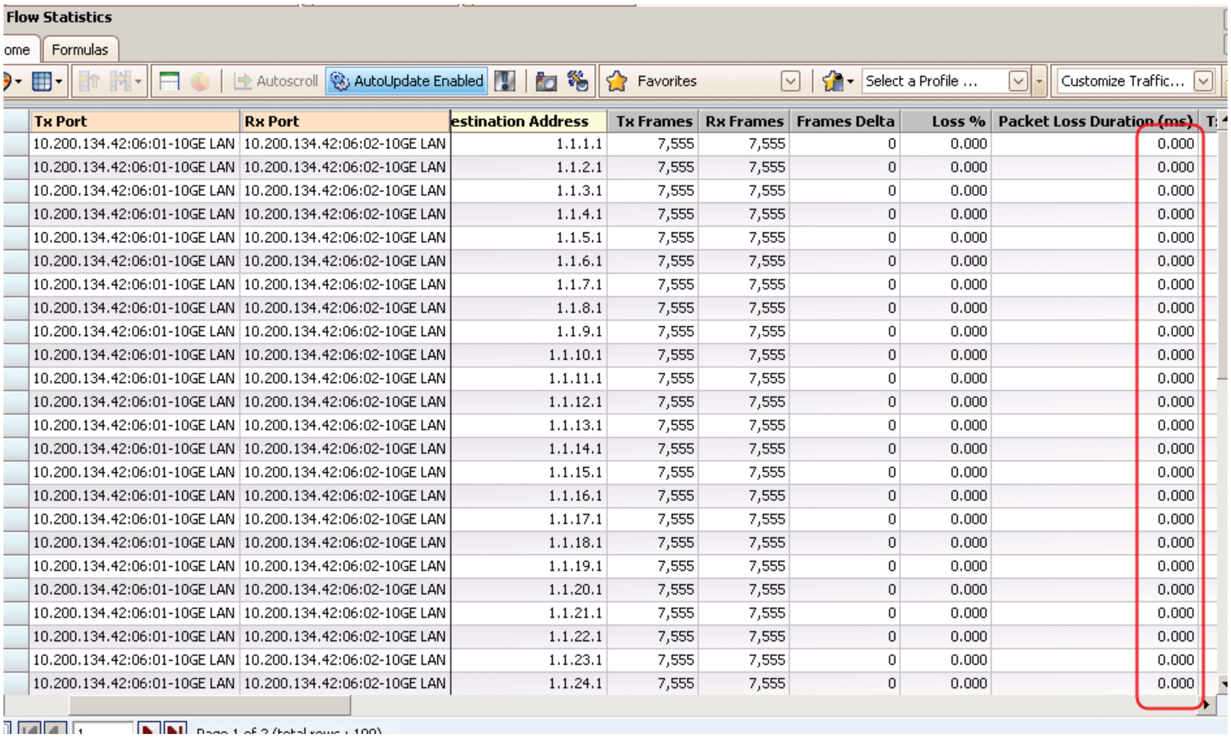


Test Scenario 5: Verify maximum MPLS-TP LSPs or PWs by using 3.33 ms Y.1731 CCM or BFD interval

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.

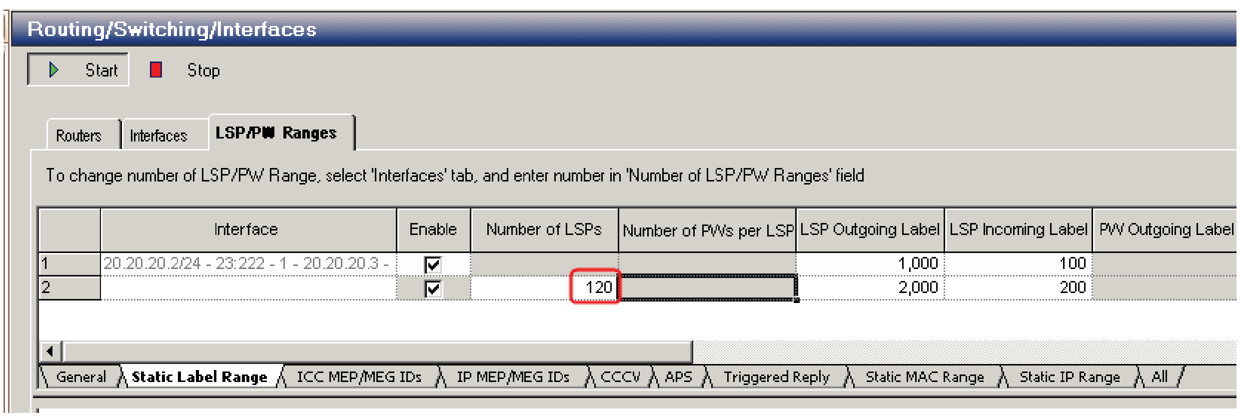


6. Observe the Packet Loss Duration due to switchover for all 100 LSPs. Ensure that they are within an acceptable range before increasing the number of LSPs under test.



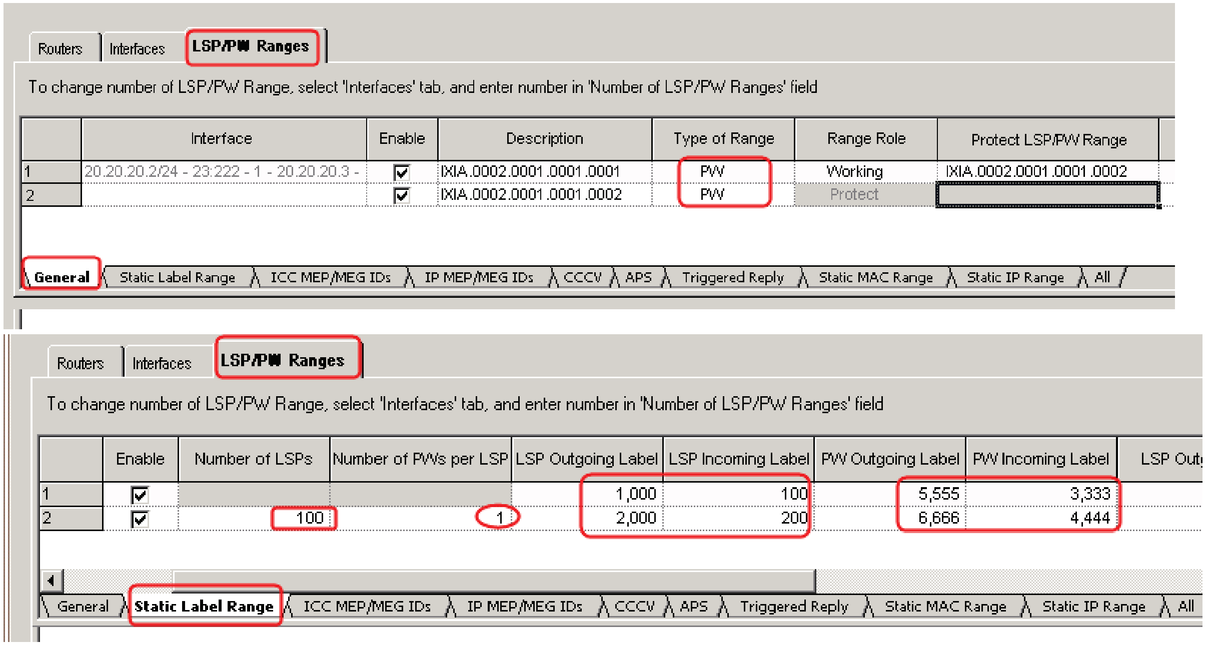
Tx Port	Rx Port	estination Address	Tx Frames	Rx Frames	Frames Delta	Loss %	Packet Loss Duration (ms)
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.1.1	7,555	7,555	0	0.000	0.000
10.200.134.42:06:01-10GE LAN	10.200.134.42:06:02-10GE LAN	1.1.2.1	7,555	7,555	0	0.000	0.000
10.200.134.42:06:01-10GE 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

7. 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.



	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 -	☑			1,000	100	
2		☑	120		2,000	200	

8. 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.



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.

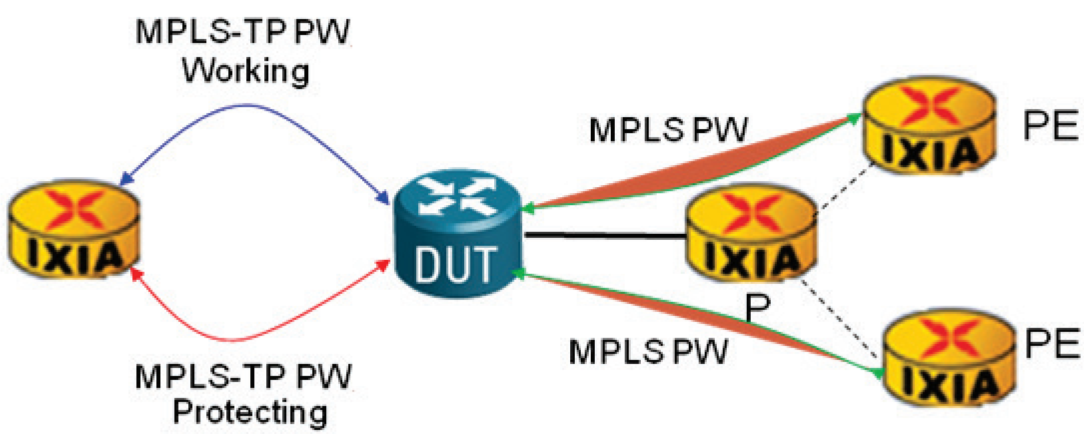
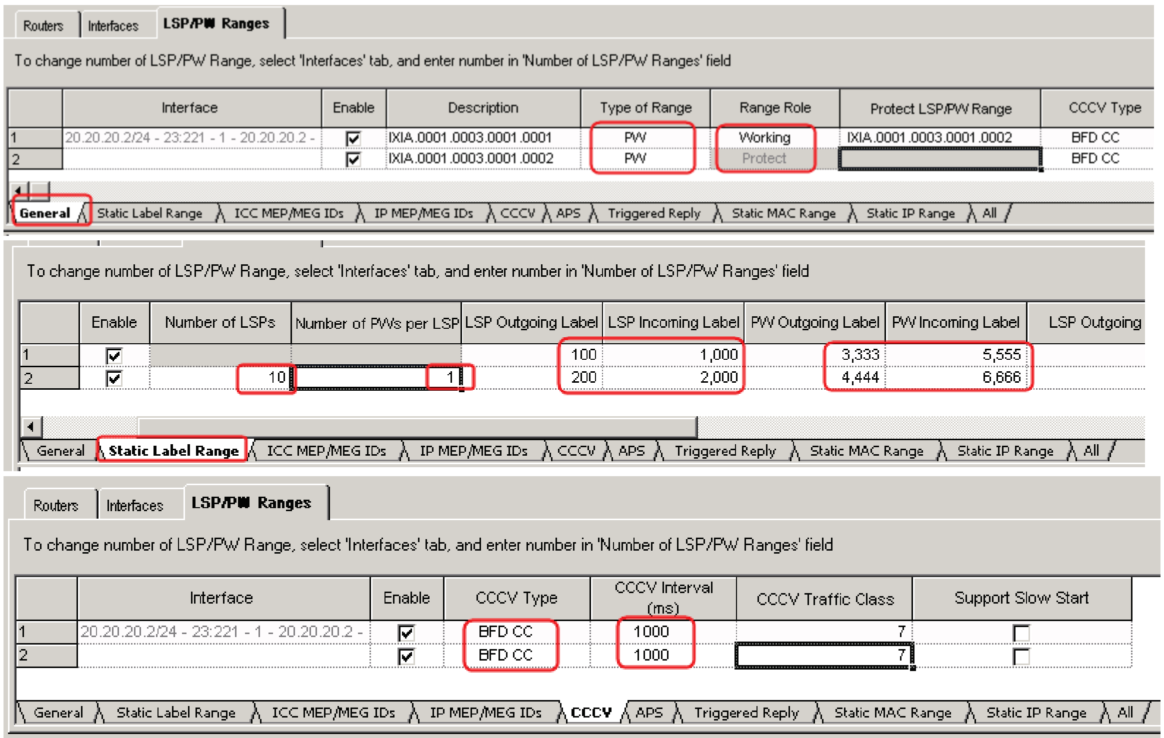


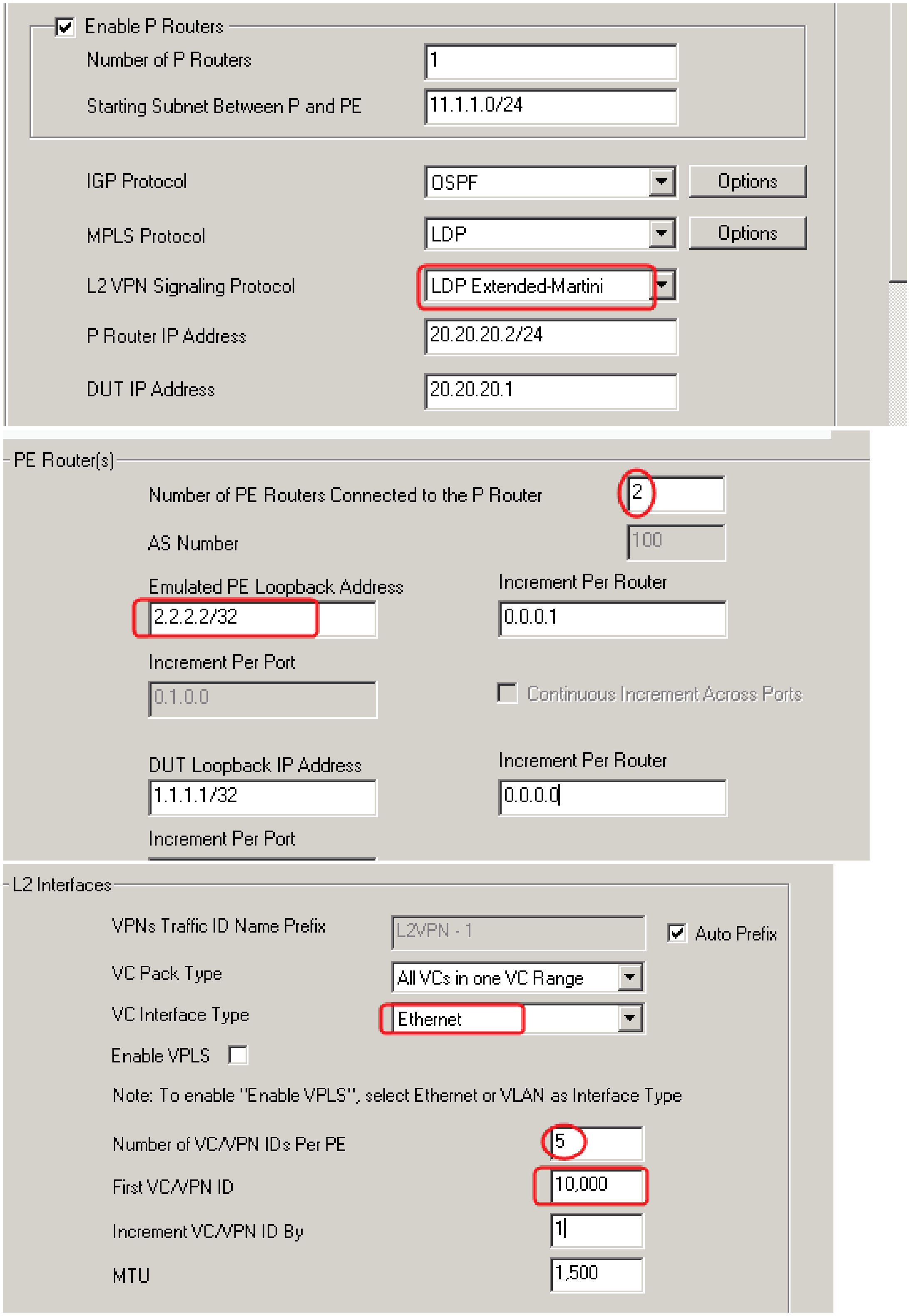
Figure 9 Test Setup for Testing IP/MPLS and MPLS-TP Coexistence

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.

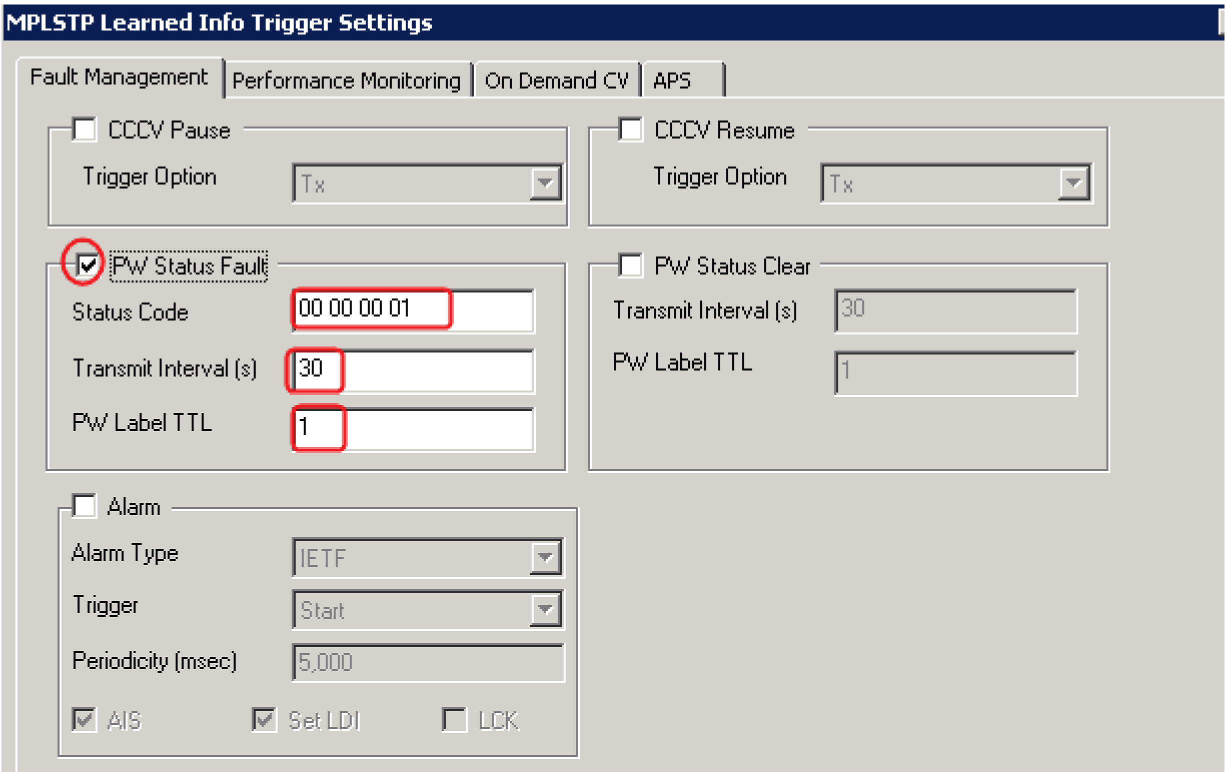


2. Use the L2VPN/VPLS wizard to configure the MPLS P/PE emulation port. Select 'LDP Extended Martini' as the L2VPN Signaling Protocol. Emulate 1 P and 2 PE routers each with 5 Ethernet PWs (EoMPLS VC).

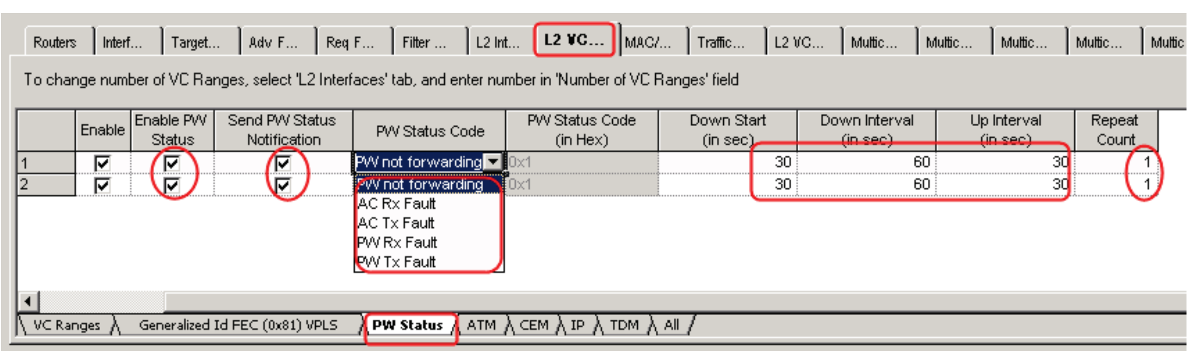


3. Start control plane for both test ports. Ensure that the MPLS-TP port has 20 CCCV sessions UP, and the MPLS port has 1 OSPF full session, 1 basic LDP session, and 2 t-LDP sessions up. The EoMPLS VC status is also UP.

4. Inject MPLS-TP PW status from the MPLS-TP port and capture and analyze the response on the MPLS side.



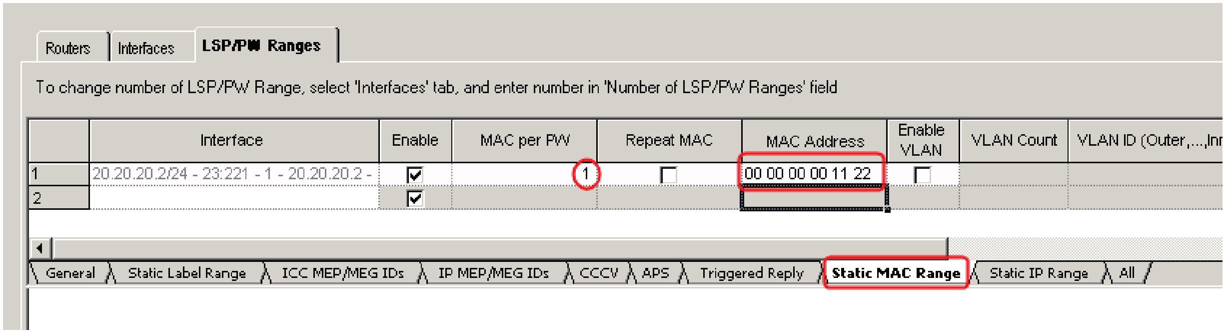
5. Inject L2VPN PW Status code from the MPLS port and capture and analyze the response from the MPLS-TP port.



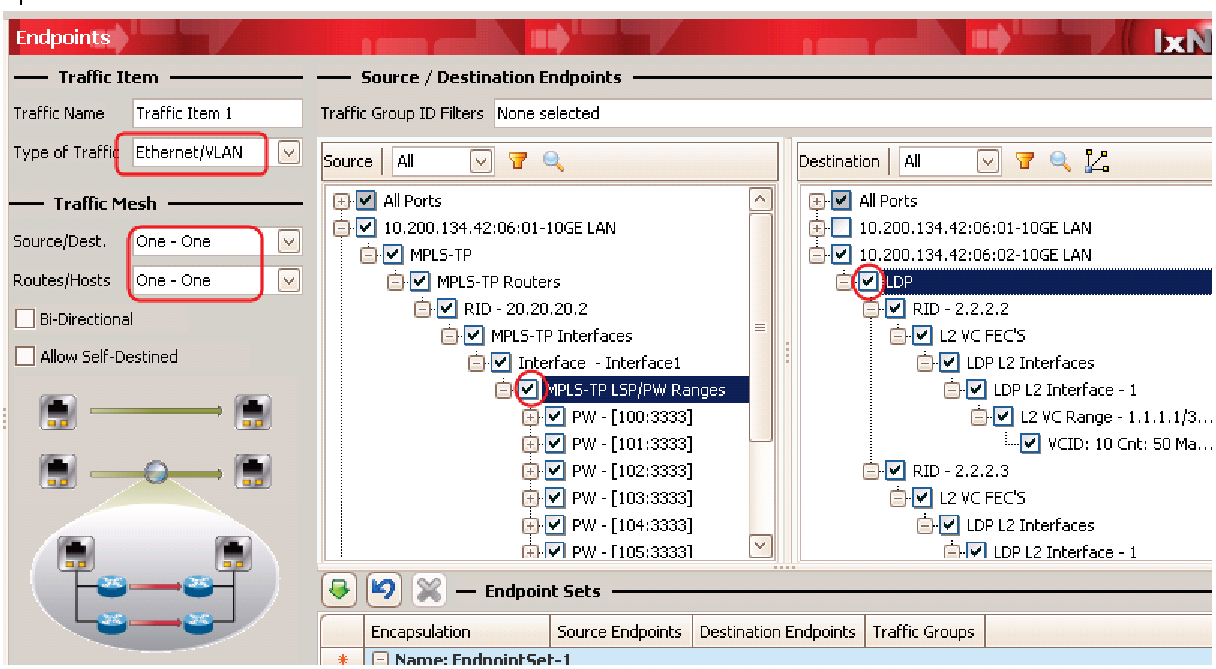
6. If VCCV-BFD is supported on the MPLS PW, we also recommended you to see if VCCV-BFD on the MPLS side will interop with BFD CC session on the MPLS-TP side.

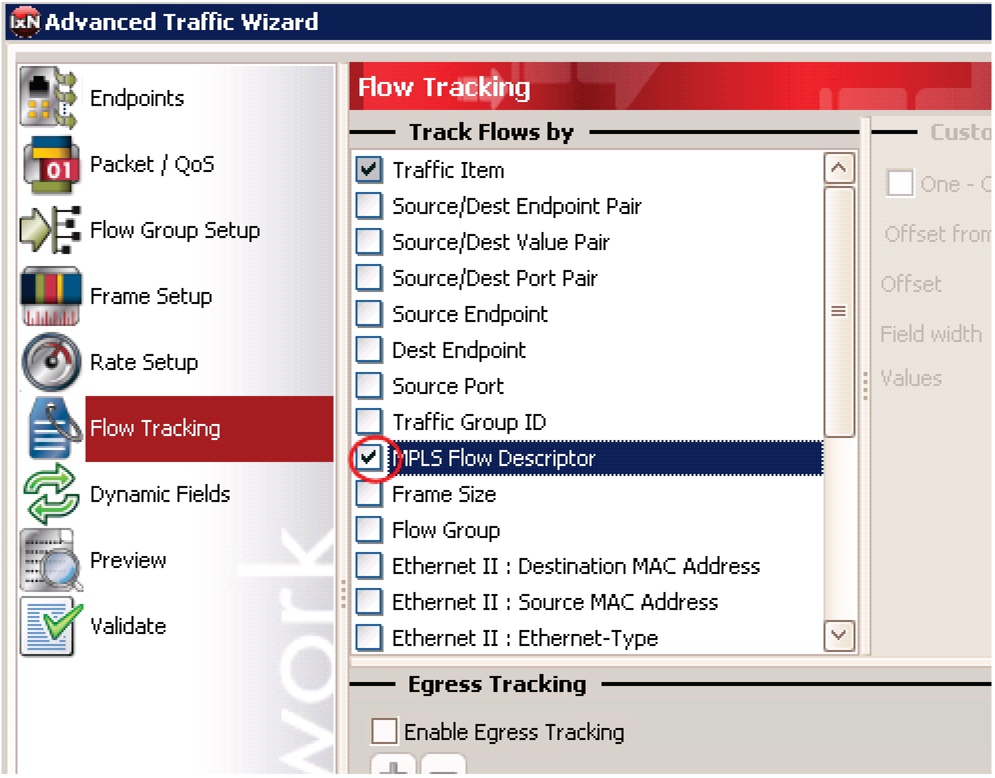
7. To generate traffic and verify end-to-end traffic delivery:

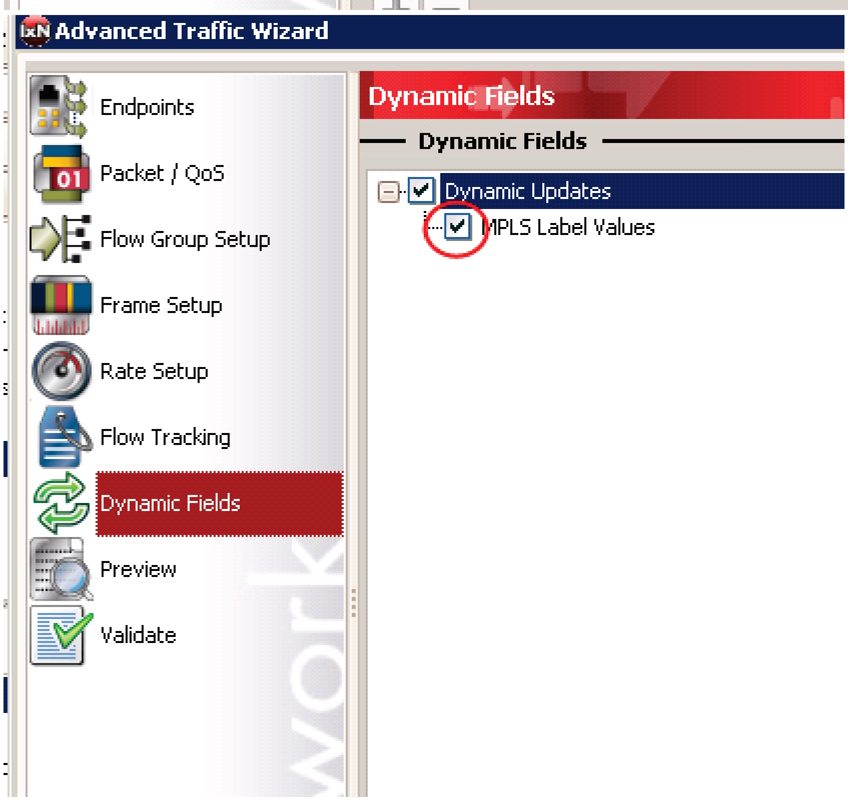
   a. Define static MAC hosts behind MPLS-TP PW ranges.



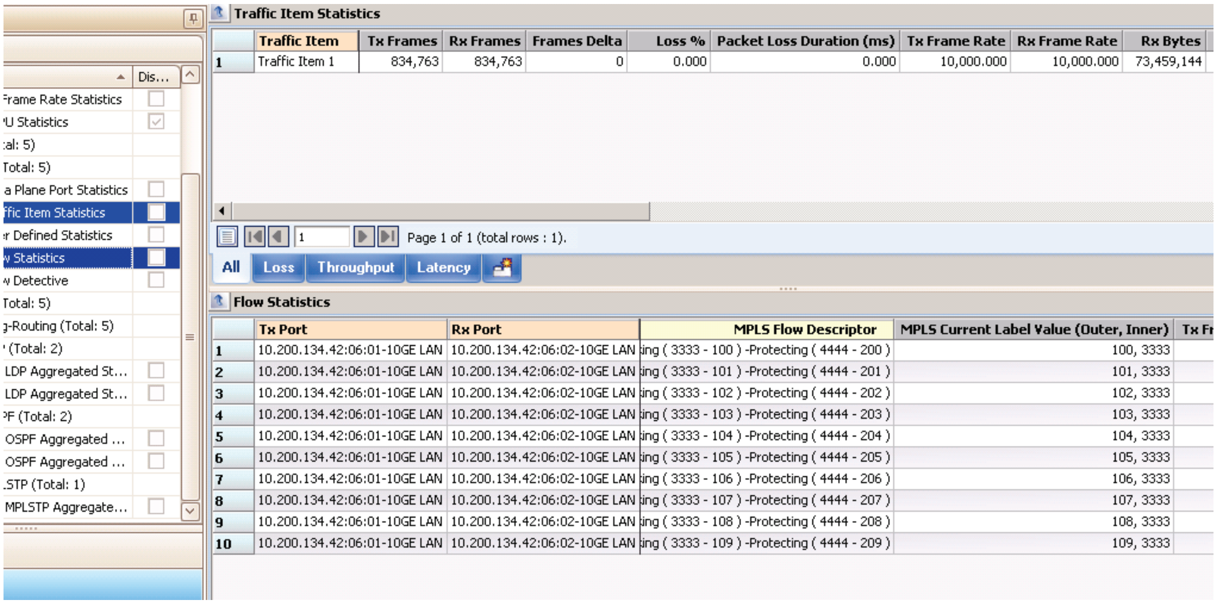
   b. Start the traffic wizard and select Ethernet/VALN as Type of Traffic. Pick up the static MAC address from MPLS-TP port and the MAC address behind each L2VPN PW VC. Enable tracking on MPLS Flow Descriptor. Turn on the Dynamic Label Change optioin.




Advanced Traffic Wizard
Endpoints
Packet / QoS
Flow Group Setup
Frame Setup
Rate Setup
Flow Tracking
Dynamic Fields
Preview
Validate
Flow Tracking
Track Flows by
Traffic Item
Source/Dest Endpoint Pair
Source/Dest Value Pair
Source/Dest Port Pair
Source Endpoint
Dest Endpoint
Source Port
Traffic Group ID
MPLS Flow Descriptor
Frame Size
Flow Group
Ethernet II : Destination MAC Address
Ethernet II : Source MAC Address
Ethernet II : Ethernet-Type
Egress Tracking
Enable Egress Tracking
Offset
Field width
Values


Advanced Traffic Wizard
Endpoints
Packet / QoS
Flow Group Setup
Frame Setup
Rate Setup
Flow Tracking
Dynamic Fields
Preview
Validate
Dynamic Fields
Dynamic Fields
Dynamic Updates
MPLS Label Values

8. 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.



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

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

Web site: www.ixiacom.com
General: info@ixiacom.com
Investor Relations: ir@ixiacom.com
Training: training@ixiacom.com
Support: 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

Support: eurosupport@ixiacom.com
+44 1628 405797
online support form:
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

Support: 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

Support: 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
+91 80 32918500
online support form:
http://www.ixiacom.com/support/inquiry/?location=india